Dr.WEB®
с 1992 года

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

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

31 октября 2016 года

Второй осенний месяц не преподнес никаких сюрпризов пользователям Android-устройств. В самом начале октября в каталоге Google Play был обнаружен троянец, использующий зараженные смартфоны и планшеты в качестве прокси-серверов.

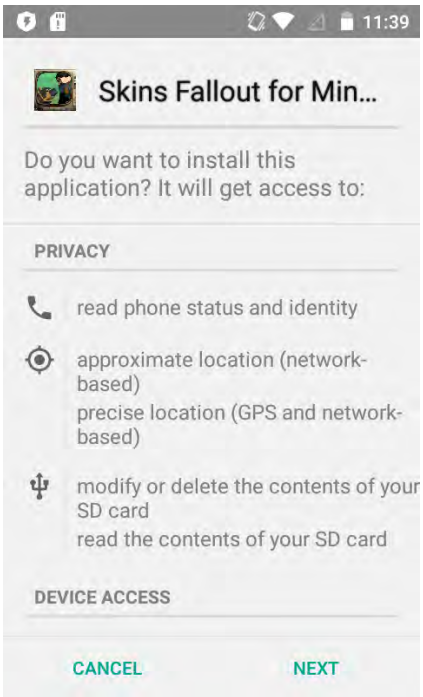
Главные тенденции октября

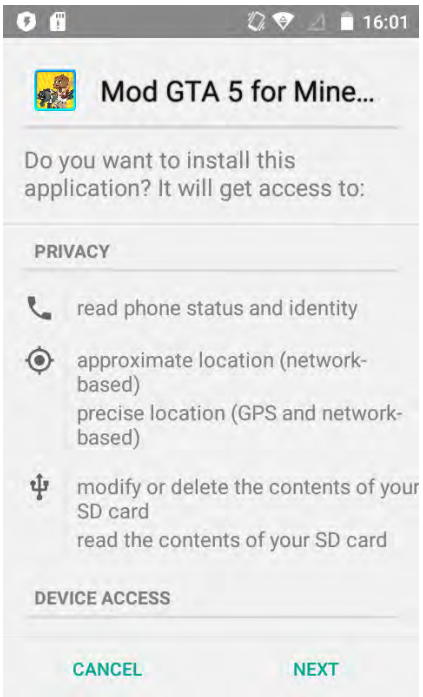
- Обнаружение Android-троянцев в каталоге приложений Google Play

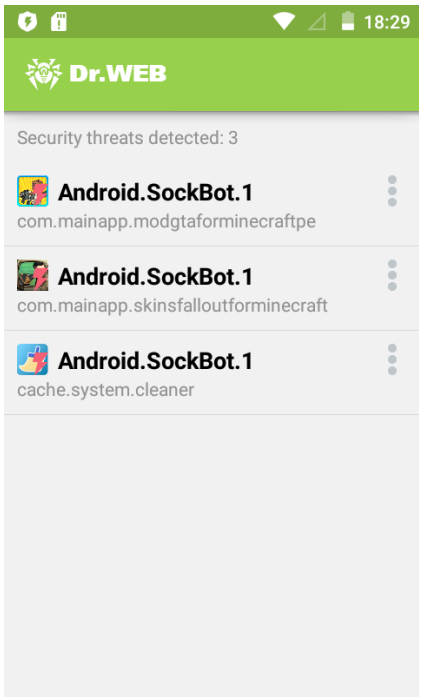
Обзор вирусной активности для мобильных Android-устройств в октябре 2016 года

«Мобильная» угроза месяца

В конце сентября — начале октября специалисты по информационной безопасности обнаружили в каталоге Google Play троянца Android.SockBot.1. Эта вредоносная программа была встроена в различные приложения, такие как справочники по прохождению игр, а также любительские модификации и дополнения к игровым приложениям. После запуска на мобильном Android-устройстве Android.SockBot.1 незаметно устанавливает интернет-соединение и использует зараженный смартфон или планшет в качестве прокси-сервера. Благодаря этому злоумышленники могут анонимно соединяться с удаленными компьютерами и другими устройствами, подключенными к сети, не раскрывая своего реального местоположения. Кроме того, они могут перехватывать и перенаправлять сетевой трафик, похищать конфиденциальную информацию и даже организовывать DDoS-атаки (распределенные атаки, приводящие к отказу в обслуживании) на интернет-серверы.







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

По данным антивирусных продуктов Dr.Web для Android

- **Android.Banker.70.origin**
- **Android.Xiny.26.origin**
  Троянские программы, которые получают root-привилегии, копируются в системный каталог Android и в дальнейшем устанавливают различные приложения без разрешения пользователя. Также они могут показывать навязчивую рекламу.
- **Android.BankBot.139.origin**
  Троянцы, которые крадут логины и пароли доступа от учетных записей мобильного банкинга, а также похищают деньги с банковских счетов пользователей мобильных устройств под управлением ОС Android.
- **Android.Mobifun.7**
  Троянец, предназначенный для загрузки других Android-приложений.
- **Android.Backdoor.471.origin**
  Троянец, незаметно выполняющий вредоносные действия по команде злоумышленников.

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

- **Adware.Airpush.31.origin**
- **Adware.Leadbolt.12.origin**
- **Adware.WalkFree.1.origin**
- **Adware.WalkFree.2.origin**
- **Adware.Appsad.3.origin**

Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

Несмотря на усиленные меры безопасности, вредоносные программы для мобильных Android-устройств по-прежнему могут проникать в официальные каталоги приложений, такие как Google Play. Поэтому перед установкой понравившегося ПО пользователи должны удостовериться, что та или иная программа распространяется надежным разработчиком и не является подделкой. Кроме того, для защиты смартфонов и планшетов от вредоносных и нежелательных приложений владельцы Android-устройств могут установить антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных Android-устройств в октябре 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