Dr.WEB®
с 1992 года

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

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

26 декабря 2016 года

Минувший декабрь оказался богатым на события мобильной вирусной тематики. В начале месяца вирусные аналитики компании «Доктор Веб» обнаружили Android-троянца, который заражал системные библиотеки, внедрялся в процессы программ, после чего незаметно скачивал и устанавливал различное ПО. А позднее были выявлены вредоносные приложения, которые злоумышленники предустанавливали на десятки моделей Android-смартфонов и планшетов. Эти троянцы также скрытно загружали и устанавливали программы.

Главные тенденции декабря

- Обнаружение Android-троянца, который заражает системные библиотеки и внедряется в процессы приложений
- Обнаружение вредоносных программ, предустановленных на множестве мобильных Android-устройств

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

«Мобильная» угроза месяца

В начале декабря специалисты компании «Доктор Веб» обнаружили троянца Android.Loki.16.origin, который незаметно загружал и устанавливал ПО на мобильные устройства. Эта вредоносная программа пыталась получить root-доступ с использованием эксплойтов, после чего копировала в системные каталоги несколько вспомогательных модулей. С их помощью она заражала системные библиотеки ОС Android и запускалась вместе с ними, получая те же полномочия, что и они. В результате Android.Loki.16.origin мог без разрешения пользователя скачивать, устанавливать и удалять любые приложения. Подробнее об этом троянце рассказано в публикации на сайте компании «Доктор Веб».

По данным антивирусных продуктов Dr.Web для Android

- **Android.MulDrop.66.origin**
  Троянец, который распространяет и устанавливает другие вредоносные приложения.
- **Android.Sprovider.15.origin**
  Троянец, который загружает на мобильные Android-устройства различные приложения и пытается их установить. Кроме того, он может показывать рекламу.
- **Android.DownLoader.337.origin**
  Троянец, предназначенный для загрузки других вредоносных приложений.
- **Android.Loki.10.origin**
  Вредоносная программа, предназначенная для загрузки других троянцев.
- **Android.MobiDash.44**
  Троянец, показывающий навязчивую рекламу на Android-устройствах.

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

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

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

Троянцы в прошивках

В середине месяца вирусные аналитики «Доктор Веб» обнаружили несколько троянцев, которых злоумышленники внедрили в прошивки десятков моделей Android-устройств. Один из них, получивший имя Android.DownLoader.473.origin, по команде вирусописателей незаметно скачивал и устанавливал программы, например, нежелательное приложение Adware.AdBox.1.origin, показывающее рекламу. Другой троянец, добавленный в вирусную базу как Android.Sprovider.7, также загружал и пытался установить приложения. Кроме того, он открывал в браузере различные веб-страницы, самостоятельно выполнял телефонные звонки и показывал рекламу. Подробнее об этих вредоносных программах можно узнать, обратившись к соответствующей новости.

Чтобы заразить мобильные устройства, киберпреступники не останавливаются ни перед чем – они внедряют троянцев даже в прошивки. В результате пользователи рискуют столкнуться с вредоносными программами, купив совершенно новый смартфон или планшет. Чтобы выявить предустановленные вредоносные приложения, владельцам Android-устройств следует использовать антивирусные продукты Dr.Web для Android. При обнаружении троянцев в системных каталогах необходимо обратиться в службу поддержки производителя и запросить обновление операционной системы, в котором проблема будет устранена.

Обзор вирусной активности для мобильных Android-устройств в декабре 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.av-desk.ru
«Доктор Веб» в других странах