УДК:004.49
004.056.57
621.395.721.5

Вирусы для мобильных устройств

Бирюкова Т.В., Госуниверситет УНПК, 11-ИБ

На первый взгляд, проблема вирусов является лишь частным случаем проблемы безопасности цифровой системы, но история «стационарных» компьютерных вирусов опровергает это предположение: в ходе своего развития вредоносные программы для персональных компьютеров постепенно мутировали от невинных поделок до сложных профессиональных решений, связанных с извлечением финансовой выгоды.

История вирусов для мобильных устройств начинается в июне 2004 года, когда командой вирусописателей-профессионалов 29A был создан первый вирус для смартфонов. Вирус «называет себя» Caribe, функционирует на базе операционной системы Symbian и распространяется по Bluetooth.

Самый первый вирус хоть и произвел много шума, являлся исключительно концептуальной разработкой. Авторы такого рода разработок, движимые любознательностью и стремлением поспособствовать укреплению безопасности атакованной ими системы, обычно не заинтересованы в их распространении или злоумышленном использовании. Действительно, оригинальный экземпляр Worm.SymbOS.Cabir(первый вирус для мобильных устройств) был разослан в антивирусные компании по поручению самого автора, однако позже исходные коды червя появились в интернете, что повлекло за собой создание большого количества новых модификаций данной вредоносной программы. Фактически, после публикации исходных кодов Cabir начал самостоятельно «бродить» по мобильным телефонам во всем мире.

Через месяц после Cabir антивирусные компании обнаружили очередную технологическую новинку. Virus.WinCE.Duts - это первый известный вирус для платформы Windows CE (Windows Mobile), а также —

первый файловый вирус для смартфонов. Duts заражает исполняемые файлы, предварительно, спросив разрешения у пользователя.

Продолжение виртуальной атаки на Windows Mobile не заставило себя долго ждать: через месяц после Duts появился Backdoor. Эта вредоносная программа открывает доступ к зараженному устройству по сети, ожидая подключения злоумышленника на определенном порту. Когда зараженное устройство подключается к интернету, бэкдор отсылает его IP-адрес по электронной почте своему хозяину.

На этом активность самых квалифицированных исследователей безопасности мобильных устройств практически заканчивается. Последовавший за Brador Trojan.SymbOS.Mosquit представляет собой изначально безвредную игру для платформы Symbian. Модифицированная игра при запуске начинает отправлять SMS-сообщения на указанные в коде номера телефонов, подпадая под определение «троянской программы».

После трехмесячного перерыва, в ноябре 2004, на некоторых интернет-форумах мобильной тематики был под видом установочного пакета новых иконок и «тем» рабочего стола размещен новый Symbian-троянец — Trojan.SymbOS.Skuller. Программа представляет собой SIS-файл — приложение-инсталлятор для платформы Symbian. Ее запуск и установка в систему приводит к подмене иконок (AIF-файлов) стандартных приложений операционной системы на иконку с изображением черепа. Одновременно в систему, поверх оригинальных, устанавливаются новые приложения. Переписанные приложения перестают функционировать.

Второй троянец этого класса — Trojan.SymbOS.Locknut — появился через два месяца. Он эксплуатирует «доверчивость» (отсутствие проверок целостности файлов) Symbian уже более целенаправленно. После запуска вирус создает в системной директории /system/apps/ папку с неблагозвучным с точки зрения русского языка названием gavno. При этом во всех файлах вместо соответствующей их форматам служебной информации и кода содержится обычный текст. Операционная система, исходя только из расширения файла gavno.app, считает его исполняемым — и зависает,

пытаясь запустить «приложение» после перезагрузки. Включение смартфона становится невозможным.

С этого момента начали появляться троянцы, эксплуатирующие уязвимость Symbian. Они регулярно появляются и по сей день, отличаясь лишь конкретным способом эксплуатации.

Сейчас новые вредные программы под ОС для мобильных устройств (не считая модификаций уже известных вирусов) появляются в среднем один раз в месяц.

Сфера интеллектуальных мобильных устройств в настоящий момент полностью «открыта» и беззащитна как с технической, так и с социальной точки зрения. Для карманных компьютеров и «умных» телефонов «проверка боем» только началась, поэтому их безопасность находится на некоем изначальном, «нулевом» уровне.

Учитывая инертность массового сознания по сравнению со скоростью развития высоких технологий, техническое решение обнаруженной проблемы безопасности какое-то время не имеет должного эффекта. Обобщенному «пользователю компьютера» потребовались годы после начала вирусных эпидемий на то, чтобы включить антивирусные утилиты в свой набор программ, и месяцы после начала эпидемий почтовых червей на то, чтобы научиться менее легкомысленному отношению к запуску неизвестных программ, приходящих по электронной почте.

Об уровне же технической защищенности смартфонов можно приблизительно судить по тому, с какой легкостью выводится из строя (вплоть до необходимости в сервисной перепрошивке) аппарат под управлением ОС Symbian. Функционал большинства известных мобильных вирусов основан исключительно на эксплуатации нескольких «особенностей» этой операционной системы: возможности перезаписи любых файлов, включая системные, и крайней неустойчивости системы при ее столкновении с неожиданными (нестандартными для данного дистрибутива либо поврежденными) файлами.

Большинство производителей техники с функцией обмена

информацией через Bluetooth по умолчанию включают эту функцию. Владельцы подобных устройств могут даже не подозревать о том, что их мобильный телефон «видим» для всех владельцев Bluetooth-устройств в окрестности 10-20 метров и потенциально открыт для обмена информацией. Технологии беспроводной передачи данных в настоящий момент могут обеспечить злоумышленнику близкую к абсолютной степень анонимности.

Самую большую угрозу безопасности мобильных устройств представляют собой самостоятельно распространяющиеся вирусы — черви. Червь потенциально способен вызвать очень быстрое заражение большого количества систем, нарушив работоспособность мобильной сети либо превратив ее в подконтрольную злоумышленнику распределенную сеть.

В настоящий момент вирусологии известно два червя (без учета их модификаций) для мобильных телефонов: Worm.SymbOS.Cabir, размножающийся как по Bluetooth, так и при помощи MMS. При запуске он начинает сканировать окружающее пространство на наличие доступных через Bluetooth устройств, и отсылает им копию самого себя в виде SIS-архива. При этом на экране атакованного телефона, вне зависимости от установленной в нем операционной системы, появляется уведомление о входящем файле и запрос на его загрузку. Далее, если пользователь Symbian-телефона отвечает на запрос положительно, файл сохраняется в память и автоматически запускается на исполнение. Пользователям Windows Mobile-телефонов, загрузившим файл червя, ничто не угрожает. Ничто не угрожает и владельцам автомобилей с бортовыми компьютерами на базе ОС Symbian.

Червь Worm.SymbOS.Comwar, помимо технологии Bluetooth, использует для самораспространения технологию MMS. Для этого он рассылает по номерам телефонов адресной книги MMS-сообщения с вложенной копией своего инсталляционного файла. В процедуре рассылки зараженных сообщений запрограммирована задержка по времени.

В настоящий момент существует несколько программных решений для защиты мобильных устройств от вирусов. В «Лаборатории Касперского» разработаны версии антивируса для Windows CE (Pocket PC, Windows

Mobile), Symbian (6, 7, 8 версий и UIQ), а также для Palm OS. Подобные продукты предлагаются как известными производителями PC-антивирусов (TrendMicro, Network Associates, F-Secure), так и молодыми компаниями, специализирующимися непосредственно на разработке мобильных антивирусных решений (Airscanner, Simworks).

В случае с MMS-червями для мобильных телефонов оптимальной представляется защита на стороне оператора, при которой весь MMS-трафик проходит через интернет-сервер с установленным на нем антивирусным продуктом.

Список лителатуры:

1. Шевченко А. Появление и развитие вирусов для мобильных устройств [Электронный ресурс]: (с изм. и доп.)–Режим доступа:http://www.securelist.com/ru/analysis?pubid=170531631 (дата обращения 20.10.2012)

2. Про вирусы мобильных телефонов. [Электронный ресурс]: (с изм. и доп.)–Режим доступа: http://forum.zelek.ru/t6695-pro-virusi-mobilnih-telefonov.html (дата обращения 20.10.2012)

3. Сысойкина М. Мир ПК[Электронный ресурс]: (с изм. и доп.)–Режим доступа:http://www.osp.ru/pcworld/2011/07/13009499/ (дата обращения 20.10.2012)