Тенденции развития антивирусных программ.

Лежепёков И.А., Орёл ГТУ

Компьютерные вирусы – это программы, предназначенные для нанесения ущерба пользователю ЭВМ. Они малы по размерам (от 200 байт до 5 кбайт), самостоятельно запускаются, многократно копируют свой код, присоединяя его к кодам других программ.

Недавно главным 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. Вредоносный код - это не только традиционные вирусы и черви, но и всякого рода вредоносное программное обеспечение: шпионское и рекламное, «троянские программы», фишинговые атаки. К роме 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.

Сегодня вирусные угрозы отличают большие 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 червя 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. Создание компьютерных вирусов квалифицируется с юридической точки зрения как преступление. 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» на лицо. То, что было эффективно еще пару лет назад, при современных скоростях распространения «эпидемий» становится абсолютно неэффективным. Создание антивирусных программ начинается с обнаружения вируса по аномалиям в работе компьютера. После этого вирус тщательно изучается, выделяется его сигнатура-последовательность байтов, которая полностью характеризует программу вируса (наиболее важные и характерные участки кода), выясняется механизм работы вируса, способы заражения.

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 огромную долю в общем объеме продаж антивирусных компаний. Расширяются функциональные возможности антивирусных программ для рабочих станций. Однако наиболее востребованными являются продукты для крупных компьютерных сетей.

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 рекламного и шпионского ПО. 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.

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. 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.

Возможности антишпионского ПО по обнаружению известных вирусов составляют примерно 99%. Процент обнаружения шпионского ПО значительно ниже. Пока ни один из внедренных антишпионских модулей не получил высокой оценки.

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).

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 CE, так что можно считать это условие уже реализованным.

На сегодняшний день у большинства сотовых операторов не существует антивирусных программ, входящих в пакет программных средств.

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.

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.

Помимо программных средств защиты от вирусов существуют специальные аппаратные устройства, обеспечивающие защиту. 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. Конечный пользователь получит возможность сохранения инвестиций, если такая технология уже поддерживается оборудованием, на котором работает сеть.

Проблема спама является актуальной 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.

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 ICQ, как Bizex, Goner и Atlex.

С большой долей вероятности можно предположить, что данное направление будет более активно эксплуатироваться хакерами и в дальнейшем.

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.

Список литературы:

1. **Ф.Файтс, П.Джонстон, М.Кратц** «Компьютерный вирус: проблемы и прогноз». Москва, «Мир», 1998 г.
2. Dr.Web, Sophos, Antigen и др. антивирусы, антиспам, персональные и офисные сетевые экраны (firewall), программы шифрования файлов, каталогов, дисков. / ЗАО "ДиалогНаука" [Электронный ресурс] / http://www.dials.ru/
3. Лаборатория Касперского – Антивирус [Электронный ресурс] / http://www.avp.ru/
4. **А.В. Могилев, Е.К. Хеннер**, «Информатика: учебное пособие для студ. пед. вузов». Москва, Издательский центр «Академия», 2004 г.
5. Журнал «Connect!», №11.2005