

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



Обзор вирусной активности для мобильных устройств в сентябре 2019 года

9 октября 2019 года

В сентябре пользователям Android-устройств угрожали различные вредоносные программы, многие из которых злоумышленники распространяли через каталог Google Play. Это были загрузчики [Android.DownLoader](#), банковские и рекламные троянцы [Android.Banker](#) и [Android.HiddenAds](#), а также другие угрозы. Кроме того, специалисты «Доктор Веб» обнаружили несколько новых версий потенциально опасных приложений, предназначенных для слежки за пользователями. Среди них — [Program.Panspy.1.origin](#), [Program.RealtimeSpy.1.origin](#) и [Program.MonitorMinor](#).

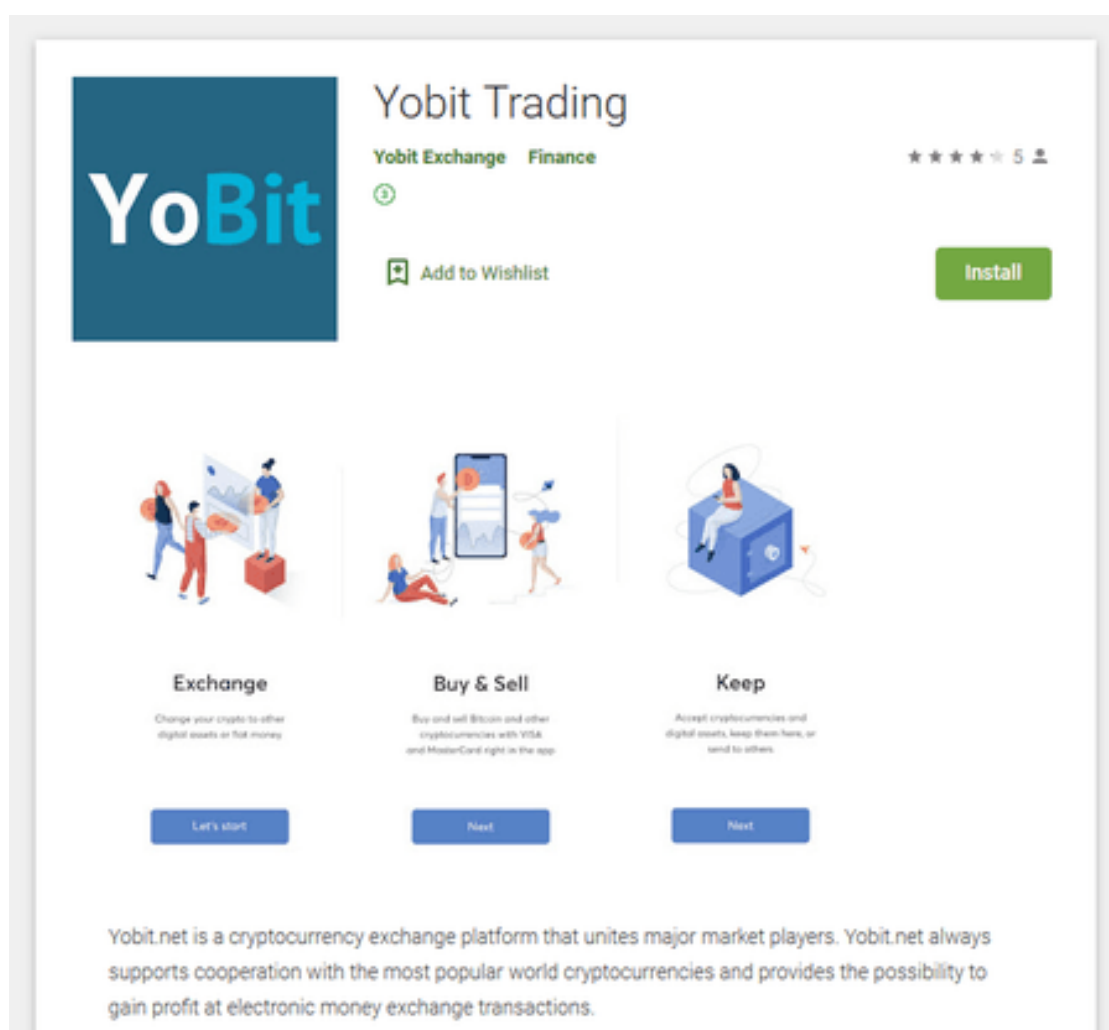
Главные тенденции сентября

- Google Play остается источником вредоносных и нежелательных приложений
- Пользователям по-прежнему угрожает шпионское ПО

Обзор вирусной активности для мобильных устройств в сентябре 2019 года

Мобильная угроза месяца

Одной из выявленных в прошлом месяце вредоносных программ был банковский троянец [Android.Banker.352.origin](#), который распространялся под видом официального приложения криптобиржи YoBit.



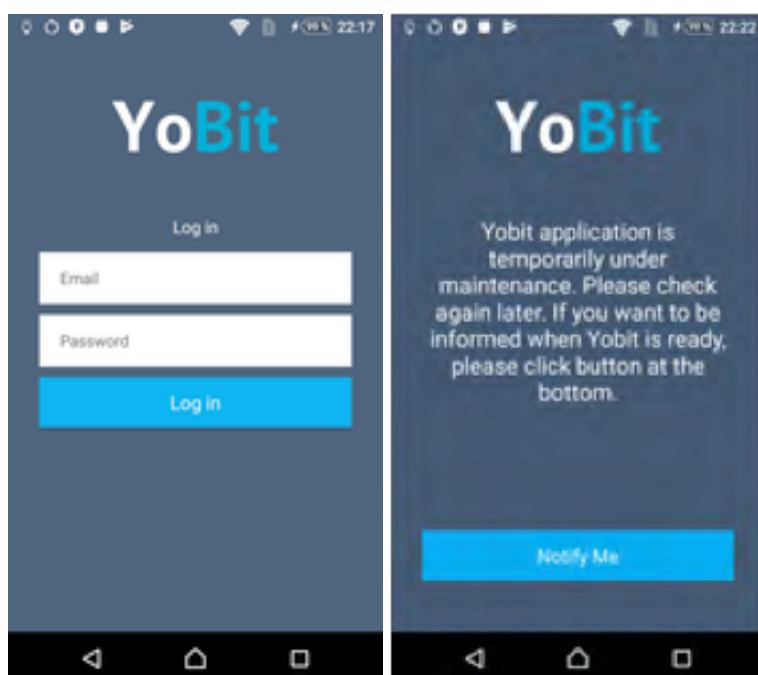
Узнайте больше

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

Обзор вирусной активности для мобильных устройств в сентябре 2019 года

Мобильная угроза месяца

При запуске Android.Banker.352.origin показывал поддельное окно авторизации и похищал вводимые логины и пароли клиентов биржи. После этого он демонстрировал сообщение о временной недоступности сервиса.

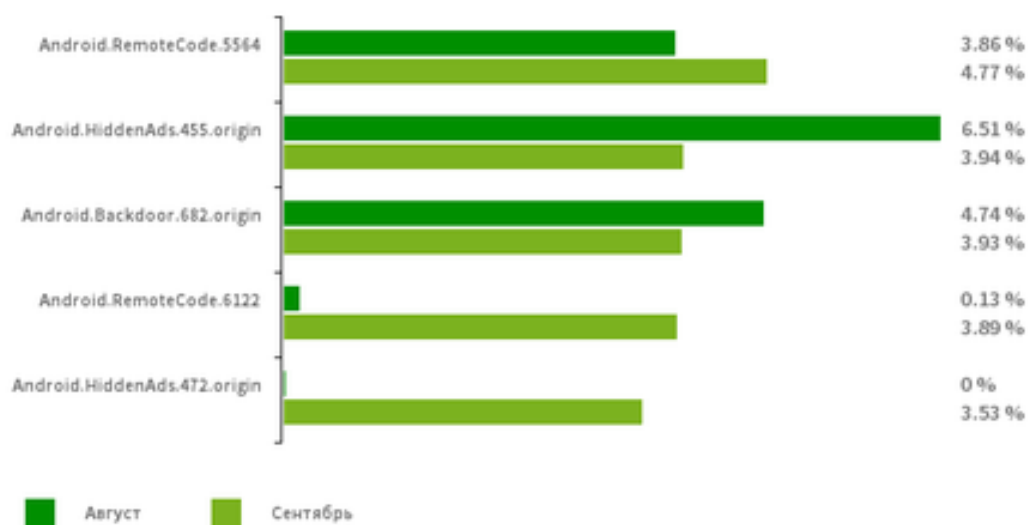


Троянец перехватывал коды двухфакторной аутентификации из СМС, а также коды доступа из email-сообщений. Кроме того, он перехватывал и блокировал уведомления от различных мессенджеров и программ-клиентов электронной почты. Все украденные данные Android.Banker.352.origin сохранял в базу Firebase Database.

Обзор вирусной активности для мобильных устройств в сентябре 2019 года

По данным антивирусных продуктов Dr.Web для Android

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



[Android.RemoteCode.6122](#)

[Android.RemoteCode.5564](#)

Вредоносные приложения для загрузки и выполнения произвольного кода.

[Android.HiddenAds.455.origin](#)

[Android.HiddenAds.472.origin](#) (новая угроза)

Троянцы для показа навязчивой рекламы.

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

Троянец, который выполняет команды злоумышленников и позволяет им контролировать зараженные мобильные устройства.

Обзор вирусной активности для мобильных устройств в сентябре 2019 года

По данным антивирусных продуктов Dr.Web для Android



Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах:

- [Adware.Patacore.253](#)
- [Adware.Gexin.3.origin](#)
- [Adware.Zeus.1](#)
- [Adware.Altamob.1.origin](#)

Потенциально опасная программа для незаметного запуска приложений без вмешательства пользователя:

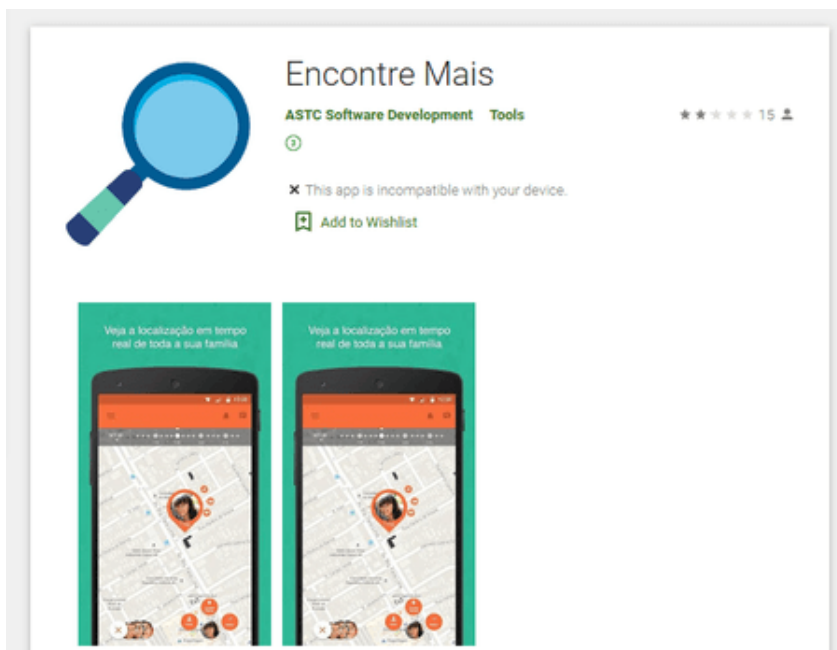
- [Tool.SilentInstaller.6.origin](#)

Обзор вирусной активности для мобильных устройств в сентябре 2019 года

Угрозы в Google Play

Помимо банковского троянца [Android.Banker.352.origin](#) в сентябре специалисты «Доктор Веб» обнаружили в Google Play вредоносную программу [Android.Banker.347.origin](#), нацеленную на бразильских клиентов кредитных организаций. Она является модификацией банков [Android.BankBot.495.origin](#), [Android.Banker.346.origin](#) и других, о которых наша компания сообщала в более ранних [публикациях](#).

Злоумышленники распространяли [Android.Banker.347.origin](#) через Google Play под видом программы для обнаружения местоположения членов семьи.



Банкер использовал специальные возможности ОС Android (Accessibility Service) для кражи информации из СМС-сообщений — например, одноразовых кодов и других секретных данных. Кроме того, как и предыдущие модификации, он мог по команде киберпреступников открывать фишинговые страницы.

В течение месяца вирусные аналитики выявили в Google Play несколько новых рекламных троянцев семейства [Android.HiddenAds](#) — например, [Android.HiddenAds.444.origin](#). Эта вредоносная программа скрывалась в безобидных программах и играх. После запуска она скрывала значок приложения и начинала показывать надоедливые рекламные баннеры. Кроме того, по команде управляющего сервера она загружала и пыталась установить APK-файлы.

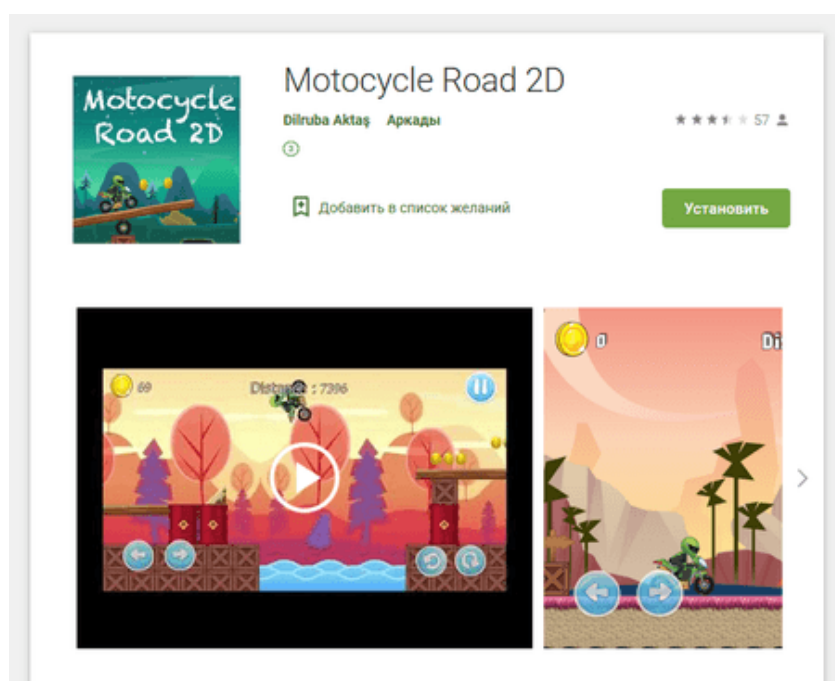
Узнайте больше

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

Обзор вирусной активности для мобильных устройств в сентябре 2019 года

Угрозы в Google Play

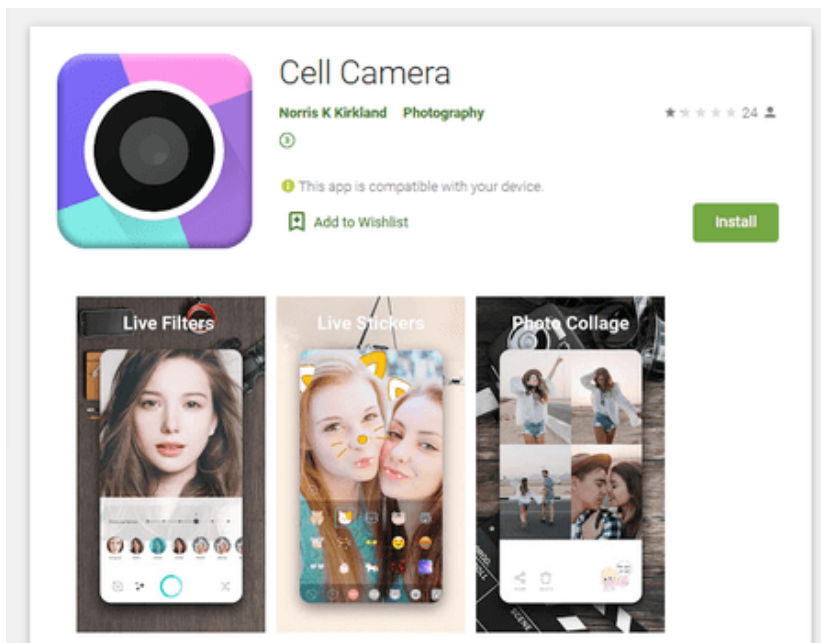
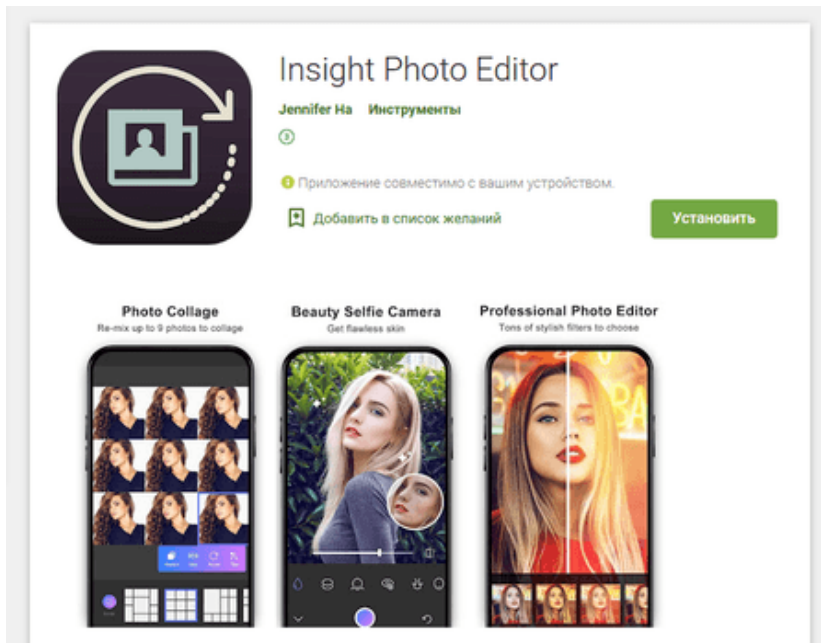
Среди обнаруженных вредоносных программ были и троянцы-загрузчики, такие как [Android.DownLoader.920.origin](#) и [Android.DownLoader.921.origin](#). Они распространялись под видом игр. Троянцы по команде сервера скачивали и пытались установить различное ПО, а также другие вредоносные программы.



В течение сентября в Google Play было найдено несколько модификаций троянцев семейства [Android.Joker](#). Эти вредоносные приложения скрывались в безобидных, на первый взгляд, программах — плагинах для фотокамер, фоторедакторах, сборниках изображений, различных системных утилитах и другом ПО.

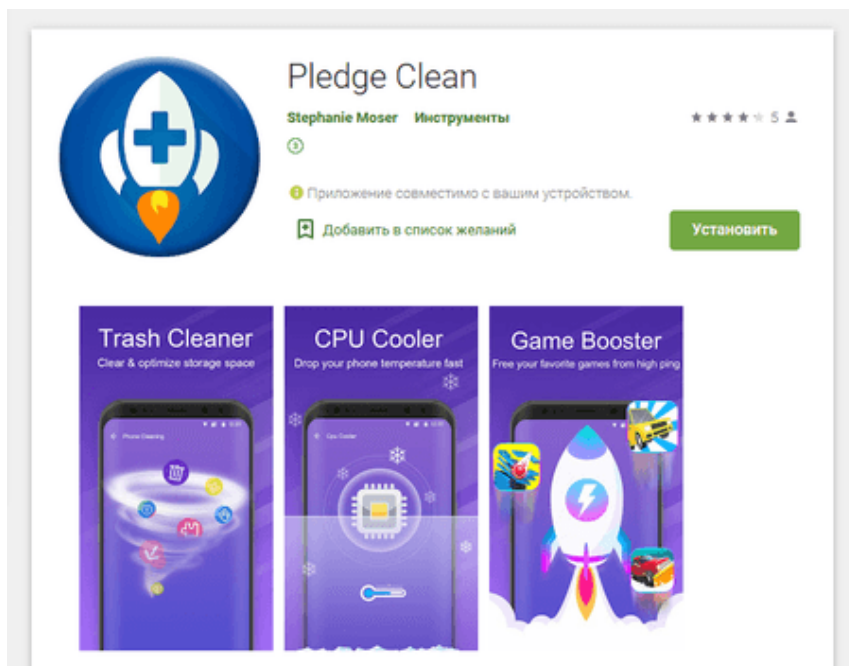
Обзор вирусной активности для мобильных устройств в сентябре 2019 года

Угрозы в Google Play



Обзор вирусной активности для мобильных устройств в сентябре 2019 года

Угрозы в Google Play

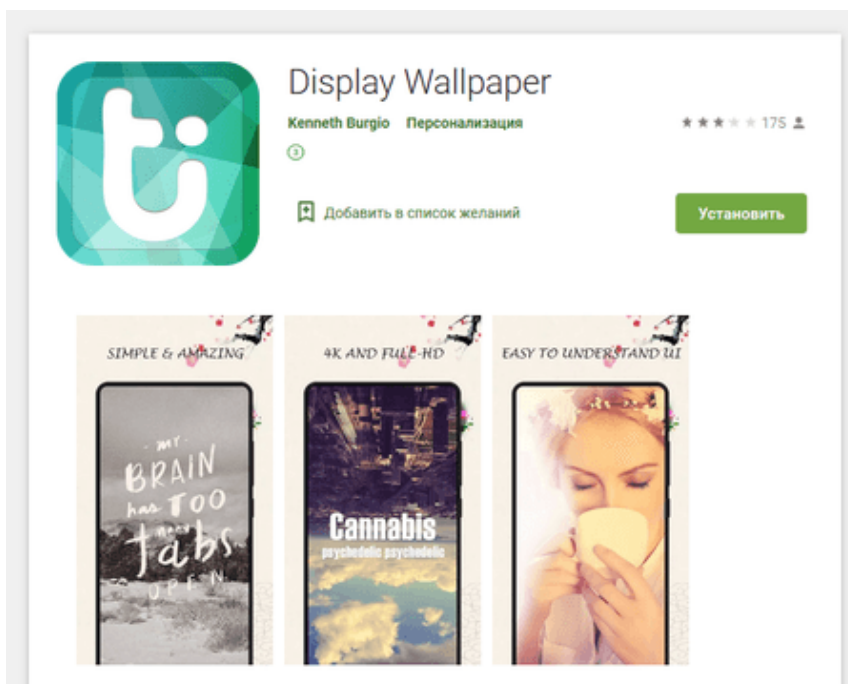
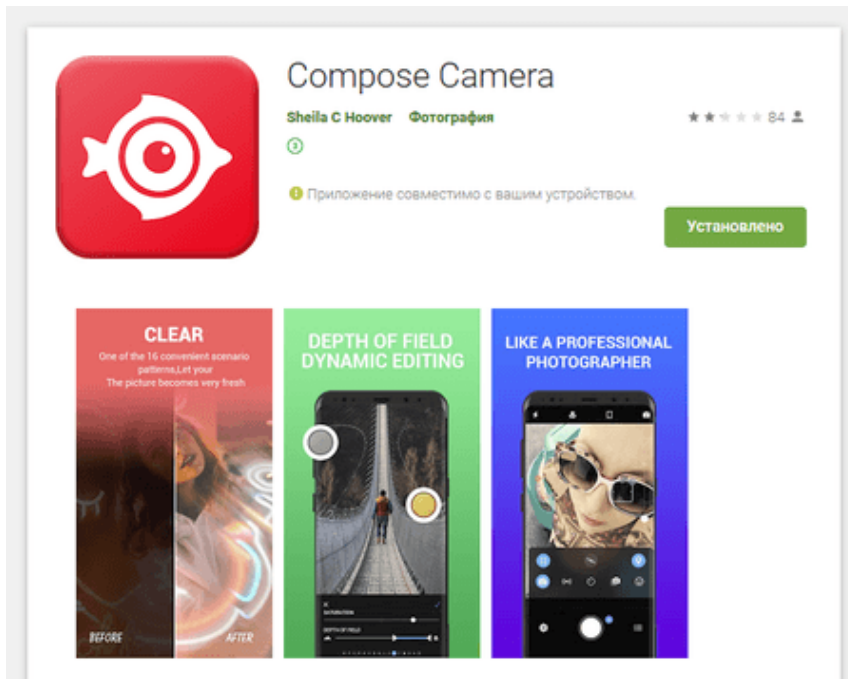


Узнайте больше

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

Обзор вирусной активности для мобильных устройств в сентябре 2019 года

Угрозы в Google Play

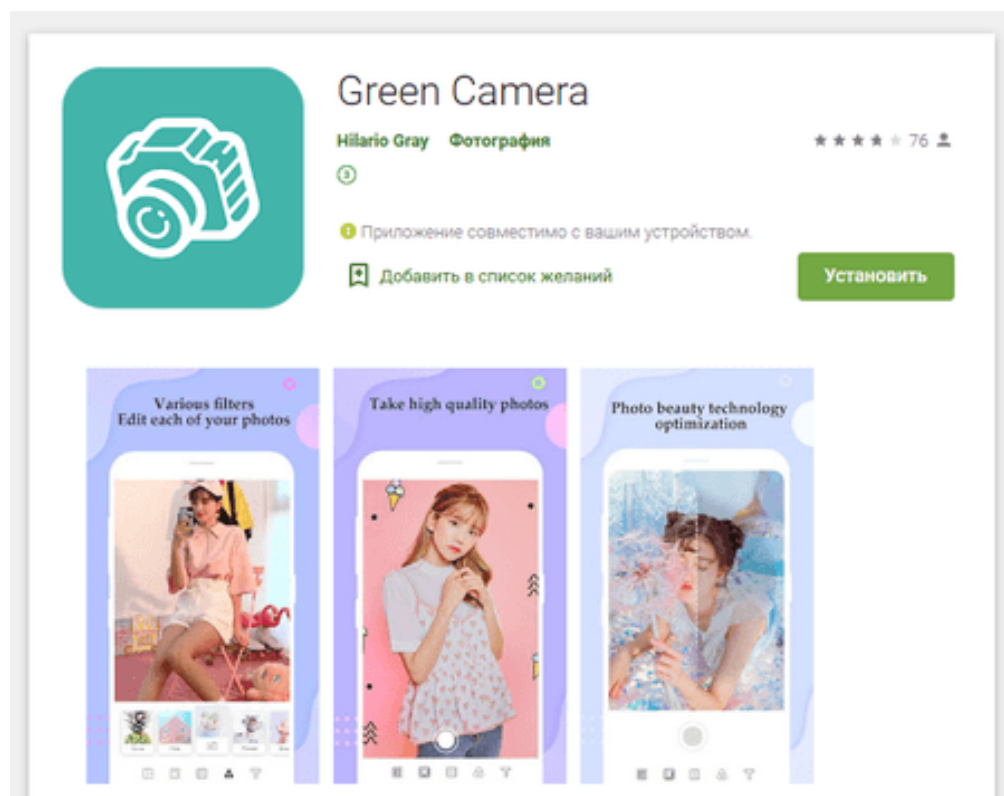


Обзор вирусной активности для мобильных устройств в сентябре 2019 года

Угрозы в Google Play

Троянцы способны загружать и запускать вспомогательные dex-файлы, а также выполнять произвольный код. Помимо этого, они автоматически подписывают пользователей на дорогостоящие услуги, для чего загружают веб-сайты с премиум-контентом и самостоятельно переходят по необходимым ссылкам. А чтобы подтвердить подписку, они перехватывают проверочные коды из СМС. Кроме того, вредоносные программы [Android.Joker](#) передают на управляющий сервер данные из телефонных книг своих жертв.

Другие троянцы, которые подписывали пользователей на дорогостоящие услуги, получили имена [Android.Click.781](#) и [Android.Click.325.origin](#). Они также загружали сайты, где автоматически подключали жертвам премиум-сервисы. Кроме того, по команде сервера они могли перехватывать уведомления, поступающие от операционной системы и других программ. Злоумышленники распространяли этих троянцев под видом приложений-фотокамер.



Узнайте больше

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

Обзор вирусной активности для мобильных устройств в сентябре 2019 года

Шпионское ПО

В сентябре специалисты «Доктор Веб» обнаружили несколько новых версий потенциально опасных программ, предназначенных для слежки за владельцами Android-устройств. Среди них были приложения [Program.Panspy.1.origin](#), [Program.RealtimeSpy.1.origin](#) и [Program.MonitorMinor](#). Это шпионское ПО позволяет контролировать СМС-переписку и телефонные звонки, общение в популярных мессенджерах, отслеживать местоположение устройств, а также получать другую конфиденциальную информацию.

Для защиты Android-устройств от вредоносных и нежелательных программ пользователям следует установить антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных устройств в сентябре 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.drweb.ru | www.антивирус.рф | 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](#)