Dr.WEB®
с 1992 года

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

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

29 декабря 2017 года

В последнем месяце 2017 года в каталоге Google Play было найдено несколько новых троянцев, которые скрывались внутри безобидных приложений. Эти вредоносные программы представляли собой банкеров, кравших конфиденциальную информацию клиентов кредитных организаций. Другой «декабрьский» Adroid-троянец, который угрожал владельцам Android-устройств, распространялся вне официального каталога ПО. Он также похищал логины и пароли, необходимые для доступа к банковским учетным записям. Кроме того, в уходящем месяце злоумышленники распространяли вредоносную программу, которая шпионила за итальянскими пользователями.

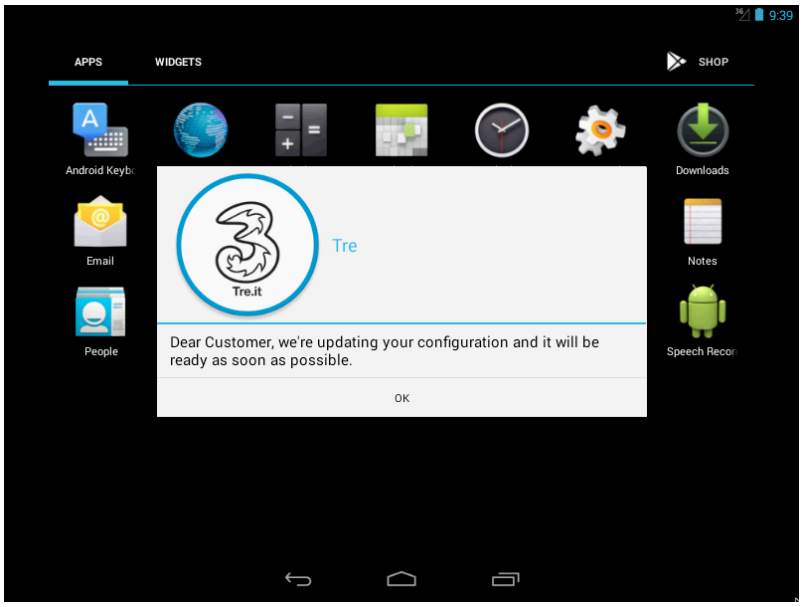
Главные тенденции декабря

- Распространение новых банковских троянцев
- Обнаружение троянца-шпиона, кравшего персональную информацию

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

Мобильная угроза месяца

В декабре в вирусную базу Dr.Web была добавлена запись для детектирования троянца Android.Spy.410.origin, который шпионил за итальянскими владельцами Android-устройств и крал их конфиденциальные данные. Так, он передавал злоумышленникам переписку из популярных программ для общения и работы с социальными сетями, таких как Skype, WhatsApp, Telegram и других. Кроме того, он перехватывал СМС-сообщения и телефонные звонки, а также мог похищать изображения, хранящиеся в памяти зараженного мобильного устройства.



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

По данным антивирусных продуктов Dr.Web для Android

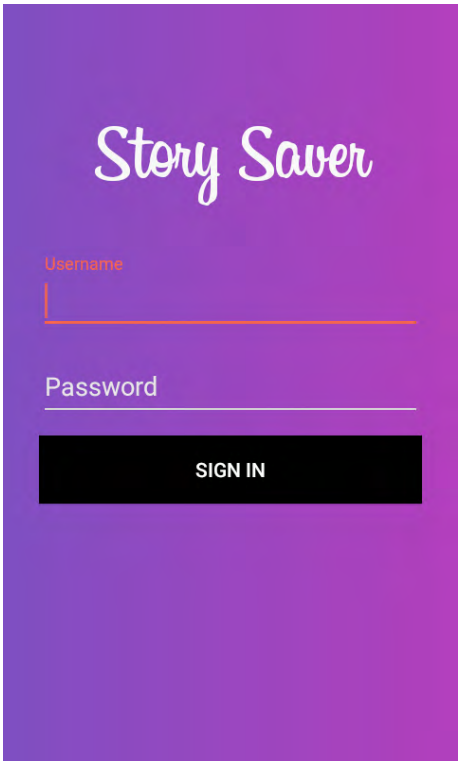
- **Android.HiddenAds.171.origin**
  Троянец, предназначенный для показа навязчивой рекламы.
- **Android.RemoteCode.71**
  Троянская программа, которая скачивает и запускает различные программные модули, в том числе вредоносные.
- **Android.Packed.15893**
  Троянец, который крадет логины и пароли доступа от банковских учетных записей.
- **Android.DownLoader.653.origin**
- **Android.DownLoader.573.origin**
  Вредоносные программы, которые загружают других троянцев, а также нежелательное ПО.

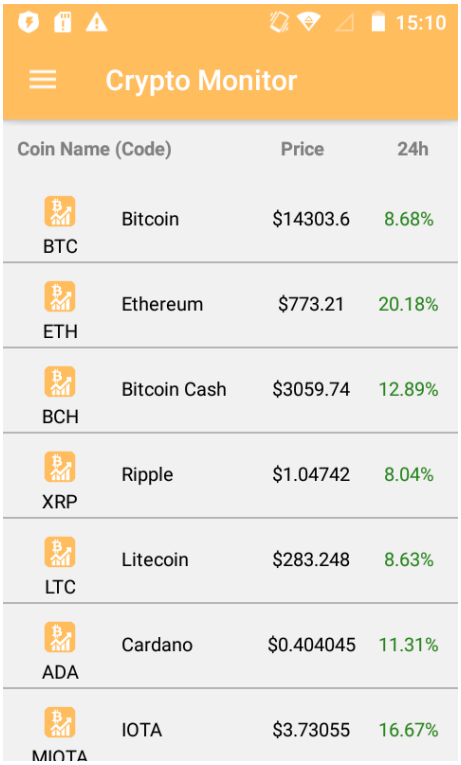
- **Adware.Jiubang.2**
- **Adware.Jiubang.1**
- **Adware.Saturn.1.origin**
- **Adware.Adviator.6.origin**
- **Adware.Leadbolt.12.origin**
  Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

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

Банковские троянцы

В декабре в официальном каталоге Android-приложений Google Play были найдены очередные банковские троянцы, которые по классификации Dr.Web получили имена Android.BankBot.243.origin и Android.BankBot.255.origin. Киберпреступники встроили их в безобидные программы, чтобы не вызывать у потенциальных жертв лишних подозрений. Эти троянцы искали на зараженных смартфонах и планшетах заданные вирусописателями банковские приложения и показывали пользователям поддельные формы ввода логина и пароля для доступа к учетным записям. После этого банкеры передавали полученную информацию злоумышленникам.





Кроме того, в уходящем месяце пользователей Android-устройств атаковал троянец Android.Packed.15893. Он также демонстрировал мошеннические окна, в которых запрашивал логины и пароли от учетных записей мобильного банкинга и передавал киберпреступникам все введенные данные.

Банковские троянцы представляют серьезную угрозу, поскольку с их помощью вирусописатели крадут деньги владельцев мобильных устройств. Злоумышленники распространяют такие вредоносные программы как через каталог Google Play, так и через сторонние магазины приложений, а также взломанные или мошеннические веб-сайты. Для защиты Android-смартфонов и планшетов от этих и других угроз пользователям необходимо установить антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных Android-устройств в декабре 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