носителей информации – виртуальных логических дисков. Вся информация, записываемая на такие носители, подвергается «прозрачному» (на лету) преобразованию с использованием одного из следующих алгоритмов: встроенный алгоритм преобразования данных с длиной ключа 128 бит; входящая в Windows реализация RC-4 (с длиной ключа 40 бит); алгоритм шифрования по длиной ключа 256 бит (при использовании эмулятора платы «Криптон», имеющего сертификат, так напр. ФАПСИ).Семейство средств защиты информации «Secret Disk» включает в себя модификации для защиты информации на автономных ПЭВМ и комплексы защиты информации, хранимой и обрабатываемой на выделенных серверах ЛВС.

Широкое внедрение в повседневную практику компьютерных сетей, их открытость, масштабность делают проблему защиты информации исключительно сложной. Выделяют две базовые подзадачи: 1.Обеспечение безопасности обработки и хранения информации в каждом из компьютеров, входящих в сеть; 2.Защита информации, передаваемой между компьютерами сети.

Международное признание для защиты передаваемых сообщений получила программная система PGP (Pretty Good Privacy - очень высокая секретность), разработанная в США и объединяющая асимметричные и симметричные шифры. Являясь самой популярной программной криптосистемой в мире, PGP реализована для множества операционных сред -MS DOS, Windows , Windows NT, OS/2, UNIX, Linux, Mac OS, Amiga, Atari и др.

Бизнес информация экономического анализа имеет строго конфиденциальным характером. Современный финансовый бизнес анализ невозможен без применений IT системы. Проблемма конфиденциальноти и защитый IT информации результатов анализа сложная но она имеет ключевое значение.

ВИРУСЫ СЕМЕЙСТВА МОБИЛЬНЫХ УСТРОЙСТВ И ИХ МОДИФИКАЦИИ

Михаил БАЛЫЧЕВ, Владимир ФЕДОРЧЕНКО
Харьковский Национальный Экономический Университет, (Украина)

Viruses are a family of mobile devices is appearing more frequently, as well as new operating systems for these devices. Developers virus software codes, each time finding more and more sophisticated method of distribution, using all communication devices.

Вирусы семейства мобильных и их модификации на сегодняшний день появляются с такой же завидной регулярностью, с какой выходят на рынок новые устройства под управлением все новых операционных систем (ОС) [1, 2]. Чаще

всего у ничего не подозревающего пользователя смартфона с встроенным Bluetooth сначала без видимых причин происходит перезагрузка, а потом и вовсе устройство выходит из строя.

История развития вирусов для мобильных устройств не продолжительна. Она началась 14-го июня 2004 года, когда появился очередной проект команды 29A (http://www.29a.net, известная специалистам группа разработчиков специфического программного обеспечения, сейчас часть ее участников осуждена, а другая прекратила поддержку проекта 29A).

Имя, которое они дали первому вирусу – Caribe – надолго осталось в истории и трудах исследователей вирусов. Данный вирус для телефонов под управлением Symbian OS (телефонов Series 60 от Nokia) умел только инсталлировался, ОС при этом просила подтверждения прав доступа, после чего программа рассылала инсталяторы, используя интерфейс Bluetooth. Целью атаки было любое устройство, имеющее этот стандарт. Caribe не фильтровал устройства, посылая вирус на них, хотя работал только на телефонах от Nokia.

Вирус, действительно начинающий историю вирусов под мобильные платформы, появился в марте 2005 года под именем Commwarrior. Он уже мог распространяться не только через Bluetooth, а еще использовал принципиально новый способ распространения - через MMS, что значительно ускорило его распространение, вирус был написан российским программистом «e10d0r», позже появился похожий иностранный вирус – Mabir.

Ситуация с карманными компьютерами и мобильными устройствами под управлением WinCE или Windows Mobile более стабильна: существует несколько вирусов и ряд их модификаций. Один из них - Duts - вирус в классическом понимании этого слова, он заражает exe-файлы, дописывая собственный код в зараженный файл,. Другой – Brador - троян, открывающий порт 2989 и предоставляющий право отправлять и получать файлы, отображать сообщения и исполнять некоторые команды операционной системы. По одной из версий оба вируса принадлежат группе 29A, причем исходный код Duts еще можно найти в Сети. Однако этот вирус написан на ассемблере, что подразумевает знания в этой области, а также в работе ОС Windows Mobile для того чтоб разобраться в принципе работы вирусов.

Способов распространения вирусов под мобильные телефоны немного. Так, это технология Bluetooth (радио с ограниченным около десяти метров радиусом действия). Беспроводные технологии в современном мире обретают все большую популярность, программисты не могли пропустить возможность таким способом распространять свои вирусы. Поэтому любое устройство, находящееся в режиме обнаружения, может подвергнуться атаке, при этом посылается сообщение в виде установочного SIS-файла (для Nokia стандарт первоначально служил для распространения игр), при получении файла пользователь вправе выбрать, принимать сообщение или нет. После принятия сообщения пользователь снова получит право выбирать, устанавливать ли приложение, и только после того, как

будет получено согласие, вирус получит доступ к устройству. Следовательно, возможно исключение заражения вирусом на любом этапе, что сказывается на его распространяемости. Классическими примерами вирусов, использующих Bluetooth для распространения, являются Caribe, CommWarrior, Mabir, MGDropper.

Существует стандарт MMS, он позволяет присоединять всяческие файлы к сообщению, и вирусы таким образом получают дополнительный способ размножения. При открытии присоединенного к сообщению файла, его установке, открывется дорога вирусу. Так распространяются такие вирусы, как Commwarrior и Mabir.

Также переносчиком вируса может выступить O-DAY soft. Используя желание пользователей получить и установить последнюю версию игры или популярной программы с каким либо дополнением, вирус встраивает и внедряет в установочные файлы версию себя - в придачу к общему пакету. Так размножается Dampig, Mos, который пользуется игрой Mosquitos, Doomboot, прикрывающийся игрой Doom.

Остановимся на последствуях заражения телефона вирусами. Как пример, рассмотрим смартфон Nokia или другой фирмы с Symbian OS. Эта ОС широко распространена, развита с точки зрения функциональности, имеет открытое детальное описание, которое может быть использовано как разработчиком так и создателем вируса. В результате с телефоном можно сделать практически все: отключить Bluetooth, встроенный файловый менеджер, телефонную книгу (вирус Dampig), повредить системные файлы ОС (Doomboot и Hobbes). Также может произойти рассылка SMS-сообщений (Mos), а вирус Onehop, который перезагружает телефон как только пользователь попытается воспользоваться системными приложениями.

Механизмы самозащиты у самих вирусов не слишком разнообразны. Так, вирус под названием Drever после инсталляции начинает затирать все антивирусные программы, обнаруженные им на карте памяти мобильного телефона. Вирус Doomboot просто не показывает своего присутствия в телефоне, он устанавливается вместе с игрой (похожий механизм у Dampig). CommWarrior прикрывается в MMS фантастическими программами или обновлениями от www.symbian.com ("Dr.Web! New Dr.Web antivirus for Symbian OS. Try it!", "MS-DOS emulator for SymbvianOS. Nokia series 60 only. Try it!", "SymbianOS update" и т.д.).

Изначально вирус должен где-то распространяться, поэтому ему нужна как основа ОС с множеством функций. Она должна быть популярна, хорошо документирована, так как вирус нуждается в информации для анализа уязвимостей ОС. И как только новая ОС становится популярной, тут же появляются и вирусы под нее.

Однако опасность возникнет лишь когда разработчики вирусов являются профессионалами и нацелены на финансовые результаты от действия вируса. Это возможно при широком распространения какой-либо одной ОС, то есть в случае монополизации рынка, или в результате глобального развития кросс-платформенных языков типа Java, которые позволят полноценно управлять телефоном.

Поэтому для исключения заражения не следует открывать и устанавливать программы, приходящие по Bluetooth, MMS с незнакомых номеров. Даже если

программа пришла от знакомого, следует это перепроверить. Разумеется, следует опасаться программ, скачанных из ненадежных (непроверенных) источников, например p2p-сетей. Также необходимо использовать шифрование особо важных данных: номеров кредитных карт, паролей и т.д. И наконец, рекомендуется использовать соответствующие антивирусные программы.

Очевидно, что с развитием технологий и программных средств под мобильные устройства вирусы для них станут такими же развитыми, как их PC-варианты. Ожидается появление полиморфных вирусов, новых методов их маскировки и противодействия антивирусам.

Таким образом складывается новое научно-техническое направление – безопасность мобильных устройств, требующее как исследования непосредственно самих вирусов, так и развития аппаратных и программных средств антивирусной защиты.

Литература

1. М.Букин. Секреты сотовых телефонов. М., «Питер», 2005, 206 с.
2. P.Wang, M.González, C.Hidalgo. Understanding the Spreading Patterns of Mobile Phone Viruses. // Science, 2009, Vol. 324 No. 5930 pp. 1071-1076.

МОЛДОВА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

А. К. РУСНАК,
Молдавская Экономическая Академия,
Кишинев, Республика Молдова

Статься рассматривает некоторые проблемы информационной безопасности в Республике и предлагает пути их решения.

Ключевые слова: *информация, информационная безопасность.*

Под информационной безопасностью понимается состояние защищённости информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера.

Цель информационной безопасности – обезопасить главные ценности информационной системы, защитить и гарантировать доступность и целостность информации, не допустить утечку информации, свести к минимуму ущерб от событий несущих угрозу информационной безопасности.

Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый целостный механизм.

Существующая в настоящий момент в мелком, среднем и даже крупном бизнесе и государственном секторе практика обработки важной (в том числе секретной) информации на компьютерах, подключенных к сети Интернет, а так же исполь-