«Доктор Веб»: *катехизис* мобильного мифотворчества

Сергей Петров

Старая сисадминская шутка о вирусе для Linux, над компиляцией которого надо еще хорошенько потрудиться, чтобы запустить его в системе с выставленными вручную правами root, сегодня уже не так актуальна. Операционная система Android основана на ядре Linux — однако это не значит, что она по умолчанию избавлена от информационных угроз, которые давным-давно одолевают компьютеры под управлением Windows. Однако большинство владельцев Android-устройств до сих пор уверены в том, что никакой особой защиты от вредоносного кода их мобильным терминалам не требуется. Мифов существует множество.

Кто виноват?

Миф 1. Да кому вообще придет в голову писать вирусы для мобильных платформ?

Давно прошли времена, когда скучающие программисты писали для собственного развлечения занятные программки, которые переворачивали вверх ногами буквы на синих панельках Norton Commander или без особого вреда копировали сами себя на все доступные компьютеры в локальной сети.

Нынешние создатели вредоносного кода работают на крупные преступные синдикаты. Игра стоит свеч, за прошлый год в мире был продан приблизительно миллиард смартфонов — только смартфонов, без учета планшетов, гибридных устройств и прочих разновидностей мобильных терминалов. При этом нынешние смартфоны и планшеты — фактически натуральные, полноценные компьютерные системы. И даже бюджетной модели достаточно, чтобы устройство внесло свой вклад в работу какого-либо ботнета или криминальной «партнерки». К тому же получение несанкционированного доступа гаджету означает, что злоумышленник будет иметь возможность использовать себе во благо информацию, связанную с этой учетной записью, от данных банковской карты до содержимого облачных хранилищ. Так что нет ни единой причины, по которой смартфоны и планшеты не могли бы стать мишенью для вредоносного ПО — и они ею, увы, становятся все чаще.

Миф 2. Умному и осторожному пользователю антивирус не нужен!

Умному пользователю в первую очередь стоит иметь в виду, что нынешние зловреды проникают самыми разными

Dr.Web для Android: возможности и технологии

Одно из наиболее интересных технологических решений «Доктор Веб» — подсистема Origins Tracing for Android. С ее помощью обеспечивается высокий уровень защиты, а также сокращение размеров вирусной базы (для гаджетов это принципиально важный вопрос).

Технически Origins Tracing можно отнести к системам поведенческого контроля — правда, с некоторыми оговорками. Дело в том, что в активном режиме используется не только контроль доступа к определенным ресурсам или перехват системных функций, отслеживание серий вызовов API, свойственных зловредному ПО, либо проверка характерных для вирусов сигнатур.

В отличие от поведенческого анализатора, работающего параллельно с запущенной программой и отслеживающего ее действия, Origins Tracing смотрит «в будущее», изучая программу еще до ее запуска. Это не отдельный модуль, как большинство систем эвристического контроля, а часть антивирусного ядра. Средствами Origins Tracing на ходу строится своего рода модель программы, основанная на декомпиляции ее байт-кода. Затем эта модель сравнивается с БД, содержащей не просто сигнатуры, а универсальные «поведенческие портреты», отражающие особенности функционирования прикладной программы.

В результате удается блокировать не единичного представителя очередной серии зловредов, а целое семейство, сводя на нет усилия авторов вредоносного ПО, создающих изощренные методы маскировки своих детищ.

Технология Origins Tracing применяется и в продуктах для настольных ПК, и в мобильных антивирусах. В частности, благодаря ей антивирусы компании справляются с «троянцами» семейства Android.SmsSend. Это очень разнообразный отряд программ-вымогателей, норовящих заставить пользователя отправить платное SMS за установку бесплатных приложений, таких, например, как браузер Opera Mini. Вариаций существует много (ибо пользователи наивны, а хакеры активны), но, после того как основная модификация данного «трояна» попала в базы Origins Tracing, антивирус обеспечивает надежную защиту. Как бы ни пытались вирусописатели изменить исходный код своего творения, антивирусное ПО благополучно выявляет зловредов, причем в автоматическом режиме. Перестановка байтов сути вредоносной программы не меняет — и именно этот факт выявляется средствами трассировки.

«Троян» Android.Spy.40.origin запрашивает доступ к функциям администратора мобильного устройства, затем скрытно подключается к серверу управления (и «развлекается», перехватывая SMS,

путями. Достаточно простого посещения надежного вроде бы сайта... И через внешний баннер загружается небольшой сценарий на JavaScript, проникает через уязвимость в браузере, заражает систему, начинает свою скрытую работу.

По данным, приводимым специалистами «Доктор Веб», за прошлый год количество зафиксированных (и частью обезвреженных) вредоносных программ для Windows увеличилось на 80% по сравнению с 2012 г. — это при 10%-ном сокращении рынка традиционных ПК. Рост же аналогичных угроз для Android оценивается ни много ни мало в 800%.

Безусловно, умный пользователь в состоянии, потратив на это определенное время, отслеживать все возникающие в мобильном мире угрозы. Однако в таком случае ни на что иное, включая еду и сон, времени у него и не останется. Не лучше ли доверить заботу о безопасности мобильных терминалов профессионалам, для которых это основной род деятельности?

Миф 3. Даже если каким-то чудом «зловреду» удастся пробраться на смартфон, самые важные онлайновые сервисы не будут скомпрометированы: ведь они полагаются на сверхнадежную двухфакторную аутентификацию!

Действительно, если для входа в учетную запись или для совершения платежа онлайн требуется указать не только пароль, но и код, присылаемый по SMS, такая система представляется более надежной, чем при использовании только пароля. Но именно что «представляется» — до тех пор, пока на смартфоне не завелся вредоносный код с соответствующей специализацией.

Наглядный пример: Android.SmsSpy, перехватчик SMS от служб двухфакторной идентификации. Сообщения с кодами моментально и тихо переправляются злоумышленникам. О службах, использующих для верификации пользователя электронные письма, и вовсе говорить нечего: если сам смартфон скомпрометирован, тем более его владелец уже не единолично контролирует свою учетную запись Google.

Миф 4. Я покупаю только «рутованные» мобильные терминалы и, следовательно, полностью контролирую их!

Одна из опасностей, которые грозят владельцам «рутованных» аппаратов, — мобильные буткиты. В 2013 г., по данным компании «Доктор Веб», по всему миру более 350 тыс. мобильных терминалов оказались инфицированы буткитом Android.Oldboot.1, — одним из первых, но не единственным представителем своего класса.

«Рутованный» смартфон предоставляет широкий спектр возможностей не только его счастливому обладателю, но и создателям буткитов, которые норовят внедриться на самый нижний уровень исполняемого в системе кода.

Миф 5. Я инсталлирую все обновления, покупаю/загружаю приложения только в Google Play — и потому риск подхватить вредоносное ПО для меня равен нулю!

В последние годы ситуация с безопасностью ПО, доступного через централизованный магазин Google, улучшилась. В первое время его существования не редкостью были вирусы, кейлоггеры и прочие небезопасные программы под видом каких-нибудь игр, словарей, медиаплееров и прочих невинных на первый взгляд приложений. По данным компании «Доктор Веб», в 2013 г. лишь малая часть вредоносного ПО для Android распространялась по миру

отсылая хакерам списки контактов, устанавливая другие программные модули, отсылая SMS с заданным текстом). Одна из основных особенностей этой заразы — использование уязвимости, позволяющей ей скрываться от многих антивирусов. Однако и этот шпион будет обнаружен по особенностям поведения, получив метку «.origin» (потом, когда специалисты компании занесут его в БД, новая его модификация обретет собственный номер, но защита будет обеспечена, что называется, «здесь и сейчас»).

Более того, антивирус справляется и с буткитами, такими как Android.Oldboot.1, которые загружаются на ранней стадии старта ОС (и далее функционируют как системная служба, открывая хакерам широкий доступ к гаджету).

Антивирусные программы «Доктор Веб» для мобильных устройств в целом спроектированы с учетом ограниченного энергетического ресурса мобильного терминала, и Origins Tracing тут не исключение. Такое своеобразное переосмысление известного механизма эвристического анализа сделано с учетом требований по энерго- и ресурсоэффективности: ни сколько-нибудь существенной нагрузки на процессор, ни чрезмерного расходования аккумулятора при активации этой функции не наблюдается.

Вполне традиционно для антивирусного решения, DrWeb для Android предусматривает быстрое или полное сканирование файловой системы, а также проверку сканером отдельных файлов и папок по запросу пользователя.

Файловый монитор SplDer Guard выполняет проверку файловой системы в реальном времени при попытке сохранить файлы в память устройства. Особое внимание уделяется сменным носителям (microSD, реже SD и др.). Dr.Web для Android Light предусматривает защиту карты памяти от инфицирования файлами автозапуска и Exploit.Cpllnk, представляющими опасность для Windows-устройств, а также возможность восстановления файлов, ранее перемещенных в карантин.

Полная версия мобильного ПО безопасности компании «Доктор Веб» включает модуль защиты от спама. Антиспам блокирует нежелательные звонки и SMS, причем не только с заданных вручную номеров, но и с заранее неизвестных. Сообщение блокируется по ключевым словам: названия продуктов либо известных компаний (особенно злоупотребляют SMS-спамом службы такси), просто любимые спамерами термины («виагра», «такси», «автозапчасти» и т. д.), ссылки («перейдите на [адрес сайта, запрещенный в настройках]»). Предусмотрен режим добавления терминов

непосредственно из Google Play, причем в каждом отдельном случае очень непродолжительное время.

Но полной безопасности пока нет, так что определенные возможности для инсталляции шпионского ПО через этот вроде бы сверхнадежный канал все-таки остались. Тем обиднее было бы для любого пользователя оказаться в числе 0,1% «избранных».

Если вы выбираете в онлайновом магазине некую полезную утилиту — например, удобный (в отличие от стандартного для Android) календарь с информативным виджетом планировщика задач на ближайшее время — внимательно присматривайтесь к набору разрешений, на которые эта утилита рассчитывает.

Доступ к системной памяти и данным календаря для стороннего планировщика задач действительно необходим. Однако, если он хочет еще и получать данные GPS, контролировать Web-камеру и микрофон, обладать возможностью отправлять SMS в фоновом режиме, стоит насторожиться. Особенно в случае, если утилита эта бесплатная (даже без встроенного рекламного модуля), была загружена всего только несколькими десятками/сотнями пользователей и демонстрирует сплошь восторженные отзывы.

Необходимо указать на опасность загрузки Android-приложений из лежащих вне онлайнового магазина Google источников. Даже вроде бы вызывающий полное доверие сторонний сайт может быть скомпрометирован, вам могут прислать фишинговую ссылку, побуждая тем самым загрузить вредоносный код вместо полезной утилиты.

Более того, известны такие вирусные программы для x86-платформы, как Trojan.Droidpak. Они не наносят вреда Windows и пользовательским данным (и потому некоторыми антивирусами даже не распознаются как угроза), зато содержат код для заражения Android-устройств, подключаемых к данному ПК по WiFi, — например, фишинговые клиенты для доступа к онлайновым банковским системам.

Что делать?

Аппаратные возможности сегодняшних смартфонов и планшетов весьма внушительны, так что нет смысла пытаться сэкономить ресурсы, отключая защитное ПО.

Ответственно отнеситесь к обеспечению мобильной безопасности. Незачем заходить на подозрительные новостные сайты и агрегаторы, Web-код которых вполне может содержать вредоносное ПО. Незачем устанавливать прикладные программы, требующие доступа к самым дальним закоулкам смартфона. Помните, что злоумышленники изобретательны и умеют маскировать свои творения, как это делают, например, авторы Android.SmsBot (предназначен для несанкционированной отправки платных SMS).

Установите систему антивирусной защиты, скажем Dr.Web для Android Light. Это бесплатная версия более мощного антивирусного комплекса «Dr.Web для Android». От коммерческой версии «упрощенная» отличается тем, что несколько отстает по версиям, а также рядом функций. У пользователей пакетов Dr.Web Security Space и «Антивирус Dr.Web» есть возможность получить полную версию мобильного антивируса (см. врезку «DRWeb для Android: возможности и технологии»). Однако даже в «легком» варианте этот антивирусный пакет обеспечивает достаточно высокий уровень защиты от мобильных угроз. PC

Dr.Web для Android: возможности и технологии (окончание)

из журнала звонков либо SMS, который ведется в антивирусной программе. Подсистема фильтрации очень мощная, в ней реализованы весьма тонкие функции. Скажем, с определенного номера можно принимать звонки и не принимать SMS, составить «белый список» (и принимать звонки только от доверенных абонентов), есть функция создания пользовательских профилей и др.

Облачный URL-фильтр Cloud Checker блокирует доступ с гаджета к Web-страницам, содержащим противоправную или иную недопустимую информацию. Система встраивается в наиболее популярные браузеры. Категорий для запрета довольно много, включая «Наркотики», «Известные источники вирусов», «Нецензурная лексика», «Терроризм» и др. Среди них есть и такая, как «Электронная почта», — это предотвращает доступ на внешние почтовые системы, что оценят компании, внедряющие в бизнес-процесс идеологию BYOD.

Им же особенно понравится подсистема предотвращения потери данных в случае кражи устройства «Антивор». Она предусматривает такие радикальные меры, как блокировка телефона после перезагрузки (с требованием ввести пароль, причем число попыток ограниченно), разблокировка с помощью SMS, получение GPS-координат устройства в виде ссылки на Google Maps, возможность дистанционно удалить данные в памяти устройства и на сменной карте памяти, включение на устройстве громкого звукового сигнала и блокировка экрана. Учитываются возможности многоядерных гаджетов. Использование при антивирусной проверке всех имеющихся ядер существенно ускоряет процесс (этот режим требует активации в настройках, по умолчанию он отключен).

Есть сетевой экран, самый настоящий — с фильтрацией трафика, установкой правил доступа к сети. Одним из основных нововведений версии 9.0 для Android стала функция аудита безопасности, давно привычная для настольных версий антивирусных систем и весьма необычная для мобильных. Соответствующий компонент выполняет комплекс проверок, фиксируя уязвимости в ОС и прикладном ПО, приложения, с которыми возможны несовместимости антивируса, и предлагая методы их устранения. Впрочем, следует отметить высокую степень совместимости: в Dr.Web для Android учитываются даже весьма экзотические функции, вроде Samsung Multi Window (обеспечивает одновременную работу двух приложений и обмен информацией между ними).