Dr.WEB®
с 1992 года

# Обзор вирусной активности для мобильных Android-устройств в ноябре 2017 года

# Обзор вирусной активности для мобильных Android-устройств в ноябре 2017 года

30 ноября 2017 года

В ноябре в каталоге Google Play было найдено множество вредоносных приложений.

В начале месяца в нем был обнаружен троянец-майнер, использовавший вычислительные мощности мобильных устройств для добычи криптовалюты. Позже специалисты по информационной безопасности выявили СМС-троянцев, подписывавших пользователей на платные услуги. В середине ноября вирусные аналитики «Доктор Веб» обнаружили вредоносную программу, которая скачивала и запускала дополнительные троянские модули. Эти модули загружали веб-сайты и переходили по расположенным на них рекламным ссылкам и баннерам. Кроме того, в Google Play распространялся троянец, предназначенный для загрузки различных приложений. Помимо этого в каталоге были найдены Android-банкеры, которые крали конфиденциальные сведения пользователей и похищали деньги с их счетов.

## Главные тенденции ноября

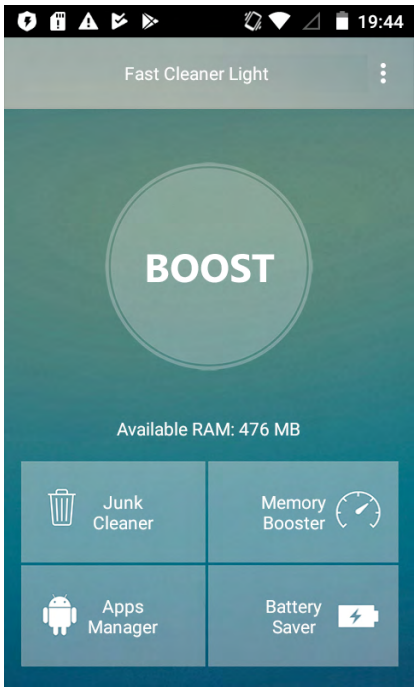
- Обнаружение в каталоге Google Play большого числа троянцев, которые были встроены в безобидные приложения

# Обзор вирусной активности для мобильных Android-устройств в ноябре 2017 года

## «Мобильная» угроза месяца

В ноябре вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play 9 программ, в которые был встроен троянец Android.RemoteCode.106.origin. В общей сложности эти приложения были загружены не менее 2 370 000 раз. После запуска Android.RemoteCode.106.origin скачивает и запускает дополнительные вредоносные модули. Они используются для автоматического открытия заданных управляющим сервером веб-страниц и нажатия на расположенные на них рекламные баннеры и ссылки. Подробнее об Android.RemoteCode.106.origin рассказано в публикации, размещенной на сайте компании «Доктор Веб».





# Обзор вирусной активности для мобильных Android-устройств в ноябре 2017 года

## По данным антивирусных продуктов Dr.Web для Android

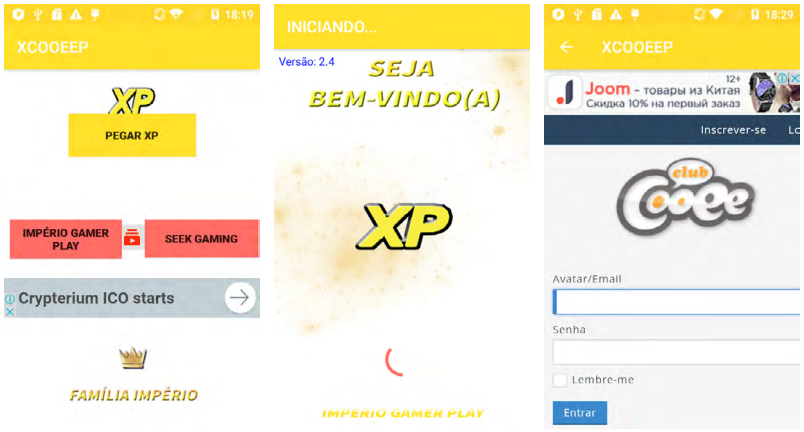

- **Android.HiddenAds.238**
  Троянцы, предназначенные для показа навязчивой рекламы.
- **Android.Triada.63**
- **Android.Triada.152**
  Представитель семейства троянцев, выполняющих разнообразные вредоносные действия.
- **Android.DownLoader.653.origin**
  Троянец, загружающий другие вредоносные программы.
- **Android.Click.171.origin**
  Троянец, который с определенной периодичностью обращается к заданным веб-сайтам и может использоваться для накрутки их популярности, а также перехода по рекламным ссылкам.


- **Adware.Jiubang.2**
- **Adware.Jiubang.1**
- **Adware.Adviator.6.origin**
- **Adware.Airpush.31.origin**
- **Adware.SalmonAds.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 ноябре 2017 года

## Троянец-майнер

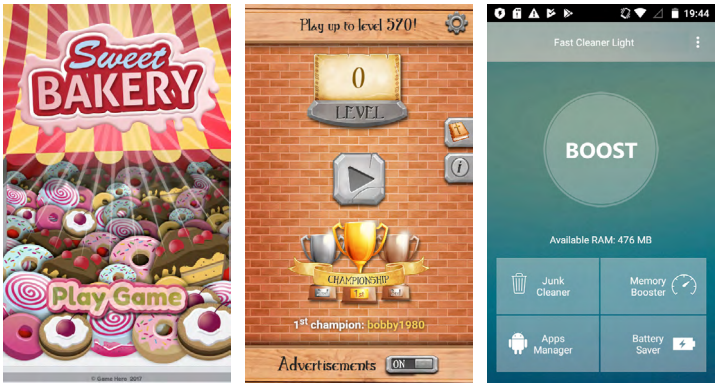
В начале ноября в каталоге Google Play был выявлен троянец Android.CoinMine.3, который использовал вычислительные мощности Android-смартфонов и планшетов для добычи криптовалюты Monero. Эта вредоносная программа скрывалась в приложении под названием XCOOEEP, предназначенном для доступа к онлайн-чату Club Cooee.




Android.CoinMine.3 загружал в невидимом окне WebView веб-сайт с расположенным на нем скриптом для майнинга, который запускался автоматически. В результате интенсивной работы процессора при добыче криптовалюты зараженное мобильное устройство могло снизить свою производительность и нагреться, а его аккумулятор – разряжаться быстрее.

## СМС-троянцы

Среди распространявшихся через Google Play вредоносных приложений, выявленных в прошедшем месяце, оказалось несколько СМС-троянцев. Они были встроены в приложения Secret Notepad, Delicate Keyblard и Super Emotion, детектируемые Dr.Web как Android.SmsSend.23371, Android.SmsSend.23373 и Android.SmsSend.23374. Эти вредоносные программы пытались отправить дорогостоящие СМС и подписать абонентский номер владельца зараженного устройства на ненужные услуги.



# Обзор вирусной активности для мобильных Android-устройств в ноябре 2017 года

## Троянец-загрузчик

В ноябре в каталоге Google Play были обнаружены новые модификации троянца Android.DownLoader.658.origin, который по команде управляющего сервера предлагал владельцам мобильных устройств скачать и установить различные приложения. Кроме того, он мог самостоятельно загружать ПО. Особенности Android.DownLoader.658.origin:

- встроен в безобидные приложения;
- задействует вредоносный функционал только в случае выполнения ряда условий (например, если он не запущен в эмуляторе или на мобильном устройстве выключены функции для разработчиков);
- может показывать уведомления, в которых предлагает скачать и установить ту или иную программу;
- для защиты от обнаружения и анализа авторы троянца используют специальный упаковщик, детектируемый антивирусом Dr.Web как Android.Packed.1.

## Банковские троянцы

В прошедшем месяце в каталоге Google Play был выявлен троянец Android.Banker.202.origin, который скрывался в безобидных приложениях. После старта он извлекал из своих файловых ресурсов и запускал вредоносную программу Android.Banker.1426. Этот троянец скачивал с управляющего сервера один из Android-банкеров семейства Android.BankBot, предназначенный для кражи логинов, паролей и другой конфиденциальной информации.

Аналогичная схема применялась в ряде троянцев семейства Android.Banker, которые тоже были обнаружены в Google Play в ноябре. Они извлекали и запускали скрытый внутри них вредоносный компонент, который также извлекал из своих файловых ресурсов и запускал другой троянский компонент. Он, в свою очередь, скачивал с удаленного центра и пытался установить одного из банковских троянцев.

Обнаружение большого числа вредоносных приложений в каталоге Google Play говорит о том, что злоумышленники по-прежнему находят способы обхода его защитных механизмов. Чтобы обезопасить мобильные устройства от троянцев и других нежелательных программ, владельцам Android-смартфонов и планшетов необходимо установить антивирусные продукты Dr.Web для Android.

# Обзор вирусной активности для мобильных Android-устройств в ноябре 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