Визитка

ВЯЧЕСЛАВ МЕДВЕДЕВ,
старший аналитик отдела развития компании «Доктор Веб»

Кому уходят СМС?

Разговоры о том, что Интернет все больше входит в нашу жизнь, наверное, уже давно набили оскомину. Но, хотим мы этого или нет, это реальность

Возможность получения нужной информации, легкость общения, покупки в один клик, управление своими финансами – никто не будет отрицать, что все это не только удобно, но и приятно. Но вот беда: не все, что продается под видом меда, действительно им является. Рост удобства не сопровождается ростом безопасности. Статистика безжалостна: большинство сайтов и приложений так или иначе содержит уязвимости.

Вредоносные программы для платформы Android – это не миф. При этом можно утверждать, что угрозы для мобильных устройств по целому ряду причин гораздо опаснее своих собратьев, созданных для обычных компьютеров.

- Операционные системы для мобильных устройств, создававшиеся изначально исключительно для максимально удобного личного пользования и работы на достаточно слабых аппаратных конфигурациях, не имеют в своем составе развитых средств безопасности – возможности разделения прав доступа к различным объектам, ограничения по установке приложений, иных ограничений из обязательного для безопасности списка родительского контроля.
- Смартфоны (да и многие планшеты) снабжены видеокамерой, микрофоном, средствами позиционирования. Это позволяет злоумышленникам контролировать каждый шаг жертвы и следить за ее личной жизнью – большинство домашних компьютеров не дают таких возможностей для слежки. Более того, опасность может предоставлять даже аккумулятор: еще в 2011 году исследователь Чарли Миллер сообщал о возможности перепрограммирования аккумуляторного микроконтроллера в целях перегрева батареи.
- Как правило, смартфоны подключаются к сети Интернет (а для чего они еще нужны?), не имея даже средств защиты, которые считаются необходимыми для обычных компьютеров, и это тоже не усиливает их безопасность.

Добавим к списку проблем и то, что пользователи устройств, как правило, не являются специалистами по безопасности (а специалисты по безопасности, к сожалению, не представляют себе масштаб проблемы – но это особый разговор) и игнорируют даже элементарные требования безопасности и осторожности при работе с веб-ресурсами, позволяющие избежать серьезных проблем при действиях в Интернете или в процессе обмена данными со своими знакомыми. В итоге мы получаем большой интерес криминальных структур (именно структур, а не только отдельных хакеров) к мобильным устройствам.

Согласно статистике основное внимание вирусописателей направлено на Android – число вредоносных программ для других мобильных ОС исчисляется единицами. В 2013 году количество вредоносных программ для Android увеличилось на 122%. А по сравнению с уровнем распространения мобильных угроз в 2010-м, когда первые вредоносные приложения для Android только появились, рост составил 9280% (см. рис. 1).

На графике можно увидеть любимую всеми составителями отчетов параболу – так что велика вероятность, что в 2014-м количество вредоносных программ увеличится более чем в два раза: период поиска, когда вирусописатели нащупывали возможности для внедрения троянцев в мобильные устройства, давно миновал, и наработки прежних лет сейчас активно используются на практике.

При этом злоумышленники не только воспроизводят старые идеи: идет активный поиск новых путей отъема денег. Число семейств вредоносных программ достигло 331 – за прошедший год их рост составил 185%. Выше мы уже говорили, что мобильные телефоны дают хакерам много возможностей, но большая часть троянцев покушается исключительно на денежные средства – случаи использования вредоносных программ в террористических целях или ради шантажа если и есть, то исчисляются единицами. И самым популярным семейством троянцев является Android.SmsSend (он же Trojan-SMS.AndroidOS в терминологии другого отечественного разработчика антивирусных решений), занявший без малого половину рынка мобильных угроз (см. рис. 2).

Троянцы появившегося еще в 2010 году семейства Android.SmsSend предназначены для скрытой отправки

дорогостоящих СМС-сообщений на короткие номера, рассылки сообщений по адресной книге и подписки пользователей на платные контент-услуги. В отдельных случаях троянцы SmsSend могут проторить дорогу иным угрозам, перенаправляя пользователя на зараженные веб-страницы или внедряя в устройство другие вредоносные программы, в том числе утилиты скрытого удаленного управления. Сейчас в семейство входит 1377 модификаций.

Троянцы могут распространяться как в виде самостоятельных приложений (.apk), например, под видом обновлений (как правило, браузера или флеш-плеера) или инсталляторов известных приложений, так и внутри бесплатных легитимных программ, модифицированных злоумышленниками. После запуска зараженных приложений пользователь получает ожидаемый функционал, поэтому нежелательные действия, такие как отправка СМС-сообщений, обычно остаются незамеченными.

В качестве примера обертки, в которую заворачивались для маскировки Android.SmsSend, можно привести популярные мультимедийные проигрыватели, сборники изображений (в этом случае число загрузок превысило 12 тысяч!), а также приложения для составления диет и гороскопов. При запуске вредоносные приложения предлагали пользователям получить доступ к запрошенному контенту, после чего извлекали скрытых внутри самой программы троянцев и начинали процесс их установки.

На развитие семейства Android.SmsSend (как и иных вредоносных программ) сильно повлияла коммерциализация рынка киберпреступности. Зачастую вредоносные файлы создаются с учетом конкретных интересов злоумышленников – например, они могут собирать данные жителей определенного региона. Так, маскировка под легитимные программы все еще остается наиболее популярным методом на территории Китая, о чем свидетельствует появление в 2013 году целого ряда модификаций троянцев, угрожавших китайским пользователям и, по сообщениям в сети Интернет, попавших и в Россию.

Заметным событием, связанным с троянцами Android.SmsSend в прошлом году, стало обнаружение в сентябре самого крупного за последнее время мобильного ботнета, состоящего из Android-устройств. По оценкам специалистов компании «Доктор Веб», в состав бот-сети входило более 200 тысяч смартфонов и планшетных компьютеров. Для заражения мобильных устройств использовалось сразу несколько СМС-троянцев, которые маскировались под инсталляторы легитимного программного обеспечения, такого как веб-браузеры и клиенты для работы с социальными сетями (см. рис. 3).

Основным предназначением Android.SmsBot является все та же несанкционированная отправка премиум-сообщений в целях получения злоумышленниками незаконного заработка. Однако в данном случае параметры работы троянца не указываются заранее в конфигурационных файлах или в самом коде – SmsBot получает указания к действию непосредственно с принадлежащего киберпреступникам управляющего сайта, что в значительной мере расширяет их возможности. Многие версии троянцев Android.SmsBot способны по команде выполнять и другие действия, например, загрузку прочих вредоносных программ, удаление определенных СМС, сбор и отправку информации о мобильном устройстве на удаленный сервер, совершение звонков. Отдельные модификации могут запрашивать состояние баланса мобильного счета с помощью USSD- или СМС-запросов и в зависимости от результата получать от управляющего сервера указание отправить на номер сообщения определенной стоимости.

Возможность перехвата СМС-сообщений роднит SmsBot с более опасными программами, например, Android.Spy. Такие приложения либо имитируют интерфейс настоящих мобильных банковских клиентов и обманным способом заставляют пользователей предоставить свои персональные данные, либо устанавливаются под видом важных программных обновлений или сертификатов и в дальнейшем позволяют злоумышленникам перехватывать все входящие

Рисунок 1. Динамика роста количества описаний Android-угроз в вирусной базе Dr.Web в период с 2010 по 2013 год

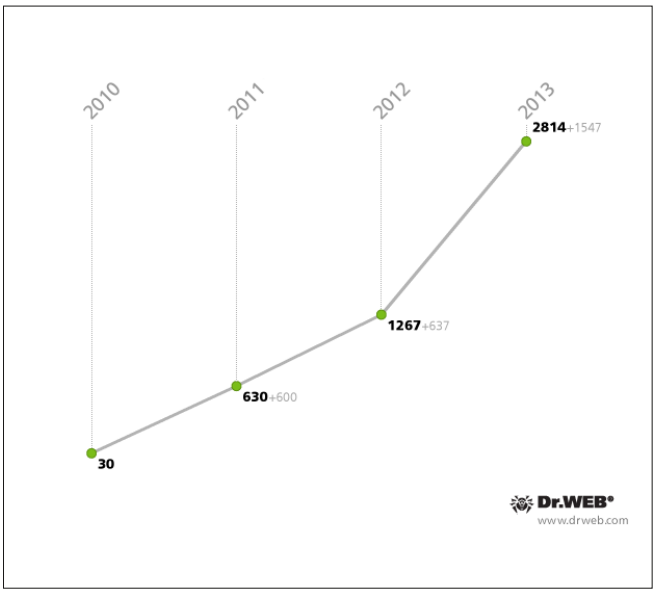
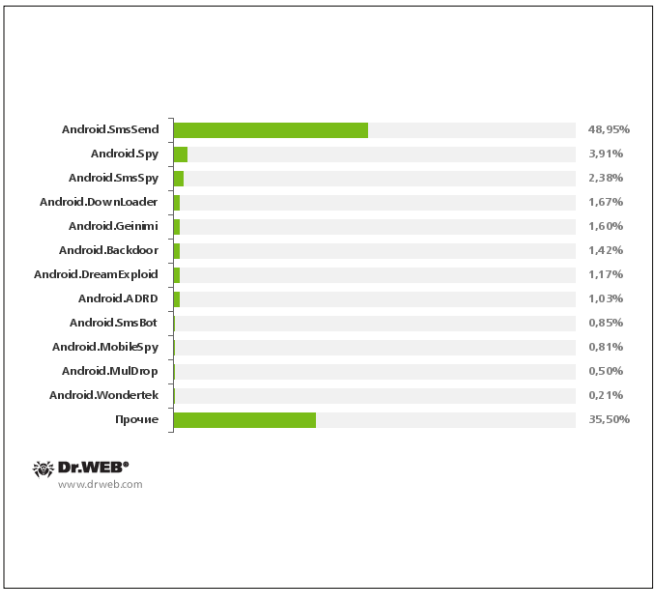


Рисунок 2. Наиболее многочисленные Android-угрозы согласно объему записей вирусной базы компании «Доктор Веб»



СМС-сообщения, в которых может содержаться различная секретная информация, например, одноразовые mTAN-коды систем «Банк-Клиент», что в свою очередь дает возможность сокрытия или модификации СМС-подтверждений о совершении платежа или перевода.

В известных случаях вредоносная программа распространялась по следующей схеме: потенциальная жертва, пытавшаяся воспользоваться услугами банка через веб-браузер на уже зараженной машине, получала уведомление о необходимости авторизации по номеру мобильного телефона, для чего на мобильное устройство предлагалось установить специальное приложение, размещенное в официальном каталоге Google Play. Это приложение представляло собой банковского троянца для мобильной платформы Android.

Мало просто создать вредоносную программу, ее нужно внедрить на мобильное устройство жертвы. В случае с мобильными приложениями еще совсем недавно для этой цели жертве нужно было разлочить устройство, теперь в этом нет необходимости: вредоносные программы проникают и в официальный каталог приложений ОС Android – Google Play. Более того, при этом зачастую даже отсутствует необходимость получения на инфицируемом смартфоне или планшете администраторских привилегий – современным троянцам для успешной работы достаточно стандартных пользовательских прав. Злоумышленники, загрузившие такие приложения в систему Google Play, составляют описания с учетом содержания самых популярных запросов, что облегчает их попадание в результаты выдачи поисковой системы Google Play.

Регистрация аккаунта разработчика обходится киберпреступникам всего в 25 долларов. Эти скромные затраты окупаются с лихвой, поскольку до изъятия программы из Google Play ее успевают скачать десятки тысяч пользователей.

Нужно отметить, что в случае загрузки троянца с Google Play заражение как таковое может и не произойти. После запуска вредоносного приложения пользователю демонстрируется лицензионное соглашение, в конце которого расположена незаметная гиперссылка на правила, где говорится о том, что при согласии с предложенными условиями с устройства будут отосланы СМС на короткие номера и с баланса пользователя будут списаны денежные средства.

Троянец Android.SmsSend мог проникать к жертве с помощью Android.Androways.1.origin, обнаруженного в минувшем апреле. Данный вредоносный модуль был создан злоумышленниками под видом вполне обычной рекламной системы, демонстрирующей разнообразные информационные сообщения и позволяющей создателям игр и приложений зарабатывать на своих программных продуктах, интегрируя в них данный модуль. Как и многие легальные рекламные платформы, Android.Androways.1.origin был способен демонстрировать push-уведомления, выводимые в панель состояния операционной системы, однако в этих сообщениях нередко отображались заведомо ложные предупреждения о необходимости загрузки обновлений для тех или иных программ. Согласившись на загрузку такого «обновления», пользователи подвергались риску стать жертвой мошенников (см. рис. 4).

Общее число пострадавших пользователей могло превысить 5,3 млн человек, что стало одним из крупнейших случаев заражения Android-устройств вредоносными приложениями, которые распространялись с использованием каталога Google Play за все время его существования.

Особо опасным нужно признать распространение троянцев через QR-код, который содержит ссылку, ведущую на вредоносную программу.

Опасность заключается в том, что содержимое QR-кода может быть никак не связано с описанием его назначения – пользователи и не подозревают, что последует за попыткой отсканировать код. Это увеличивает потенциал распространения, так как такой код можно разместить на любом сайте, а содержащаяся в нем ссылка все равно

Рисунок 3. Географическое распределение зараженных устройств по оценкам специалистов компании «Доктор Веб»

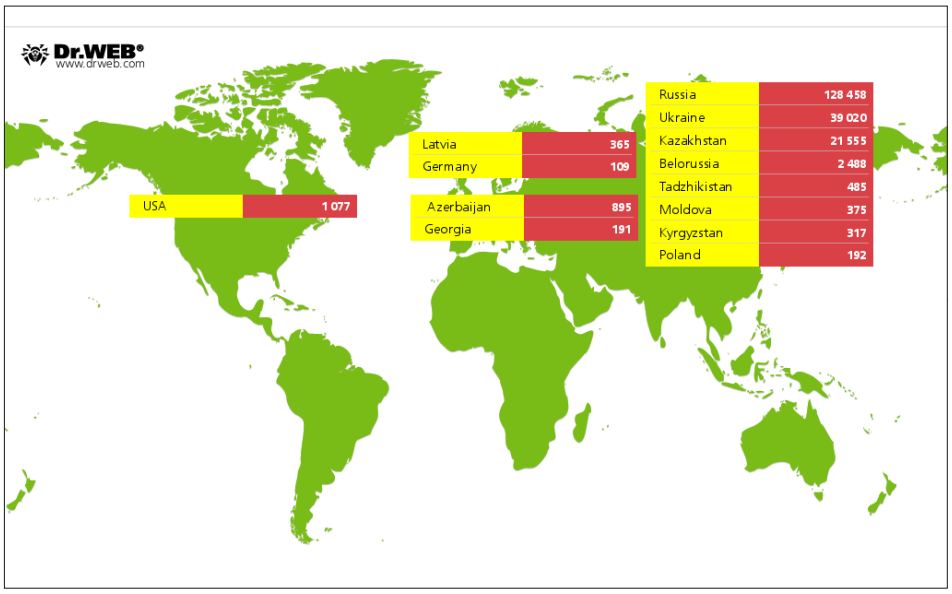
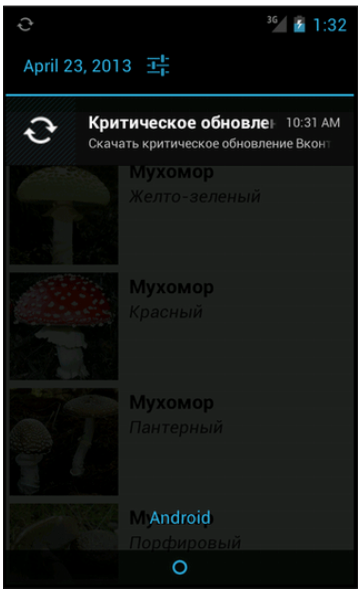


Рисунок 4. Ложное предупреждение, выдаваемое Android.Androways.1.origin



будет вести на вредоносный объект. С использованием данного способа распространялся, например, троянец Android.SmsSend.15.

Если вредоносная программа была установлена без разрешения пользователя, злоумышленникам нужно скрыть ее на инфицируемом устройстве либо максимально усложнить ее удаление. И в 2013 году значительно увеличилось число случаев применения вирусописателями специальных приемов, затрудняющих проведение анализа вредоносных Android-приложений, а также усложняющих процесс их обнаружения и удаления на мобильных устройствах. Техника обфускации может существенно затруднить обнаружение вредоносной программы не только антивирусами, но и системой входного контроля Bouncer, предназначенной для предотвращения попадания таких программ в Google Play.

Одной из наиболее распространенных методик самозащиты в Android-троянцах стало использование стандартной системной функции администратора устройства, когда приложению даются расширенные полномочия, такие как возможность управления блокировкой экрана, запроса пароля при выходе из ждущего режима и даже выполнение сброса параметров к заводским установкам с потерей всех имеющихся данных – при использовании преступниками этой возможности попытка стандартным способом удалить входящую в список администраторов вредоносную программу приводит к ошибке.

И если в общем случае такая ситуация не является проблемой для опытных пользователей (троянца всего лишь необходимо лишить соответствующих полномочий), то большинство обычных владельцев мобильных устройств с этой проблемой справиться не могут.

Но в ряде случаев для того, чтобы обезопасить свое мобильное устройство, простого отключения полномочий администратора может быть недостаточно. Создатели вредоносных приложений идут дальше и вносят в их функционал контроль активности данного режима, и, если пользователь пытается его отключить, троянцы предпринимают попытки не допустить этого. Например, они могут препятствовать открытию системных настроек или выводить запрос на получение нужных прав до тех пор, пока пользователь не согласится это сделать.

Не облегчает жизнь пользователей и наличие ошибок в системе, позволяющих вредоносным программам (например, Android.Obad) скрывать свое присутствие в соответствующих списках, а также распространение на рынке коммерческих систем для защиты Android-приложений от декомпиляции, взлома и модификации (например, обфускации), поскольку подобные механизмы могут быть использованы не только разработчиками легитимных программ, но и злоумышленниками (Android.Spy.67 и Android.Tempur.5.origin).

Семейства Android.SmsSend и Android.SmsBot активно продаются на нелегальном рынке. Их авторы зачастую предлагают своим клиентам не только сами вредоносные приложения, но и сопутствующие им готовые решения в виде удаленных панелей управления, а также программных средств для построения вредоносных сетей и партнерских программ. Цены на данные услуги варьируются от нескольких сотен до нескольких тысяч долларов (см. рис. 5).

А как всему этому безобразию могут противостоять антивирусные программы? К сожалению, на ситуацию с антивирусной защитой сложно смотреть с оптимизмом. Да, количество загрузок самого популярного антивируса – Dr.Web для Android – превысило 30 миллионов. Но если даже среди стационарных компьютеров, необходимость антивирусной защиты которых признается всеми, число незащищенных машин по некоторым оценкам достигает 30%, то что говорить о мобильных устройствах, если большинство пользователей считают мифом существование вредоносных программ для них.

Не облегчает ситуацию и фрагментация рынка мобильных устройств – производители антивирусных средств не могут ориентироваться только на мощные устройства с топовой конфигурацией: необходимо обеспечить защиту всех устройств, в то время как знания обо всех известных вредоносных программах реализуются десятками мегабайт антивирусных баз.

Усугубляет проблему и то, что для мобильных устройств антивирус зачастую является единственным средством защиты, обязанным взять на себя оборону от всех угроз.

Единственным выходом из сложившейся ситуации является опора на продукты, создаваемые на основе инновационных разработок – ПО, сочетающее традиционную устойчивость к воздействию вредоносных программ с применением технологий, открывающих возможность использования компактных вирусных баз. Например, технология Origins Tracing™ for Android позволяет определять новые семейства вирусов или перекомпилированные варианты уже известных семейств на основе базы знаний о предыдущих угрозах и, безусловно, может сделать пользование мобильным телефоном, смартфоном и планшетом гораздо более безопасным. EOF

Рисунок 5. Пример киберкриминальных услуг