



«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2019 года



Обзор вирусной активности для мобильных устройств в марте 2019 года

3 апреля 2019 года

В марте компания «Доктор Веб» рассказала об уязвимости в мобильном браузере UC Browser, который способен скачивать новые модули со стороннего сервера. Злоумышленники могли использовать эту функцию для заражения Android-смартфонов и планшетов. Кроме того, вирусные аналитики поделились сведениями о троянце Flexnet, который крал деньги с банковских карт и счетов мобильных телефонов. В течение месяца в каталоге Google Play были выявлены очередные вредоносные приложения.

Главные тенденции марта

- Обнаружение уязвимости в браузере UC Browser
- Распространение банковских троянцев
- Выявление новых вредоносных программ в каталоге Google Play

Обзор вирусной активности для мобильных устройств в марте 2019 года

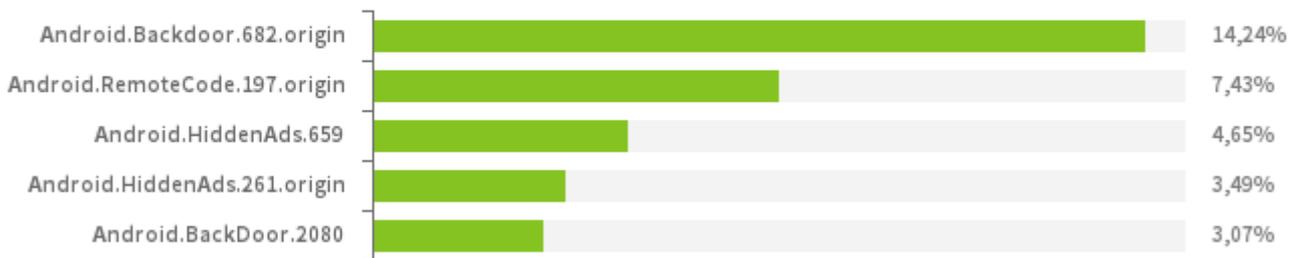
Мобильная угроза месяца

В конце марта компания «Доктор Веб» [рассказала](#) об уязвимости в Android-браузере UC Browser, которую обнаружили наши вирусные аналитики. Эта программа загружала дополнительные плагины в обход серверов Google Play, нарушая правила каталога этого ПО. Злоумышленники могли вмешаться в процесс скачивания плагинов и сделать так, чтобы вместо них браузер загружал и запускал вредоносные файлы. Опасности подверглись свыше 500 000 000 пользователей мобильных устройств. Детали этой уязвимости описаны в нашей вирусной библиотеке.

Обзор вирусной активности для мобильных устройств в марте 2019 года

По данным антивирусных продуктов Dr.Web для Android

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



- [Android.Backdoor.682.origin](#)
- [Android.Backdoor.2080](#)

Троянцы, которые выполняют команды злоумышленников и позволяют им контролировать зараженные мобильные устройства.

- [Android.RemoteCode.197.origin](#)

Вредоносное приложение, предназначенное для загрузки и выполнения произвольного кода.

- [Android.HiddenAds.659](#)
- [Android.HiddenAds.261.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.

Обзор вирусной активности для мобильных устройств в марте 2019 года

По данным антивирусных продуктов Dr.Web для Android

Наиболее распространенные
нежелательные и потенциально опасные программы
согласно статистике детектирований антивирусных продуктов Dr.Web для Android



- Adware.Zeus.1
- Adware.Jiubang.2
- Adware.Toofan.1.origin
- Adware.Gexin.3.origin

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

- [Tool.VirtualApk.1.origin](#)

Потенциально опасная программная платформа, которая позволяет приложениям запускать арк-файлы без их установки.

Обзор вирусной активности для мобильных устройств в марте 2019 года

Android-банкеры

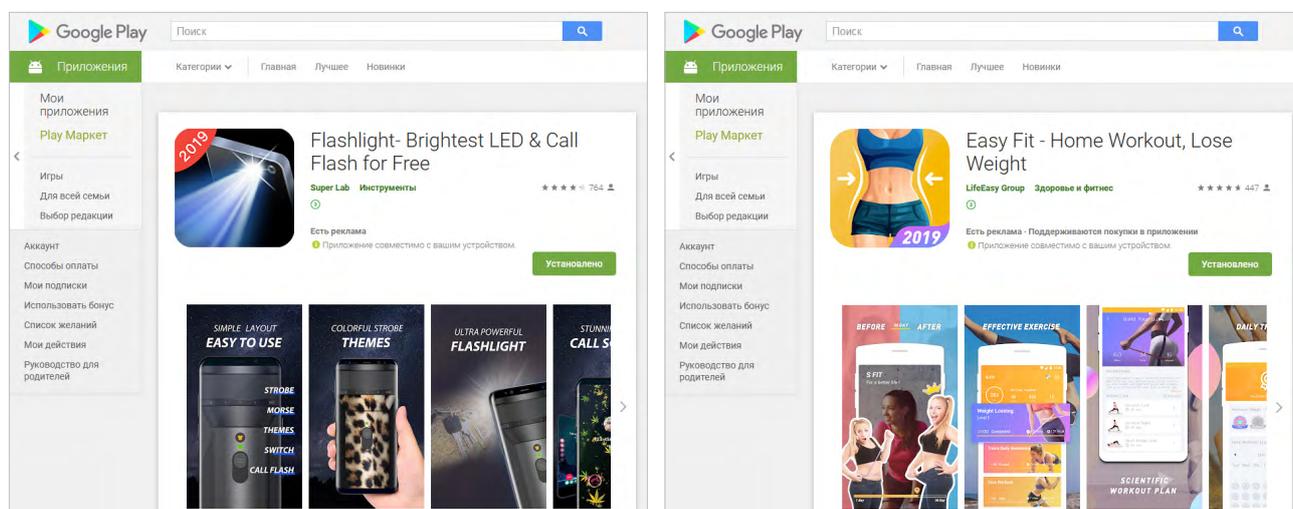
Злоумышленники продолжают распространять банковских троянцев, созданных на основе исходного кода вредоносного приложения [Android.ZBot](#). Один из них — троянец Flexnet. Он крадет деньги с банковских карт, а также может оплачивать различные сервисы, используя счета мобильных телефонов жертв. Например, с помощью этого троянца киберпреступники способны пополнять баланс игр, оплачивать услуги хостинг-провайдеров и переводить средства на собственные мобильные телефоны. Подробнее о банке Flexnet рассказано в новостной [публикации](#) на нашем сайте.

Обзор вирусной активности для мобильных устройств в марте 2019 года

Угрозы в Google Play

В марте в каталоге Google Play вновь были обнаружены различные вредоносные программы. Среди них — троянцы [Android.FakeApp.152](#) и [Android.FakeApp.162](#), которые загружают мошеннические сайты. На них пользователям за вознаграждение предлагается пройти опросы. Для получения денег потенциальным жертвам якобы необходимо выполнить некий проверочный платеж. На самом деле никакой проверки нет — пользователи лишь переводят средства мошенникам и не получают обещанную награду.

Кроме того, вирусные аналитики выявили очередных троянцев семейства [Android.HiddenAds](#), например [Android.HiddenAds.1133](#), [Android.HiddenAds.1134](#), [Android.HiddenAds.1052](#) и [Android.HiddenAds.379.origin](#). Об аналогичных вредоносных программах наша компания [сообщила](#) в феврале. Эти троянцы распространяются под видом полезных приложений — фото- и видеоредакторов, фильтров для камеры, фонариков, спортивного ПО и т. п.



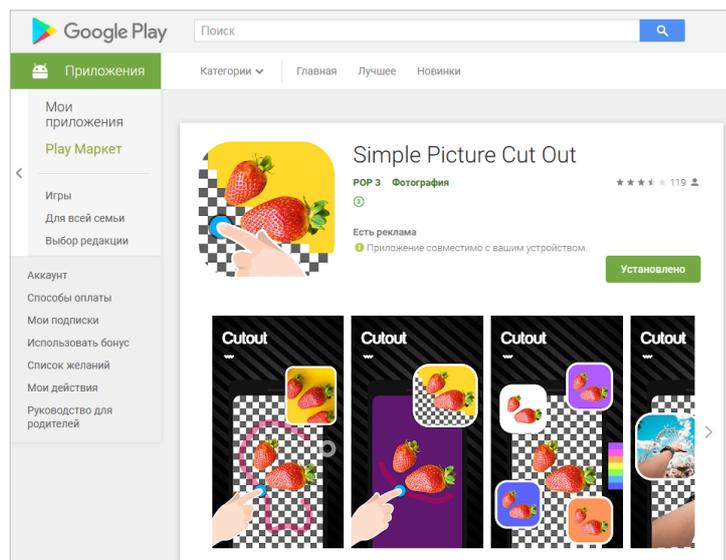
После установки и запуска они скрывают свои значки и начинают постоянно показывать

Узнайте больше

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

Обзор вирусной активности для мобильных устройств в марте 2019 года

Угрозы в Google Play



рекламу поверх других программ и интерфейса операционной системы, мешая нормальной работе с Android-устройствами.

Пользователям Android-устройств угрожают троянцы, которые распространяются не только через вредоносные сайты, но и через официальный каталог ПО Google Play. Для защиты смартфонов и планшетов 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 марте 2019 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»,
2003-2019

Узнайте больше

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