Dr.WEB®
с 1992 года

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

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

30 ноября 2016 года

В течение последнего осеннего месяца 2016 года произошло несколько инцидентов с участием вредоносных программ для Android. В начале ноября вирусные аналитики «Доктор Веб» выявили нового троянца в каталоге Google Play, а позднее был обнаружен троянец, который был предустановлен на популярных мобильных Android-устройствах.

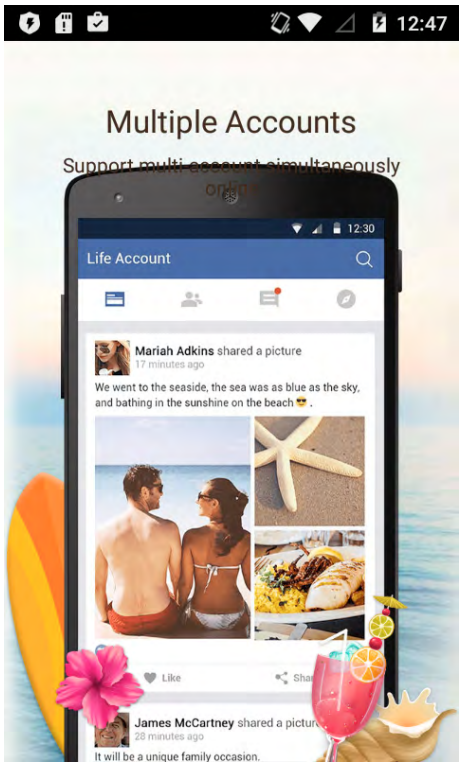
Главные тенденции ноября

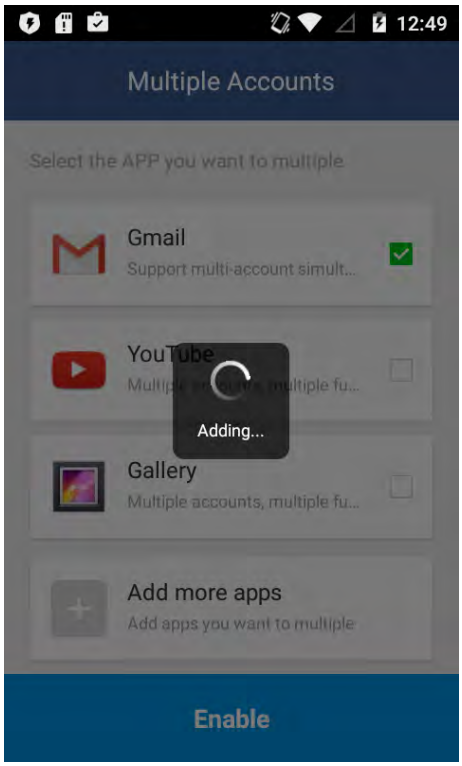
- Обнаружение Android-троянца в каталоге приложений Google Play
- Обнаружение вредоносной программы, предустановленной на мобильных Android-устройствах

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

«Мобильная» угроза месяца

В начале ноября вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play троянца Android.MulDrop.924, который распространялся под видом безобидного приложения с именем Multiple Accounts: 2 Accounts. Оно позволяло владельцам мобильных устройств одновременно использовать в установленных программах несколько учетных записей. На момент обнаружения это вредоносное приложение успели скачать более 1 000 000 пользователей. В настоящее время троянец удален из каталога.





Особенности Android.MulDrop.924:

- часть функционала вынесена во вспомогательные модули, которые спрятаны в PNG-изображении;
- скачивает приложения без ведома пользователя и предлагает установить их;
- показывает навязчивую рекламу.

Подробнее об Android.MulDrop.924 рассказано в новостной публикации на сайте компании «Доктор Веб».

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

По данным антивирусных продуктов Dr.Web для Android

- **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 могут показывать навязчивую рекламу.
- **Android.DownLoader.337.origin**
  Троянец, загружающий на мобильные устройства другие программы.
- **Android.Mobifun.7**
  Троянец, предназначенный для загрузки других Android-приложений.
- **Android.Cooee.1.origin**
  Троянская программа, предназначенная для незаметной загрузки и установки приложений, а также показа рекламы.
- **Android.MulDrop.66.origin**
  Троянец, который распространяет и устанавливает на Android-устройства другие вредоносные приложения.

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

- **Adware.Airpush.31.origin**
- **Adware.WalkFree.2.origin**
- **Adware.Leadbolt.12.origin**
- **Adware.Appsad.3.origin**
- **Adware.Batad.10**

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

Предустановленные троянцы

Во второй половине ноября специалисты по информационной безопасности обнаружили Android-троянца, который был предустановлен на некоторых популярных мобильных устройствах — например, на смартфоне BLU R1 HD. Эта вредоносная программа, добавленная в вирусную базу Dr.Web как Android.Spy.332.origin, изначально представляла собой системное ПО для обновления прошивки и ранее не была опасной. Однако в новой версии в нее был добавлен троянский функционал.

Особенности Android.Spy.332.origin:

- незаметно скачивает, устанавливает и удаляет ПО;
- выполняет shell-команды;
- передает на управляющий сервер конфиденциальную информацию, такую как сведения об СМС-сообщениях, телефонных звонках и ряд технических данных о зараженном мобильном устройстве.

Вредоносные программы для мобильных устройств под управлением ОС Android по-прежнему угрожают безопасности пользователей. Время от времени Android-троянцы могут распространяться через официальный каталог Google Play и даже предустанавливаться на смартфоны и планшеты. Для предотвращения попадания вредоносных и нежелательных приложений на Android-устройства, а также для обнаружения уже проникших на них троянцев пользователям следует установить антивирусное ПО Dr.Web для Android.

Обзор вирусной активности для мобильных Android-устройств в ноябре 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