УДК 004.056

И.С. Гришко

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ НА ПЛАТФОРМЕ ANDROID

В данной статье проведен обзор состояния безопасности мобильных устройств на платформе Android. Рассмотрены основные угрозы безопасности мобильных устройств. Описано направление развития обеспечения безопасности на платформе Android.

Ключевые слова: *безопасность, Android, вредносные приложения, вирусы, интернет-преступность.*

Согласно данным «Лаборатории Касперского» количество вредоносных приложений для мобильных устройств, функционирующих на операционной системе Android насчитывает более 10 млн. [1] Механизм распространения вирусных программ имеет характер, схожий с распространением инфекций: часто, получив права доступа, вредоносная программа инициирует отправку сообщений на номера абонентов из контакт-листа устройства с ссылкой на скачивание архива APK вируса. Ситуацию осложняет маскировка вирусов под известные приложения или распространение их в официальных магазинах приложений, таких как Google Market.

Мобильные устройства могут быть использованы злоумышленниками при DDoS-атаках на различные интернет- ресурсы. Появившийся в 2012 году троян Android.DDoS.1.origin отправлял сетевые пакеты на указанный адрес по команде злоумышленника. Распространение данного вируса происходило вместе с легитимными приложениями, но те в свою очередь распространялись на неофициальных источниках.

Одним из самых известных вредоносных программ для операционной системы Android является семейство Android.SmsSend. [2] Принцип работы троянов этого семейства следующий: троян инициирует отправку платных SMS-сообщений на короткие номера, может подписывать абонента на платные услуги, в итоге счет абонента опустошается, в связи с чем стоит задуматься об услугах автопополнения с банковского счета. Данное семейство троянов часто маскируется мошенниками под видом известных программ, например, известного интернет-браузера или игры. Пользователь часто скачивает троян, не удостоверившись в безопасности устанавливаемого файла. Так же мошенники используют знание психологии: в том случае, когда вирусное ПО само не может получить root-прав от устройства, оно явно запрашивает от пользователей подтвердить установку, которые в свою очередь не задумываются об опасности и подтверждает установку трояна. Скорее всего при установке вредоносного ПО в соглашении будет написано, что программа будет отправлять платные SMS, но пользователь предпочтет согласиться сразу.

Даже если на мобильном устройстве установлен антивирус, он не всегда сможет распознать в программе дроппера, содержащего опасность. В приложениях Android вирусы могут быть обфусцированы в архивах.apk, но это самый простой вариант. Более сложные механизмы используют шифрование файлов вирусного ПО. Старший аналитик из Malwarebytes Натан Колье опубликовал в блоге описание вредоноса, получившего название Trojan.Dropper.RealShell. [3] По словам Колье, вредонос хранит свои файлы в папках “res” и “Assets” внутри APK. В отличии от обычных дропперов, которые скрывают свое присутствие в APK, обновленная версия вредоноса использует необычную технику компиляции библиотек путем соединения нескольких файлов в один. Такой подход усложняет обнаружение вредоноса на системе и усложняет его поиск по сигнатурам. Внутри APK файлы вредоноса выглядят как временные или ненужные файлы, и только после компиляции всего приложения можно определить, что именно из этих файлов и состоит сам дроппер. Аналитики Malwarebytes ожидают рост количества атак с использованием обфусцированных APK взамен существующей практики принудительной установки нежелательного ПО на систему. Практика обфусцирования APK не является новой, однако методы и приемы злоумышленников становятся более сложными, что говорит о повышении интереса вирусописателей к мобильным платформам.

Для защиты информации на мобильных устройствах необходимо использовать шифрование носителей информации. Максимально обезопасить свои данные на устройствах под управлением ОС Android позволяет полное шифрование диска. Шифрование данных было добавлено в Android 3.0 Honeycomb, данная версия Android была ориентирована для планшетов. [4] Впервые для владельцев смартфонов возможность шифрования появилась в версии 4.0.

Полное шифрование диска защищает конфиденциальные данные в случае потери устройства, кражи или конфискации по какой-либо причине. Для сотрудников спецслужб получение данных на зашифрованных устройствах весьма затруднено и зависит от ряда условий. Если устройство выключили во время транспортировки или же просто разрядилась батарея, то процесс получения данных осложняется. Дело в том, что полное шифрование уязвимо для атаки "холодная загрузка" (cold-boot), с помощью которой методом физической заморозки устройства возможно считать информацию из оперативной памяти. Это достигается благодаря тому, что оперативная память при потере питания очищается в течение определённого количества времени, а при заморозке процесс очищения замедляется и может продолжаться от нескольких секунд до нескольких минут. Из оперативной памяти устройств на базе Android можно извлечь ключи AES, но расшифровка диска возможна только при разблокированном загрузчике.

28 мая 2015 года Google представила на конференции Google I/O 2015 новую версию Android Marshmallow, отличающуюся от предыдущих наличием возможности пользователю самому устанавливать, какие приложения к чему будут иметь доступ. Так же новая версия Android поддерживает сканер отпечатков пальцев на нативном уровне. [5]

На сегодняшний день обеспечение безопасности – один из направляющих векторов совершенствования платформы Android. Происходит борьба между злоумышленниками и разработчиками, в которой немалую роль играет и пользователь: в значительной степени можно обезопасить свое устройство, если не устанавливать программы из подозрительных источников, интересоваться событиями информационных технологий и вовремя обновлять операционную систему и не пользоваться непроверенными общественными сетями выхода в Интернет, по желанию можно настроить свое устройство на использование VPN.

Библиографический список

1. Сайт компании АО «Лаборатория Касперского» / Инфографика о вирусах на Android. URL: http: // www.kaspersky.ru/internet-security-center/infographics/android-threats

2. Сайт ООО «Доктор Веб» / Android.SmsSend.566.origin.URL: http: // vms.drweb.ru/virus/?i=4182469

3. Official security blog Malwarebytes UNPACKED / Complex Method of Obfuscation Found in Dropper RealShell.URL: https: // blog.malwarebytes.org/mobile-2/2015/06/complex-method-of-obfuscation-found-in-dropper-realshell/

4. Сайт для android-разработчиков Developers / HoneyComb. URL: http: // developer.android.com/intl/ru/about/versions/android-3.0-highlights.html

5. Сайт конференции Google I/O 2015.URL: https: // events.google.com/io2015/

ГРИШКО ИВАН СЕРГЕЕВИЧ – магистрант, Северный (Арктический) федеральный университет имени М.В. Ломоносова, Россия.