



«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2018 года



Обзор вирусной активности для мобильных устройств в феврале 2018 года

28 февраля 2018 года

В феврале 2018 года был обнаружен троянец-майнер, который мог удаленно заражать различные Android-устройства с активным режимом отладки. Кроме того, в уходящем месяце пользователям угрожал троянец [Android.BankBot.336.origin](https://www.drweb.com/ru/press-releases/android-bankbot-336-origin), крадший конфиденциальную информацию и похищавший деньги с банковских счетов.

Главные тенденции февраля

- Распространение троянца-майнера, способного самостоятельно заражать некоторые Android-устройства
- Распространение очередного банковского троянца

Обзор вирусной активности для мобильных устройств в феврале 2018 года

Мобильная угроза месяца

В феврале получил [распространение троянец Android.CoinMine.15](#), которого вирусописатели использовали для добычи криптовалюты Monero. Эта вредоносная программа представляла собой червя и могла самостоятельно заражать подключенные к сети смартфоны, планшеты, телевизоры, роутеры и другие Android-устройства, если на них был включен режим отладки Android Device Bridge (ADB). В случае успешного инфицирования очередного устройства один из компонентов троянца пытался обнаружить следующую доступную цель и устанавливал на нее копию [Android.CoinMine.15](#).

Обзор вирусной активности для мобильных устройств в феврале 2018 года

По данным антивирусных продуктов Dr.Web для Android

Наиболее распространенные вредоносные программы согласно статистике детектирования антивирусных продуктов Dr.Web для Android



[Android.RemoteCode.121.origin](#)

[Android.RemoteCode.117.origin](#)

Троянские программы, которые скачивают и запускают различные программные модули, в том числе вредоносные.

[Android.HiddenAds.253](#)

[Android.HiddenAds.222.origin](#)

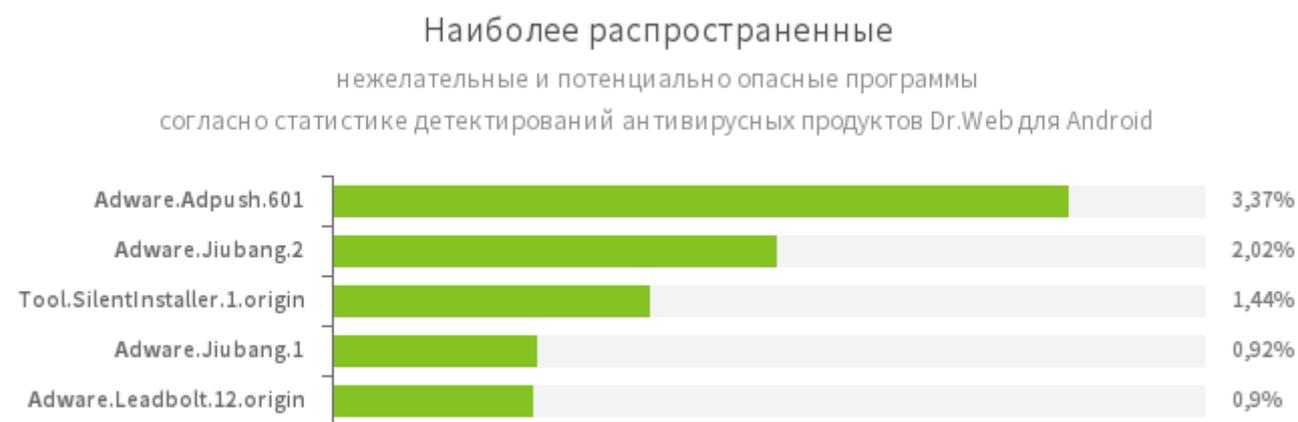
Обзор вирусной активности для мобильных устройств в феврале 2018 года

По данным антивирусных продуктов Dr.Web для Android

Троянцы, предназначенные для показа навязчивой рекламы. Распространяются под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают их в системный каталог.

[Android.Mobifun.4](#)

Троянец, загружающий другие вредоносные приложения.



Adware.Adpush.601

Adware.Jiubang.2

Adware.Jiubang.1

[Adware.Leadbolt.12.origin](#)

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

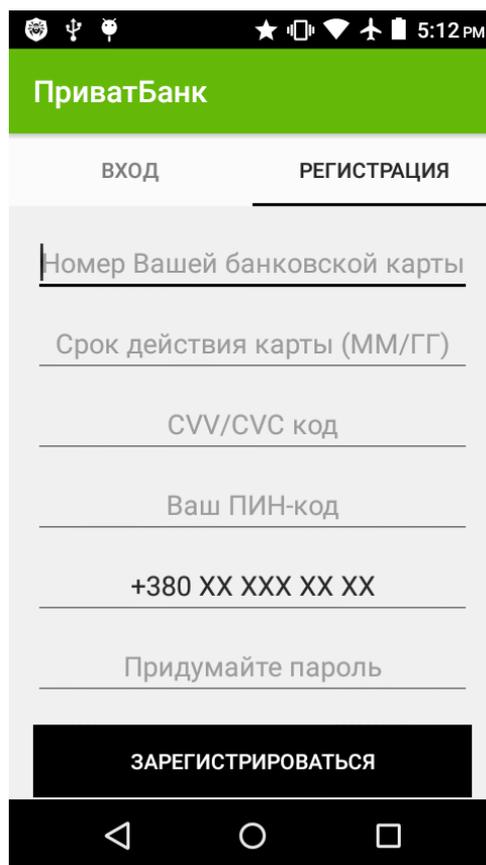
[Tool.SilentInstaller.1.origin](#)

Потенциально опасная программа, предназначенная для незаметного запуска приложений без вмешательства пользователя.

Обзор вирусной активности для мобильных устройств в феврале 2018 года

Банковский троянец

В уходящем месяце в каталоге Google Play был обнаружен троянец [Android.BankBot.336.origin](#), которого вирусописатели распространяли под видом универсального приложения для работы с различными системами онлайн-банкинга. Вредоносная программа похищала логины и пароли от учетных записей пользователей, а также информацию о банковских картах, после чего могла незаметно переводить злоумышленникам деньги. Вирусописатели продолжают совершенствовать вредоносные программы для ОС Android и распространяют их с применением как привычных, так и новых механизмов. При этом различные троянцы по-прежнему встречаются в каталоге Google Play. Для защиты смартфонов, планшетов и других устройств от этих угроз пользователям следует установить антивирусные продукты Dr.Web для Android.



Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

Обзор вирусной активности для мобильных устройств в феврале 2018 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

[ВебиОметр](#) | [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 | free.drweb.ru | www.av-desk.ru

[«Доктор Веб» в других странах](#)



© ООО «Доктор Веб»,
2003-2018

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)