Защита мобильных приложений от кибератак

Александр Горячев, *сотрудник вирусной лаборатории, ООО "Доктор Веб"*

Современные мобильные Android-устройства прочно вошли в нашу повседневную жизнь. Они помогают эффективно решать рабочие задачи, предоставляют широкие возможности для поддержания связи с близкими нам людьми, позволяют скоротать минутку-другую во время утомительного ожидания, да и просто-напросто отлично повеселиться на досуге.

Однако, всецело полагаясь на современные технологии, многие пользователи забывают о необходимости соблюдать элементарные правила безопасности и зачастую не принимают во внимание существующие риски, связанные с атаками на их смартфоны и планшеты. А тем временем киберпреступники не дремлют, ведь ваше мобильное устройство – это и кошелек, и ключ к банковскому счету, и доступ к огромному количеству персональной информации, которую при желании можно очень выгодно продать или же использовать в разнообразных мошеннических схемах. Именно поэтому знание основных уловок злоумышленников может помочь избежать неприятных инцидентов и сделать использование любимого девайса более безопасным.

*Фишинг – совокупность приемов, предназначенных для получения доступа к такой секретной информации, как логины и пароли.

Некоторые из банковских троянцев (например, Android.SpyEye, Android.Panda, Android.FakeSber) способны перехватывать проверочные СМС-сообщения, которые автоматически высылаются пользователям для подтверждения выполнения той или иной денежной операции (такой, например, как онлайн-покупка). Вредоносные программы крадут содержащиеся в этих сообщениях коды подтверждения и передают их злоумышленникам для завершения незаконного денежного перевода.

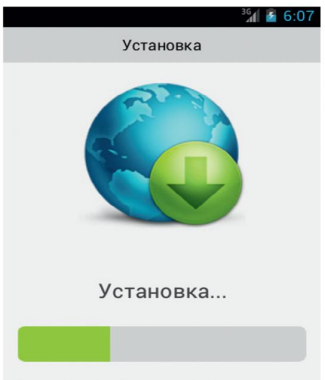

Рис. 1. Отправка дорогостоящих СМС-сообщений

Основные векторы атак

Для осуществления атак на мобильные Android-устройства в арсенале киберпреступников припрятано немало хитроумных методик, однако самыми распространенными среди них остаются фишинг*, а также использование разнообразных вредоносных приложений.

Атаки с использованием фишинга основаны на доверчивости и невнимательности пользователей, и в большинстве случаев они ведутся от имени известных компаний, организаций или даже государственных ведомств. В таких случаях жертве обычно сообщается о взломе или внезапной блокировке одной из ее учетных записей, после чего предлагается выполнить ряд действий по восстановлению доступа к ней.

Примером реализации подобной атаки может служить, например, СМС-сообщение якобы от имени социальной сети, в котором пользователя просят перейти по указанной ссылке для восстановления работоспособности его "заблокированной" персональной страницы. Конечно же, на самом деле никакой блокировки нет, а предоставленная ссылка в действительности ведет на Web-сайт, внешне очень похожий на оригинальный. Запаниковав, жертва непременно попытается вернуть доступ к своей учетной записи, добровольно предоставив мошенникам всю необходимую информацию. Обман, вероятно, вскоре будет раскрыт, однако это будет уже неважно, так как главная цель киберпреступников – получение доступа к учетной записи пользователя – успешно достигнута.

По сравнению с фишингом, применение вредоносных программ дает злоумышленникам еще большую свободу в достижении своих незаконных целей. Рассмотрим наиболее часто встречающиеся типы опасных Android-приложений и совершаемых с их помощью атак.

Отправка дорогостоящих СМС-сообщений

Неавторизованная пользователем отправка платных СМС – один из наиболее старых и распространенных типов незаконной деятельности, совершаемой киберпреступниками на мобильных Android-устройствах при помощи троянских программ, принадлежащих, например, к таким семействам, как Android.SmsSend и Android.SmsBot. Распространяясь под видом безобидных игр и легитимных приложений, эти троянцы тайком выполняют отправку одного или нескольких дорогостоящих коротких сообщений, подписывая абонентский номер на платные контент-услуги. В результате этого с мобильного счета пользователей единовременно или на постоянной основе списывается определенная денежная сумма, часть которой поступает в карман мошенникам (рис. 1).

Кража банковской информации и незаконные денежные операции

Выполнение банковских операций на мобильных устройствах – закономерное развитие современных финансовых услуг. Неудивительно, что практика дистанционного контроля операций и управления счетами в настоящее время находит все большее распространение среди пользователей. Однако, если вы являетесь клиентом подобных сервисов и при этом обладаете Android-устройством, будьте настороже: киберпреступники уже начали охоту за вашими деньгами. Для этого они используют разнообразных банковских троянцев, в той или иной степени отличающихся по функционалу. Например, многие подобные троянцы могут имитировать внешний вид настоящих приложений "Банк-Клиент" кредитных организаций и обманом выуживать у своих жертв аутентификационные данные, необходимые для доступа к управлению счетами (рис. 2).

Кибершпионаж

Помимо кражи банковских сведений злоумышленников может интересовать и другая конфиденциальная информация пользователей Android-устройств. Благодаря успешно проведенной спланированной

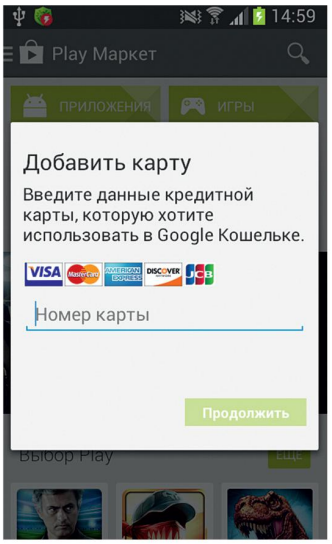

Рис. 2. Кража банковской информации и незаконные денежные операции

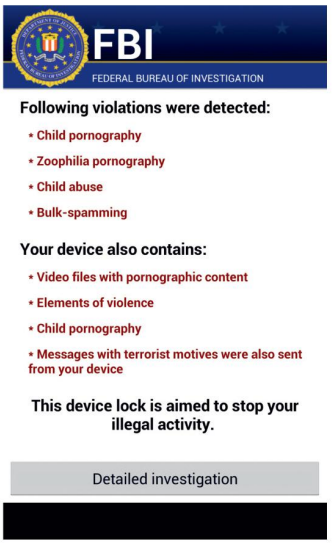

Рис. 3. Блокировка мобильных устройств и требование выкупа

атаке им станет известно очень многое об интересующем их человеке. При этом злоумышленником может выступать не только группа злостных хакеров или секретная правительственная служба с хитроумными троянцами-шпионами, но и ваш коллега, родственник или обычный сосед-"доброжелатель". Всем им в этом помогут полулегальные программы-шпионы, которых на рынке представлено великое множество (Android.MobileSpy, Android.Mobistealth, Android.Flexispy и целый ряд других). Подобные приложения скрытно передают своим хозяевам самые разные сведения о своей цели. Например, информацию об СМС-переписке, совершенных звонках, имеющихся контактах в телефонной книге, обо всех передвижениях (благодаря GPS-приемнику), истории веб-браузера и многом другом. В умелых руках подобная информация может стать весьма ценным предметом.

Блокировка мобильных устройств и требование выкупа

Некогда распространенная лишь среди настольных компьютеров под управлением Windows, блокировка с целью получения выкупа становится все большей проблемой и для пользователей ОС Android. Начавшие появляться на рубеже весны и лета 2014 г., троянцы-вымогатели семейства Android.Locker ознаменовали появление очередной серьезной угрозы для владельцев мобильных устройств. Подобные троянцы (рис. 3) опасны тем, что, попадая на целевое устройство, блокируют его и требуют за разблокировку крупную сумму денег. При этом самостоятельная разблокировка может оказаться весьма затруднительной или же вовсе невозможной, т.к. подобные троянцы препятствуют нормальной работе с зараженным устройством и не дают выполнить на нем никаких привычных действий, включая отправку сообщений, совершение звонков и т.п.

Более того, существуют троянцы-вымогатели, которые помимо "простой" блокировки вдобавок зашифровывают важные для пользователей файлы, такие как фотографии, видео, музыку, документы и архивы. Такие случаи особенно опасны, так как нет никакой гарантии, что эти файлы удастся когда-либо успешно восстановить даже в случае оплаты выкупа.

Все это – лишь часть угроз, которые могут подстерегать владельцев Android-устройств. Число вредоносных программ для этой мобильной операционной системы постоянно растет, при этом функционал многих их них со временем становится все более изощренным. Для обеспечения хотя бы минимального уровня безопасности нужно всегда быть начеку, проявлять внимательность и осторожность, ведь первая линия обороны – это собственные знания и здравый смысл.