Dr.WEB®
с 1992 года

Обзор вирусной активности для мобильных Android-устройств в июле 2017 года

Обзор вирусной активности для мобильных Android-устройств в июле 2017 года

31 июля 2017 года

В июле специалисты компании «Доктор Веб» обнаружили на нескольких моделях Android-смартфонов предустановленного троянца, которого злоумышленники внедрили в системную библиотеку. Эта вредоносная программа проникала в процессы приложений и могла незаметно скачивать и запускать дополнительные модули. Кроме того, в каталоге Google Play была выявлена игра со встроенным в нее троянцем-загрузчиком. Также в июле вирусные аналитики исследовали опасного банковского троянца, получающего контроль над зараженными устройствами и крадущего конфиденциальные данные.

Главные тенденции июля

- Обнаружение в прошивке нескольких моделей Android-устройств троянца, который внедрялся в процессы приложений и незаметно запускал вредоносные модули
- Выявление троянца-загрузчика в каталоге Google Play
- Появление опасного банковского троянца

Обзор вирусной активности для мобильных Android-устройств в июле 2017 года

«Мобильная» угроза месяца

В июле вирусные аналитики компании «Доктор Веб» выявили троянца Android.Triada.231, которого злоумышленники встроили в одну из системных библиотек ОС Android. Эта вредоносная программа проникает в процессы всех работающих приложений и может незаметно скачивать и запускать дополнительные троянские модули. Троянец был обнаружен сразу на нескольких моделях Android-устройств.

Особенности Android.Triada.231:

- встраивание в системную библиотеку выполнено на уровне исходного кода;
- проникает в процессы всех запускаемых приложений и внедряет в них вредоносные модули;
- для удаления троянца с устройства требуется установка чистого образа операционной системы.

Подробнее о троянце рассказано в публикации, размещенной на сайте компании «Доктор Веб».

Обзор вирусной активности для мобильных Android-устройств в июле 2017 года

По данным антивирусных продуктов Dr.Web для Android

- **Android.DownLoader.337.origin**
- **Android.DownLoader.526.origin**
  Троянские программы, предназначенные для загрузки других приложений.
- **Android.HiddenAds.85.origin**
- **Android.HiddenAds.68.origin**
- **Android.HiddenAds.83.origin**
  Троянцы, предназначенные для показа навязчивой рекламы. Распространяются под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают их в системный каталог.

- **Adware.Avazu.8.origin**
- **Adware.SalmonAds.1.origin**
- **Adware.Jiubang.1**
- **Adware.Batmobi.4**
- **Adware.Cootek.1.origin**
  Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

Обзор вирусной активности для мобильных Android-устройств в июле 2017 года

Троянец в Google Play

В июле специалисты компании «Доктор Веб» обнаружили в каталоге Google Play троянца Android.DownLoader.558.origin, встроенного в популярную игру BlazBlue. Эта вредоносная программа входит в состав программного модуля, предназначенного для оптимизации обновления ПО. Ее опасность заключается в том, что она способна незаметно скачивать и запускать непроверенные компоненты приложений. Подробная информация об Android.DownLoader.558.origin содержится в нашей новости.

Банковский троянец

В прошедшем месяце был обнаружен опасный банковский троянец Android.BankBot.211.origin, который пытался получить доступ к специальным возможностям (Accessibility Service) в ОС Android. С их помощью он мог управлять зараженными устройствами и красть всю вводимую на клавиатуре информацию, в том числе пароли. Кроме того, Android.BankBot.211.origin показывал фишинговые формы для ввода конфиденциальных данных поверх запускаемых банковских программ, ПО для работы с платежными сервисами и других приложений. С особенностями работы этого троянца можно ознакомиться, прочитав соответствующий материал на нашем сайте.

Вирусописатели по-прежнему атакуют пользователей мобильных Android-устройств. Они постоянно расширяют функционал троянцев и стараются распространять их всеми доступными способами. Для защиты от вредоносных приложений владельцам смартфонов и планшетов рекомендуется установить антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных Android-устройств в июле 2017 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
125040, 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