**Тенденции развития антивирусного рынка**

Михаил Савельев

Сегодня вряд ли кто будет спорить о том, что защищаться от вирусов надо. Это демонстрируют данные ежегодного отчета Ernst & Young. В зависимости от внешних условий изменяются и антивирусные технологии. Понимание грядущих изменений необходимо для того, чтобы сегодня сделать правильные инвестиции в обеспечение безопасности. Теме дальнейшего развития антивирусных средств и посвящен настоящий обзор.

Не так давно основным требованием к антивирусному программному обеспечению было количество улавливаемых вирусов. Затем внимание стало уделяться скорости обновления базы вирусных сигнатур, что, несомненно, и сейчас является одним из самых важных критериев оценки эффективности того или иного антивирусного продукта. Однако условия меняются, и те антивирусные компании, которые по старинке придерживаются данного подхода и строят стратегию развития исходя из принципа «быстрее всех поймаем любой вирус», все чаще терпят фиаско. Анализ причин сложившейся ситуации, вероятно, следует начать с того, что сейчас вредоносный код - это не только традиционные вирусы и черви, но и такие «незваные гости», как всякого рода вредоносное программное обеспечение: шпионское и рекламное, «троянские программы», фишинговые атаки и т. д. Не стоит забывать и о «набившем оскомину» спаме. Кроме того, сегодня все чаще приходится сталкиваться с комбинированными угрозами, как по способам распространения (через файлы или по сети, эксплуатируя уязвимости ПО), так и по воздействию на атакуемую систему (от задействования вычислительных ресурсов до кражи или уничтожения информации).

Сегодня вирусные угрозы отличают впечатляющие скорости распространения, особенно современных компьютерных червей. Например, эпидемия червя Sasser в 2004 г. в течение недели с момента возникновения охватила 80 млн компьютеров. По теоретическим прогнозам, распространение «заразы» по всей сети Интернет сегодня может произойти минимум за 15 минут, максимум - за несколько часов.

Сокращается и время, затрачиваемое злоумышленниками на разработку подобных вредоносных программ. Интервал между анонсированием уязвимости и запуском нового вируса составляет в среднем 5 дней. Именно столько времени понадобилось хакерам для создания червя Zotob в августе 2005 г. Для сравнения, на создание того же Sasser'a год назад ушло 18 дней. Так что «прогресс» налицо. Что касается атак DayZero, то здесь вообще не приходится говорить о каком-либо интервале, ибо для таких атак используются обнаруженные хакерами, но пока не анонсированные уязвимости. Стало быть, и сигнатурные методы обнаружения вредоносной активности уже не спасают. То, что было эффективно еще пару лет назад, при современных скоростях распространения «эпидемий» становится абсолютно неэффективным. Поэтому сейчас основные разработчики активно внедряют технологии поведенческого анализа, направленные на обнаружение аномалий в поведении программ и процессов, атак, использующих еще неизвестные уязвимости, а также вредоносного кода, для которого пока не разработано никаких сигнатур (или они не доставлены до всех пользователей антивируса).

Следует также отметить, что защита, реализованная только на серверах и рабочих станциях, уже не является гарантированно эффективной. При таком подходе бороться с «инфекцией» приходится уже внутри сети, что увеличивает размер ущерба от заражения и затрудняет восстановление системы. Выход в данном случае один - организация антивирусной обороны по периметру сети - на шлюзах и сетевых устройствах.

Антивирусные продукты для защиты рабочих станций и серверов до сих пор занимают львиную долю в общем объеме продаж антивирусных компаний, и до недавнего времени продукты ведущих мировых вендоров отличались главным образом функциональностью в области управления и создания отчетов. Но ситуация начинает меняться - расширяются функциональные возможности антивирусных программ для рабочих станций, мировые вендоры взялись за дополнения своих решений персональными межсетевыми экранами и антишпионскими модулями. Многим антивирусным компаниям уже удалось реализовать (хотя бы частично) эти принципы защиты в своих продуктах. Так, например, средства обнаружения шпионского ПО применяют такие производители, как Trend Micro, McAfee и Symantec.

Каким представляется антивирусное решение в будущем? Логично предположить, что первыми на рынке появятся решения того поставщика, кто сумеет грамотно и полностью реализовать требования, предъявляемые к антивирусному ПО владельцами крупных сетей.

**Чего хотят от антивирусов крупные компании?**

Корпорации хотят видеть у себя антивирусное решение, которое защищало бы сеть от всего спектра угроз, объединенных под общим названием «вредоносный код». Использование самостоятельных решений по защите от спама, шпионского и другого вредоносного ПО неудобно по нескольким причинам. Основная - это самостоятельная консоль управления для каждого из таких продуктов, что не всегда хорошо даже в рамках сети небольшого предприятия, а в крупной сети и совсем лишено смысла. Множество центров управления разными продуктами снижает эффективность реагирования на инциденты и может вызвать дополнительные проблемы при борьбе с комбинированными угрозами.

Помимо того, что антивирусное решение становится комплексным, оно должно обеспечивать соответствующий уровень защиты от всех видов вредоносного кода. Если с обнаружением вирусов ситуация в целом достаточно стабильная, то с фильтрацией спама, шпионского ПО и т. д. дела обстоят далеко не так хорошо. Важным фактором здесь является и то, что разные продукты от разных поставщиков - это увеличение затрат на поддержку и эксплуатацию, что, естественно, приводит к повышению ТСО (совокупной стоимости владения).

**Что реализовано и какие недостатки?**

**Проблемы шпионского и рекламного ПО**

По результатам отчета исследовательской группы Gartner (Antivirus Vendors Strike Back With Anti-Spyware Products, ID G00129655) от 20 до 40% обращений пользователей в службу поддержки компании связано именно с проблемой получения такого рода вредоносного программного обеспечения. До недавнего времени существовало несколько самостоятельных антишпионских решений (например, Giant Company Software и Intermute, купленные сейчас компаниями Microsoft и TrendMicro), но ни одно из них не принадлежало ведущим разработчикам в области информационной безопасности. Как и во многих других сферах, масштабируемая и централизованная система управления средствами защиты является критически важным фактором, на который обращают внимание крупные компании, что, собственно, и отличает требования к решениям по информационной безопасности крупных корпораций от запросов небольших компаний. В этом довольно хорошо преуспели антивирусные компании.

Системы управления средствами защиты (компаний McAffee, Trend Micro, Computer Associates и др.) выполнены на достаточно высоком уровне, чего как раз не хватает продуктам независимых поставщиков антишпионских решений. Однако не в пользу самостоятельных разработчиков таких решений говорит тот факт, что корпорации предпочитают не усложнять существующую структуру своей сети и тем более ее защиту, без особой на то необходимости. Кроме того, антивирусные продукты и антишпионские системы решают примерно одну задачу: так или иначе они предназначены для борьбы с вредоносным ПО, и наличие двух сканирующих систем не имеет особого смысла, к тому же при этом не исключены конфликты ресурсов и проблемы с представлением данных (как для эффективного управления, так и для анализа).

Что же предлагают ведущие мировые поставщики в области антишпионского ПО? Начнем с того, что возможности этих решений по обнаружению известных вирусов составляют примерно 99%. Процент обнаружения шпионского ПО значительно ниже. К сожалению, в настоящее время не существует достоверных независимых тестов. По некоторым исследованиям и данным аналитических отчетов (например, Gartner), процент «отлова» шпионских программ достигает 75%.

Этому есть, по крайней мере две причины:

- скорость создания, например рекламного ПО, значительно выше, чем большинства вирусов;

- отсутствие сотрудничества между исследовательскими лабораториями, занимающимися антишпионским ПО, затрудняет создание единой базы данных образцов кода.

Тем не менее работа по интеграции антишпионского функционала в «движки» антивирусов идет полным ходом. Пока ни один из внедренных антишпионских модулей не получил высокой оценки, но, учитывая те усилия, которые прилагают производители антивирусов в данном направлении, можно ожидать, что им удастся обойти поставщиков независимых антишпионских решений. В ближайшее время антивирусные компании должны будут расширить свои решения по обнаружению шпионского ПО дополнительными возможностями по выявлению разного рода схожих с ним вредоносных программ.

До сегодняшнего дня есть серьезные проблемы в области защиты от шпионского ПО в реальном режиме времени и средств удаления такого рода программ из системы (особенно это касается рекламного ПО, составляющего до 90% шпионского).

**Антивирусная защита мобильных устройств**

Мы живем в век, когда средства коммуникации достигли того уровня развития, о котором, пожалуй, еще полсотни лет назад мечтали лишь писатели-фантасты. Мы не задумываемся над тем, какое расстояние преодолеваем, набирая номер мобильного телефона человека, находящегося за тысячи километров от нас. Думаю, никто не будет спорить с тем, что удобство использования мобильного телефона в качестве записной книжки, почтового ящика и средства доступа в Интернет значительно экономит наше время и облегчает ведение дел.

Смартфоны (как и другие карманные устройства, например, PDA) только завоевывают популярность в России, тогда как в западном бизнес-сообществе эти средства не использует разве что ленивый. Хакерское сообщество, в свою очередь, потирает руки - какое непаханое поле для создания и совершенствования нового вида угроз! Вирусописатели не спят и уже запускают свои «творения» в жизнь. Так, в 2004 г. увидел свет вирус для мобильных телефонов - Cabir, способный поражать не только сами мобильные телефоны, но и другие электронные устройства, оснащенные технологией Bluetooth (например, компьютерные системы автомобильной автоматической навигации).

Таким образом, почва для обширного распространения вредоносного кода для мобильных устройств уже подготовлена. По оценке аналитиков Gartner, «инфицирование» в масштабах глобальной эпидемии возможно, если не менее 50% всех устройств будут работать под одной операционной системой. Сегодня порядка 80% смартфонов работают с ОС Symbian, 45% PDA - на основе Microsoft Windows СЕ, так что можно считать это условие уже реализованным.

Как же бороться с такого рода «инфекцией»? На сегодняшний день у большинства сотовых операторов не существует антивирусных программ, входящих в пакет программных средств. Антивирусные вендоры предлагают продукты для защиты мобильных телефонов и КПК, что, однако, не является решением проблемы в глобальном масштабе.

Антивирусные решения для мобильных устройств, «зашитые» в самом устройстве, нельзя назвать высокоэффективными в борьбе с такими угрозами: никто не в состоянии заставить пользователей своевременно обновлять соответствующее программное обеспечение, никто не контролирует, не было ли оно удалено, поскольку не позволило получить доступ к какому-либо сайту, и т. д. Кроме того, эффективность подобного ПО в случае вирусной эпидемии представляется очень низкой, так как практически невозможно организовать централизованное обновление на большом количестве разрозненных устройств, принадлежащих разным людям.

Наиболее эффективным может стать использование технологии, получившей название in the cloud, не требующей установки на мобильный телефон антивирусного ПО. Принцип ее работы заключается в проверке трафика на шлюзах доступа в Интернет, который осуществляется централизованно и не требует каких-либо специальных действий от пользователя.

**Интеграция антивирусных технологий с сетевым оборудованием**

Наиболее вероятно, что следующей фазой эволюции антивирусных продуктов станет интеграция технологий борьбы с вредоносным кодом в сетевое оборудование. Для компаний такие решения интересны в первую очередь тем, что позволяют блокировать распространение «инфекции» на этапе подключения зараженного устройства к сети, независимо от способа - через маршрутизатор, коммутатор, точку беспроводного доступа и т. д. Это избавит администраторов от головной боли, связанной с подключениями узлов, состояние защищенности которых тяжело контролировать, - мобильных пользователей (прежде всего, представителей заказчиков и партнеров), сотрудников и партнеров, входящих в сеть через VPN, и т. д. Конечный пользователь получит возможность сохранения инвестиций, если такая технология уже поддерживается оборудованием, на котором работает сеть.

**Проблема спама**

Спам - досадная проблема практически для каждого пользователя, работающего с электронной почтой. Хотя угроза спама не является «в чистом виде» вирусной, по многим признакам ее часто относят именно к этой категории. Так, к «падению» почтового сервера может привести превышение объема спама на нем. Что уж говорить о потерях, которые терпят компании из-за того, что сотрудники вынуждены тратить часть своего рабочего времени на сортировку почты.

**Интернет-пейджеры**

Одним из средств коммуникации, получивших широкое распространение, стали службы обмена мгновенными сообщениями, или интернет-пейджеры. За последнее время появилось немало программ, атакующих пользователей пейджеров, в частности, такие вирусы для любимой в России «Аськи», как Bizex, Goner и Atlex.

С большой долей вероятности можно предположить, что данное направление будет более активно эксплуатироваться хакерами и в дальнейшем. Связано это с тем, что уязвимости в стандартных почтовых программах (например, Microsoft Outlook) обнаруживаются все реже, а объем информационных сообщений через интернет-пейджеры (в компаниях, где разрешено использование таких программ), как правило, превышает объем электронной почты, ведущейся средствами корпоративной почтовой системы.

**Заключение**

Антивирусное ПО - единственный продукт информационной безопасности, используемый практически в 100% компаний. Таким образом, все «околоантивирусные» решения со временем будут интегрированы в технологии ведущих антивирусных вендоров, чтобы обеспечить конечным заказчикам возможность более качественной защиты от данного спектра угроз и единое управление для этих продуктов. Конечно, антивирусные компании не в состоянии в сжатые сроки представить на рынок собственные разработки дополнительных средств обнаружения вредоносного ПО, которые бы конкурировали с независимыми разработками. Игроки рынка должны серьезно заняться собственными разработками в области дополняющих решений, чтобы обеспечить компании едиными инструментами управления этими средствами защиты.

**Список литературы**

Журнал «Connect!», №11.2005