

телеком

Заразный мобильный

вирусы

Образованная публика давно научилась отличать безобидные вложения в письма от зловредных программ. Тем не менее, телефоны, не менее лакомый кусочек для вирусописателей, все еще не имеют антивирусной защиты. Насколько масштабна проблема вирусов для телефонов и сколько денег можно потерять на этом, разбиралась **Светлана Ханинаева**.

Ретроспектива заразы

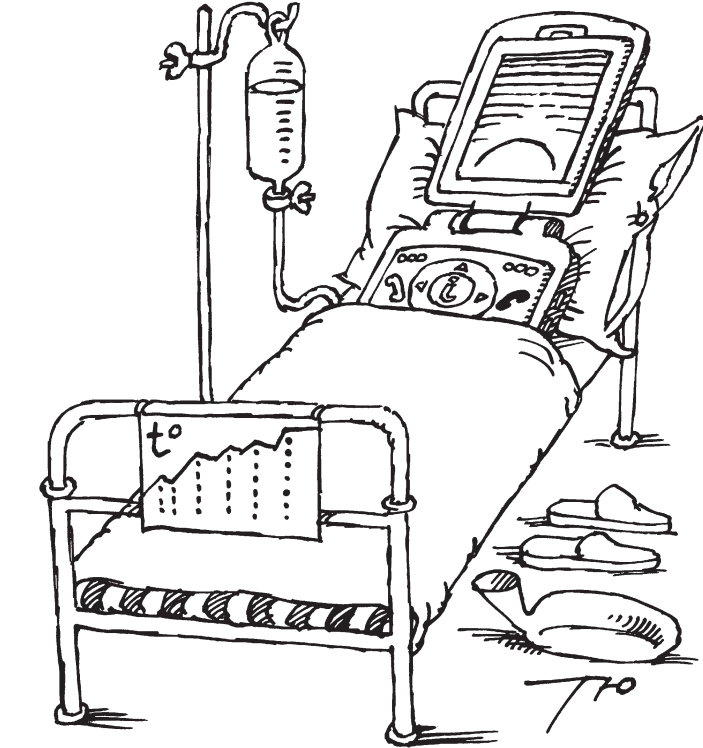
Прежде чем разбираться в многообразии вирусов для мобильных телефонов, стоит вспомнить, что мы знаем о вирусах вообще. Итак, пятница, 13 ноября 1987 года. Один из первых компьютерных вирусов Jerusalem, родом, как следует из названия, из Израиля, вызывает первую в истории крупную эпидемию, окончившуюся печальными последствиями для пользователей: от стирания всех запускаемых в тот день программ до замедления работы компьютера в пять раз. Строго говоря, компьютерные вирусы были известны еще ранее — с 70-х годов прошлого века, но вирусы в том виде, какими мы привыкли их видеть — с вредоносным функционалом, — появились именно в 80-х. Однако существенный перелом в вирусной среде произошел не так давно: около шести-восьми лет назад появились вирусы, предназначенные для заработка денег злоумышленниками. Поскольку в интернете появились деньги (например, оплата услуг или товаров кредитными картами через интернет) и информация, за которую можно получить деньги (данные о пользователях, конфиденциальная информация), вирусописатели сочли нужным использовать новые возможности не только для блатовства, но и для заработка. На место одиноких вирусописателей пришли сплоченные банды, на место ко-

печной прибыли — тысячи долларов за рассылки нежелательных почтовых отправлений (спама) и миллионы долларов, украденные со счетов пользователей. Монетизация интернета продолжалась, а вместе с ней увеличивалось и число вирусов, и нечестный заработок злоумышленников. Некоммерческие вирусы окончательно ушли в прошлое в конце 2007 года, и сейчас вирус — это вредоносная программа, направленная главным образом на получение прибыли.

То, что происходит в одной из сфер высоких технологий, неизбежно затронет и соседние. Это правило применимо и к вредоносным программам: взять хотя бы соотношение вирусов для операционной системы Windows и других систем — большинство зловредов функционируют именно на тех платформах, которые наиболее распространены. Между тем менее популярные платформы также не остаются без внимания злоумышленников: если есть возможность каким-то образом заработать деньги, ее, как правило, используют. Следующая цель вирусописателей — мобильные телефоны.

История повторяется

Как мы помним, вирусы для компьютеров прошли путь от программ, созданных для забавы, до коммерческих зловредов, служащих инструментом



для заработка денег для своих владельцев. В мобильной среде ситуация очень похожа — с той только разницей, что вместо сорока лет истории мобильные вирусы насчитывают всего несколько лет существования. 2004 год, 14 июня. В «Лаборатории Касперского» по электронной почте приходит письмо от известного коллекционера вирусов. Письмо содержит файл с непонятным расширением; при анализе файла становится понятно — это приложение для мобильных телефонов, способное размножаться самостоятельно и рассылать себя владельцам других мобильных телефонов по протоколу Bluetooth. Так, в России был зарегистрирован первый в истории человечества мобильный вирус. Строго говоря, не имеющий вредоносной функциональности, созданный скорее как подтверждение того, что на мобильных платформах могут существовать саморазмножающиеся программы, вирус Cabir тем не менее служил предвестником будущих мобильных эпидемий. Спустя всего месяц после обнаружения Cabir червь вырвался на свободу и тут же устроил эпидемию на Филиппинах. Менее чем через год во время чемпионата мира по лег-

ных телефонов по протоколу Bluetooth. Так, в России был зарегистрирован первый в истории человечества мобильный вирус. Строго говоря, не имеющий вредоносной функциональности, созданный скорее как подтверждение того, что на мобильных платформах могут существовать саморазмножающиеся программы, вирус Cabir тем не менее служил предвестником будущих мобильных эпидемий. Спустя всего месяц после обнаружения Cabir червь вырвался на свободу и тут же устроил эпидемию на Филиппинах. Менее чем через год во время чемпионата мира по лег-

МНЕНИЕ ЭКСПЕРТА

Александр Гостев,

ведущий вирусный аналитик «Лаборатории Касперского»:

«Современное положение дел в области мобильной вирусологии мы расцениваем как затишье перед бурей. С точки зрения технологий, возможностей мобильных вирусов и сред их обитания практически все уже реализовано вирусописателями в той или иной мере. Все популярные мобильные платформы уязвимы для вирусной атаки. Спектр поведения и функционал известных червей, троянцев и вирусов в полной мере повторяет то, что существует в мире компьютерных вирусов. Пока авторы мобильных вирусов занимаются созданием незначительного потока несложных троянских программ. Определяющим фактором развития мобильных вирусов на ближайшее время останется исключительно доля смартфонов на рынке и возможность нелегального зарабатывания денег при помощи зараженных телефонов».

кой атлетике в Финляндии червь распространился среди тысяч человек со всего мира: организаторам даже пришлось установить специальный пункт для очистки телефонов и смартфонов от мобильного зловреда.

От альтруизма к капитализму

Сейчас вирусных программ для мобильных телефонов и смартфонов насчитываются уже десятки. Тем не менее, до полной и окончательной смерти некоммерческих вирусов еще далеко.

Взять хотя бы Comwar — червь, который появился вскоре после начала функционирования Cabir. В арсенале зловреда: возможность распространения как через Bluetooth, так и через MMS, что делает его весьма опасным — в первую очередь для кошелька пользователя. Ущерб легко подсчитать: стоимость MMS — несколько десятков центов, номеров в телефонной книжке редко насчитывается менее ста. А если номеров больше? А если абонент находится в роуминге, где отсылка MMS уже стоит несколько долларов? Все эти вопросы совершенно не волновали создателя червя, который, как и Cabir, распространяется даже в московском метро, а значит, при отсутствии должной защиты способен в мгновение опустошить кошелек владельца телефона. Стоит отметить, что червь, хотя и наносит ущерб денежным средствам, не приносит прибыли вирусописателю.

Откуда же злоумышленники черпают свои доходы? Источники денежных средств — это, в первую очередь, баланс на счете мобильного телефона. Существуют сервисы, предоставляющие мобильный контент — картинки, рингтоны и прочие услуги — за определенную плату, которая списывается со счета пользователя. Этой возможностью не преминули воспользоваться злоумышленники. Провайдеры платного мобильного контента обычно приобретают прямой четырехзначный

номер у поставщиков услуг сотовой связи. Такая услуга достаточно дорога, и некоторые провайдеры сдают номер с префиксом в субаренду: SMS, отправленная на тот или иной номер, должна содержать в начале буквы или цифры, позволяющие идентифицировать того или иного субарендатора. Схема такова: на номер XXXX направляется SMS-сообщение, начинающееся, например, с «S1». Стоимость такой SMS может быть любой. Мобильный оператор забирет себе чуть менее 50 процентов дохода, 10% получает провайдер услуги, а остальное достается субарендатору. Вскоре после появления Comwar, например, в России активизировался вирус Redbrowser, маскировавшийся под экономичный мобильный браузер интернета. Разрекламированный как программное обеспечение, позволяющее пользоваться сетью с мобильного телефона за сущие копейки, троянец, поселившись в устройстве, методично отправлял SMS на подобный субарендованный номер. Стоимость SMS составляла около \$5. Удивительно, но факт: вирус нанес ощутимый ущерб тысячам пользователей, не имея функционала размножения. Пострадавшие сами скачивали и устанавливали программу. И если в случае с компьютерами всем уже давно известно, что бесплатного интернета не бывает, то сфера мобильных угроз до сих пор остается неизвестной, порождая заражения излишне доверчивых пользователей.

Системный подход

Все приведенные выше примеры, безусловно, отнесли к операционной системе Symbian OS, наиболее распространенной на мобильных телефонах. Здесь действует тот же закон, что и в сфере компьютерных вирусов: чем более популярна та или иная операционная система, тем больше внимания обращают на нее вирусописатели. Это не означает, что угрозы для других систем нет. К примеру,

недавно обнаруженный китайский троянец InfoJack не только воровал информацию у пользователей смартфонов на базе Windows Mobile — смартфон, по сути, становился оружием злоумышленника, поскольку вирус отключал защиту от запуска и позволял загрузку любых файлов. Надо сказать, что InfoJack также не мог распространяться сам по себе, попадая на телефоны пользователей в составе с виду безобидных мобильных дистрибутивов.

Популярный сейчас iPhone также уже стал мишенью для вирусописателей. Справедливости ради стоит отметить, что троянская программа, пока единственная из известных для этой платформы вирусов, была написана одиннадцатилетним ребенком и могла заражать только iPhone, прошедшие процедуру «разлочки» — нелегального снятия привязки к сотовому оператору. Тем не менее, это означает, что раз возможность создания вирусов существует, значит, найдутся и злоумышленники, которые пожелают ею воспользоваться.

Пользователи платформы J2ME, установленной сейчас на подавляющем большинстве обычных мобильных телефонов, казалось бы, могут вздохнуть спокойно. Но на самом деле это не так: троянских программ, существующих для заработка денег вышеописанным способом, и для этой платформы существует достаточно. По самым скромным подсчетам, такая программа за два-три дня может принести вирусописателю около \$500.

Зловредные советы

Чтобы понять, насколько существование мобильных вирусов реально, и насколько правдивы страшилки антивирусных компаний, стоит всего лишь проехать в московском метро с включенным в режиме «видимости для всех» Bluetooth. Почти со стопроцентной вероятностью телефон попытается принять какой-нибудь подозрительный

файл. В местах скопления людей — аэропортах, кафе, торговых центрах — мобильные вирусы гуляют туда-сюда, заражая все устройства в зоне действия Bluetooth. В MMS-трафике операторов связи число зараженных MMS исчисляется тысячами. Вышеупомянутый Comwar, к слову, весной прошлого года устроил масштабную эпидемию в Валенсии, заразив 115 тыс. пользователей мобильных телефонов. Ущерб от нашествия червя оценен в €10 млн.

Проблема мобильных вирусов кроется прежде всего в самих пользователях, считает ведущий вирусный аналитик «Лаборатории Касперского» Александр Гостев. Недостаток образования в сфере мобильных угроз чреват излишней доверчивостью пользователей, которые загружают на свои телефоны всевозможный контент, отследить потенциальную опасность которого практически не представляется возможным. Безусловно, это означает, что пользователям следует быть предельно осторожными: не держать Bluetooth постоянно включенным, не принимать файлы и MMS из неизвестных источников, не загружать сомнительные программы из интернета. Защищаться следует и провайдерам сотовой связи: антивирусные средства для защиты от вредоносного мобильного контента существуют не только для конечных пользователей, но и для операторов.

Тем не менее, остановить угрозу по силам и производителям программного обеспечения для телефонов: путь, который избрали разработчики Symbian OS и Apple, например, подразумевает загрузку программ только из официальных источников и запуск только проверенных приложений. Такой путь хорош, если не брать во внимание главное «слабое звено» любой системы — человека, который, как показывает практика, даже многократно обжегшись, все равно предпочитает риск вместо безопасности.



B2B | НАДЕЖНАЯ СВЯЗЬ С БИЗНЕСОМ

Комплексные решения для вашего бизнеса: телефония, доступ в Интернет, организация Виртуальных Частных Сетей, услуги Интеллектуальной Сети Связи. Мы используем проверенные технологии и собственную магистральную цифровую сеть, именно поэтому контролируем процесс и отвечаем за результат.

ОАО «Ростелеком» предлагает корпоративным клиентам комплекс современных телекоммуникационных услуг:

Доступ в Интернет

Качественный высокоскоростной доступ в Интернет от провайдера первого (магистрального) уровня.

Виртуальная Частная Сеть (IP VPN)

Построение защищенной корпоративной IP-сети клиента на базе технологии MPLS с обеспечением одновременной передачи голоса, данных и видео.

«Бесплатный вызов» по кодам 8-800-100 и 8-800-200

Поддержка прямых продаж, рекламных и маркетинговых акций; организация справочно-информационных служб и «горячих линий» на всей территории РФ или в отдельных регионах.

Дополнительная информация – по телефону 8-800-200-00-33

www.rt.ru