Dr.WEB®
с 1992 года

Обзор вирусной активности для мобильных Android-устройств в марте 2016 года

Обзор вирусной активности для мобильных Android-устройств в марте 2016 года

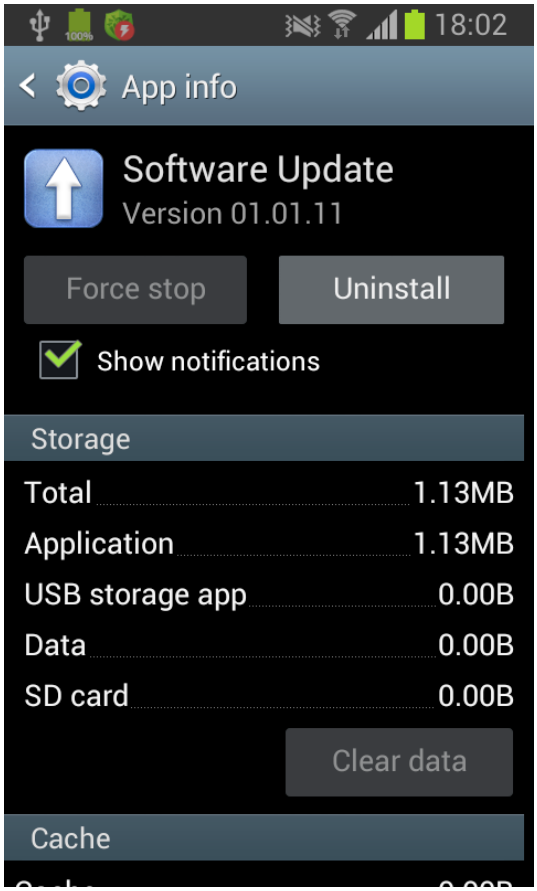
31 марта 2016 года

Главные тенденции марта

- Обнаружение рекламного Android-троянца, проникшего в популярные приложения и прошивку нескольких десятков моделей мобильных устройств
- Завершение исследования опасного троянца, внедряющегося в важный системный процесс ОС Android, а также в процессы других приложений

«Мобильная» угроза месяца

В марте специалисты компании «Доктор Веб» исследовали вредоносную программу Android.Gmobi.1, которая была обнаружена в приложениях TrendMicro Dr.Safety, TrendMicro Dr.Booster и Asus WebStorage, а также предустановлена на более чем 40 моделях мобильных Android-устройств. Она представляет собой специализированную программную SDK-платформу (Software Development Kit), используемую разработчиками ПО и производителями смартфонов и планшетов. Вероятнее всего, авторы не задумывали этот модуль как троянца, однако ведет он себя как типичная вредоносная программа.



Так, Android.Gmobi.1 может демонстрировать навязчивую рекламу нескольких типов, например, помещать ее в панель уведомлений или показывать в виде баннеров поверх окон запущенных программ. Кроме того, троянец без спроса создает ярлыки на рабочем столе ОС, открывает различные страницы в веб-браузере и в приложении Google Play, а также способен загружать, устанавливать и запускать различное ПО. Ко всему прочему, Android.Gmobi.1 обладает и шпионскими функциями – он крадет и передает злоумышленникам различную конфиденциальную информацию. Подробнее об этом вредоносном приложении можно узнать из опубликованной на сайте компании «Доктор Веб» новости.

Обзор вирусной активности для мобильных Android-устройств в марте 2016 года

По данным антивирусных продуктов Dr.Web для Android

- **Adware.WalkFree.1.origin**
  Нежелательный программный модуль, встраиваемый в Android-приложения и предназначенный для показа навязчивой рекламы на мобильных устройствах.
- **Adware.Leadbolt.12.origin**
  Нежелательный программный модуль, встраиваемый в Android-приложения и предназначенный для показа навязчивой рекламы на мобильных устройствах.
- **Adware.AdMogo.2.origin**
  Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.
- **Android.Xiny.26.origin**
  Троянская программа, которая получает root-привилегии, устанавливается в системный каталог Android и в дальнейшем устанавливает различные программы без разрешения пользователя. Также она может показывать навязчивую рекламу.
- **Adware.Airpush.31.origin**
  Нежелательный программный модуль, встраиваемый в Android-приложения и предназначенный для показа навязчивой рекламы на мобильных устройствах.

Обзор вирусной активности для мобильных Android-устройств в марте 2016 года

Примечательные троянцы

В марте вирусные аналитики «Доктор Веб» завершили исследование целой группы троянцев семейства Android.Triada, внедряющихся в важный системный процесс Zygote и выполняющих вредоносные действия по команде злоумышленников. В ОС Android процесс Zygote отвечает за запуск всех приложений и при их старте создает для них в оперативной памяти свою копию, содержащую системные библиотеки и другие необходимые для работы компоненты. Внедряясь в Zygote, троянцы фактически получают возможность инфицировать процессы всех запускаемых в дальнейшем программ и могут выполнять вредоносные действия от имени и с правами этих приложений.

Основная вредоносная функция, реализованная в настоящий момент в троянцах Android.Triada, – это незаметная отправка СМС, а также подмена текста и номера получателя у сообщений, которые отправляет пользователь зараженного мобильного устройства. Тем не менее, по команде с управляющего сервера вредоносные программы могут загрузить дополнительные компоненты, которые будут использоваться для выполнения других нежелательных действий, необходимых злоумышленникам.

Примечательно, что представители семейства Android.Triada обладают функцией самозащиты. В частности, троянцы пытаются отследить и завершить работу ряда популярных в Китае антивирусных программ. Кроме того, они контролируют целостность своих компонентов: если какой-либо из вредоносных файлов будет удален с устройства, он будет восстановлен из оперативной памяти.

Появление троянцев Android.Triada вновь показало, что вредоносные приложения для Android-смартфонов и планшетов становятся все опаснее и изощреннее и зачастую не уступают по своим функциональным возможностям троянцам для ОС Windows. Специалисты «Доктор Веб» постоянно отслеживают вирусную обстановку и оперативно добавляют в вирусную базу записи для всех новых вредоносных приложений.

Обзор вирусной активности для мобильных Android-устройств в марте 2016 года

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

Полезные ресурсы
ВебIQметр | Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | www.mobi.drweb.com | www.av-desk.ru
«Доктор Веб» в других странах