Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2020 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2020 года

19 марта 2020 года

В феврале на Android-устройствах было зафиксировано на 11,57% меньше угроз по сравнению с январем. Число обнаруженных вредоносных программ сократилось на 11,05%. В числе самых активных вновь оказались трояны, загружающие другие вредоносные приложения и способные выполнять произвольный код.

Количество выявленных нежелательных программ увеличилось на 0,48%. При этом число детектирований рекламных приложений снизилось на 11%, а потенциально опасного ПО — на 2,56%.

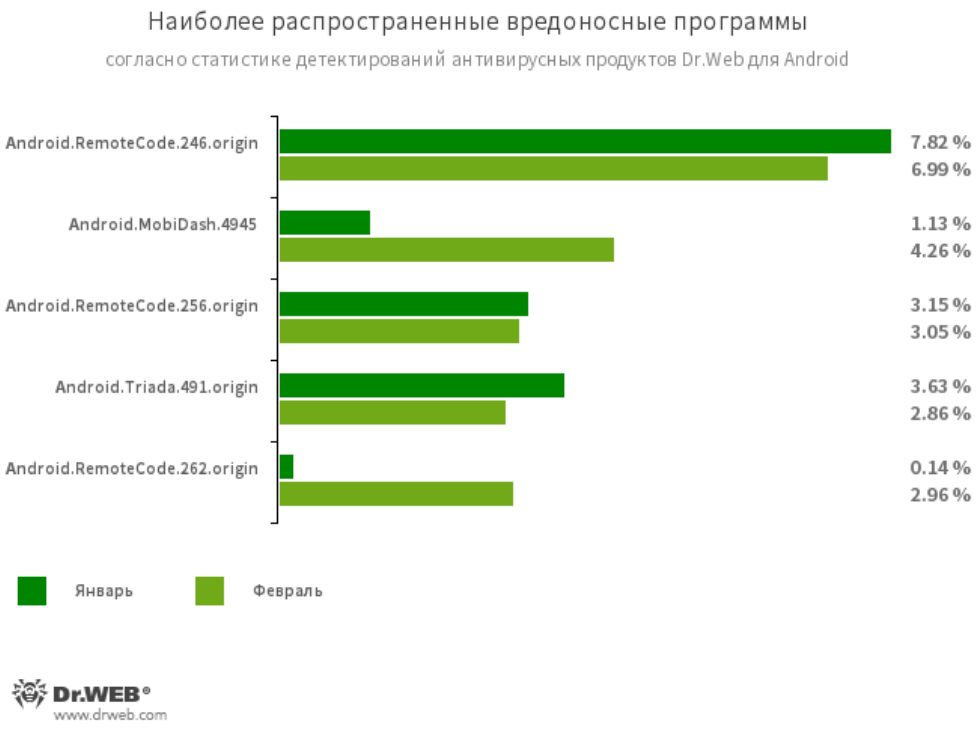
В каталоге Google Play наши специалисты выявили новые модификации рекламных троянов семейства Android.HiddenAds и мошеннических вредоносных приложений семейства Android.FakeApp. Были обнаружены и другие угрозы.

ГЛАВНЫЕ ТЕНДЕНЦИИ ФЕВРАЛЯ

- Снижение общего числа угроз, обнаруженных на Android-устройствах
- Появление новых вредоносных программ в Google Play

«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2020 года

По данным антивирусных продуктов Dr.Web для Android

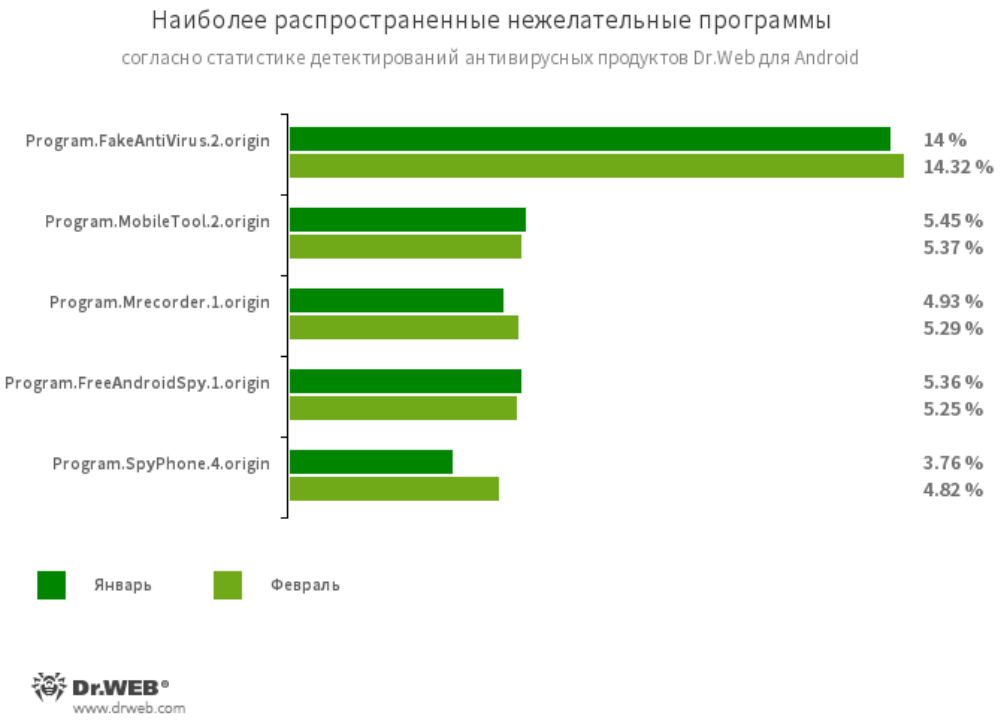


..

Android.RemoteCode.246.origin
Android.RemoteCode.256.origin
Android.RemoteCode.262.origin
Вредоносные программы, которые загружают и выполняют произвольный код.
Android.MobiDash.4945
Троянская программа, показывающая рекламу.
Android.Triada.491.origin
Многофункциональный троян, выполняющий разнообразные вредоносные действия.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2020 года

По данным антивирусных продуктов Dr.Web для Android



Program.FakeAntiVirus.2.origin

Детектирование рекламных программ, которые имитируют работу антивирусного ПО.

Program.MobileTool.2.origin

Program.Mrecorder.1.origin

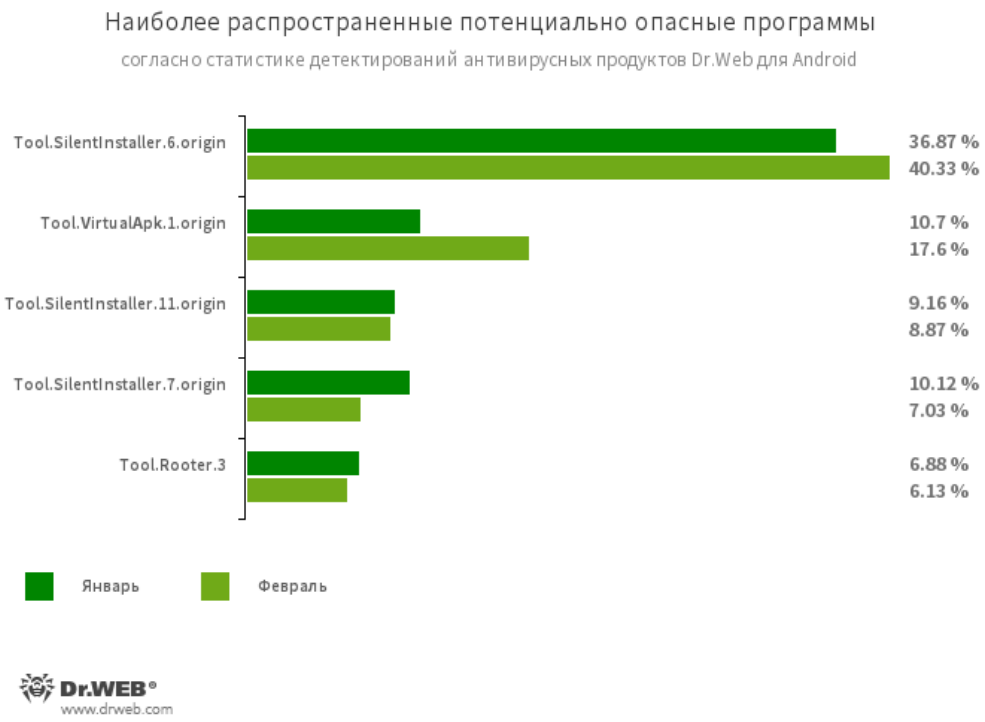
Program.FreeAndroidSpy.1.origin

Program.SpyPhone.4.origin

Приложения, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2020 года

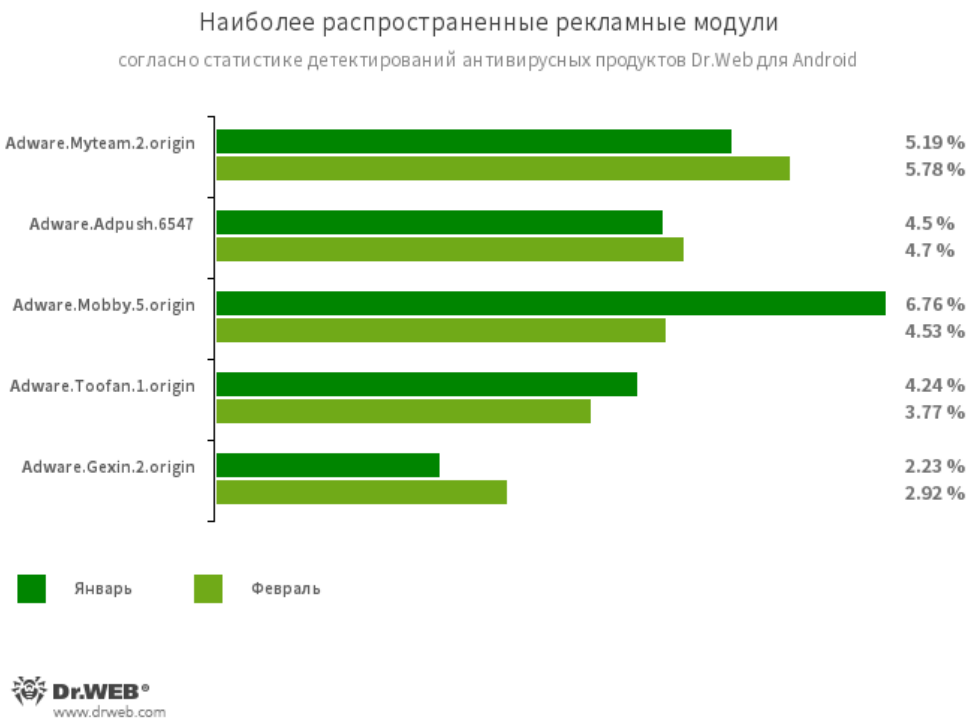
По данным антивирусных продуктов Dr.Web для Android



Tool.SilentInstaller.6.origin
Tool.SilentInstaller.7.origin
Tool.SilentInstaller.11.origin
Tool.VirtualApk.1.origin
Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки.
Tool.Rooter.3
Утилита для получения root-полномочий на Android-устройствах. Может использоваться злоумышленниками и вредоносными программами.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2020 года

По данным антивирусных продуктов Dr.Web для Android

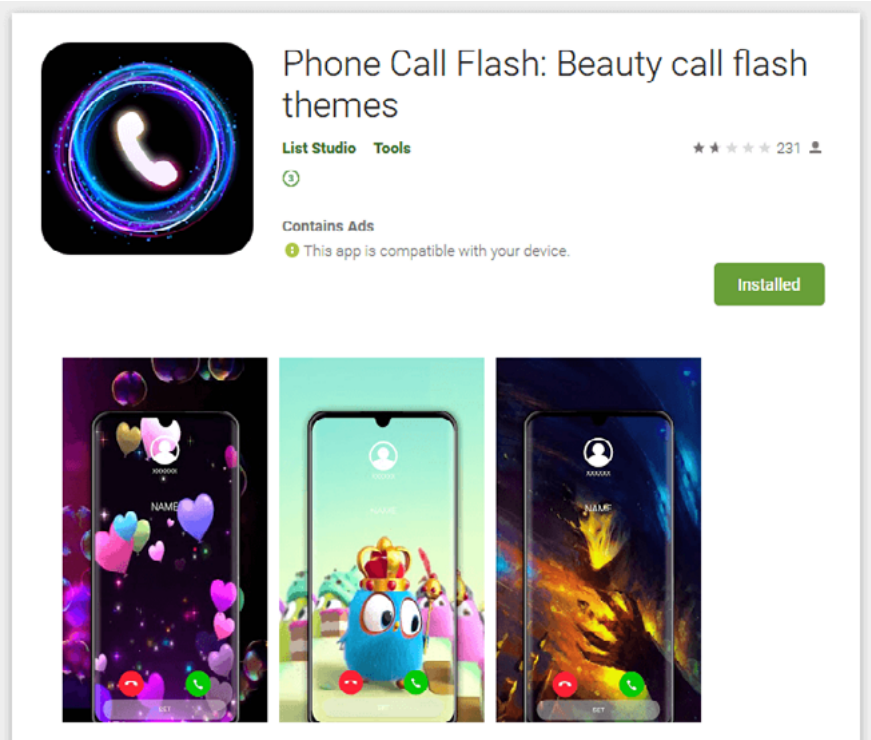


Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах:

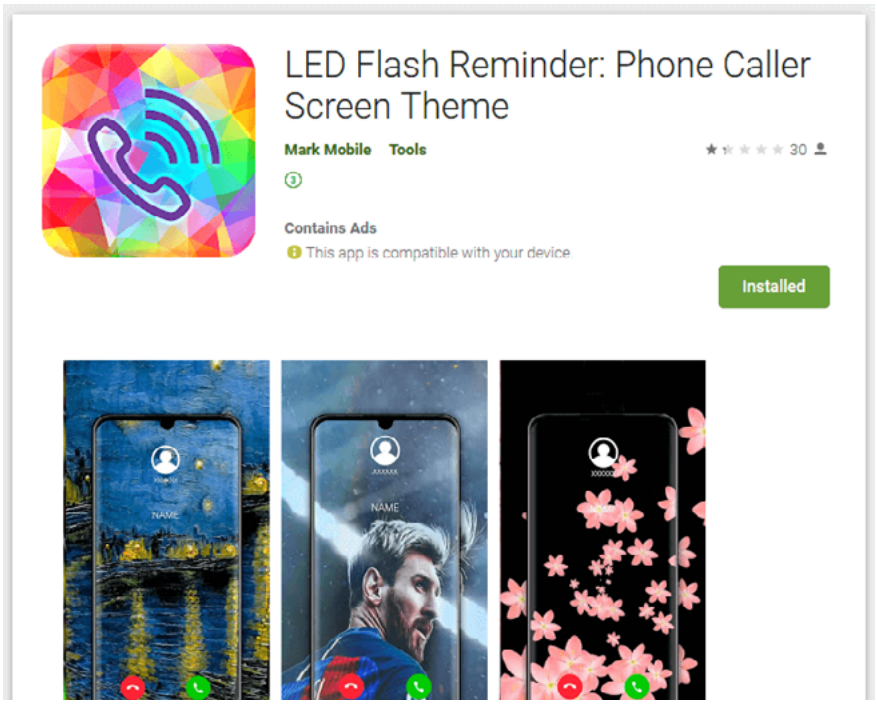
- Adware.Myteam.2.origin
- Adware.Mobby.5.origin
- Adware.Adpush.6547
- Adware.Toofan.1.origin
- Adware.Gexin.2.origin

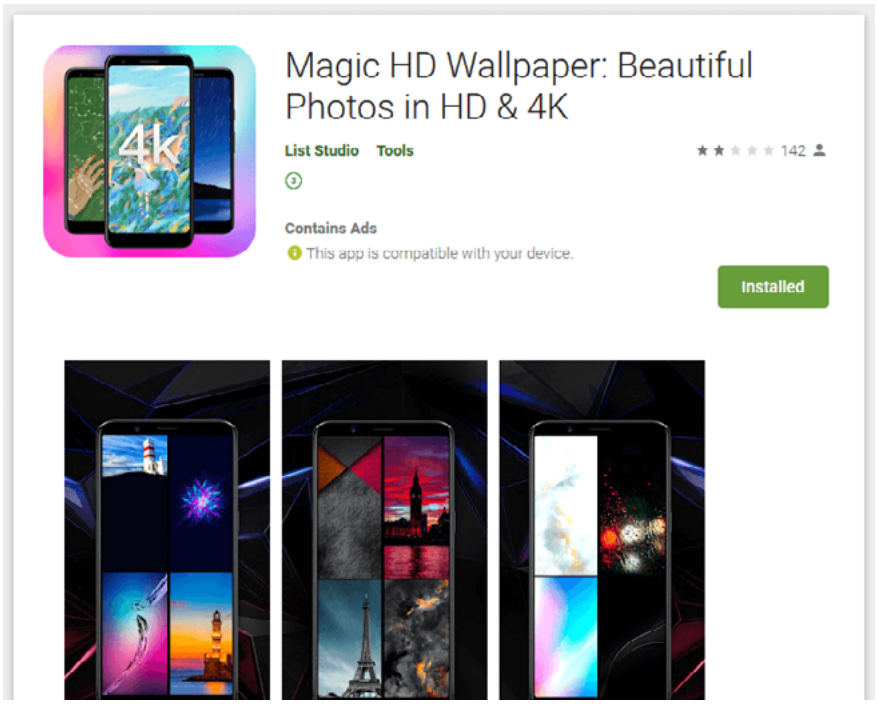
Угрозы в Google Play

В феврале наши специалисты обнаружили в каталоге Google Play несколько новых угроз. В их числе – трояны семейства Android.HiddenAds, получившие имена Android.HiddenAds.2065, Android.HiddenAds.2066 и Android.HiddenAds2067.
После запуска они скрывали свой значок из списка приложений на главном экране и постоянно показывали надоедливую рекламу. Злоумышленники распространяли их под видом безобидных программ — сборников изображений, фоторедакторов и полезных утилит.

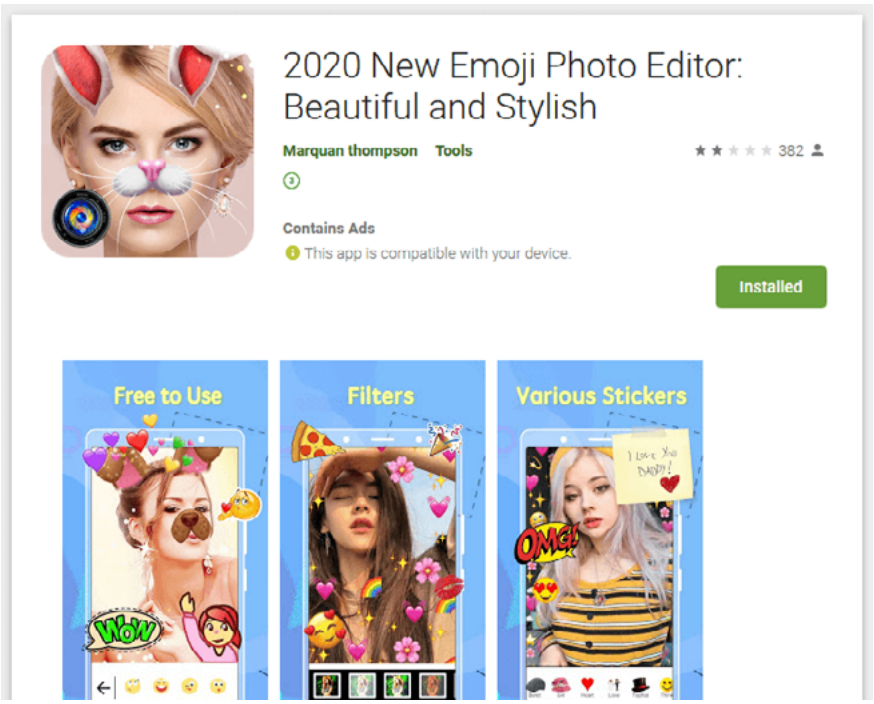


Угрозы в Google Play

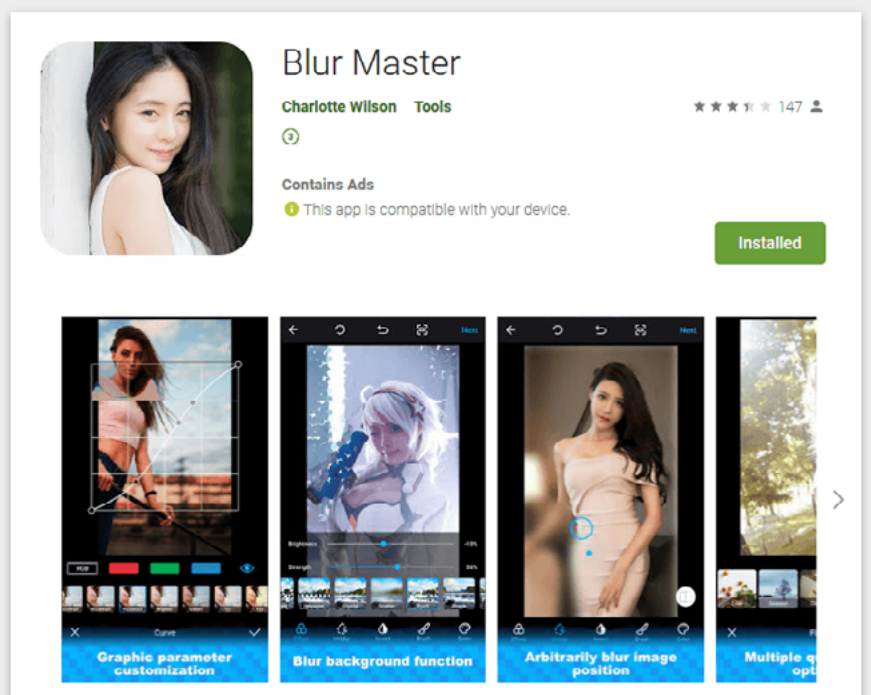




Угрозы в Google Play

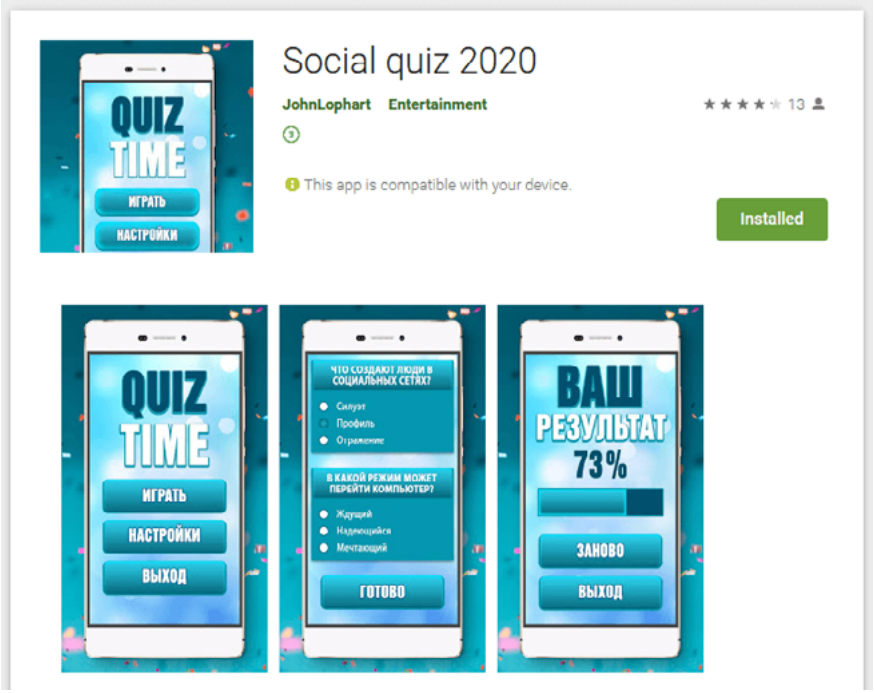


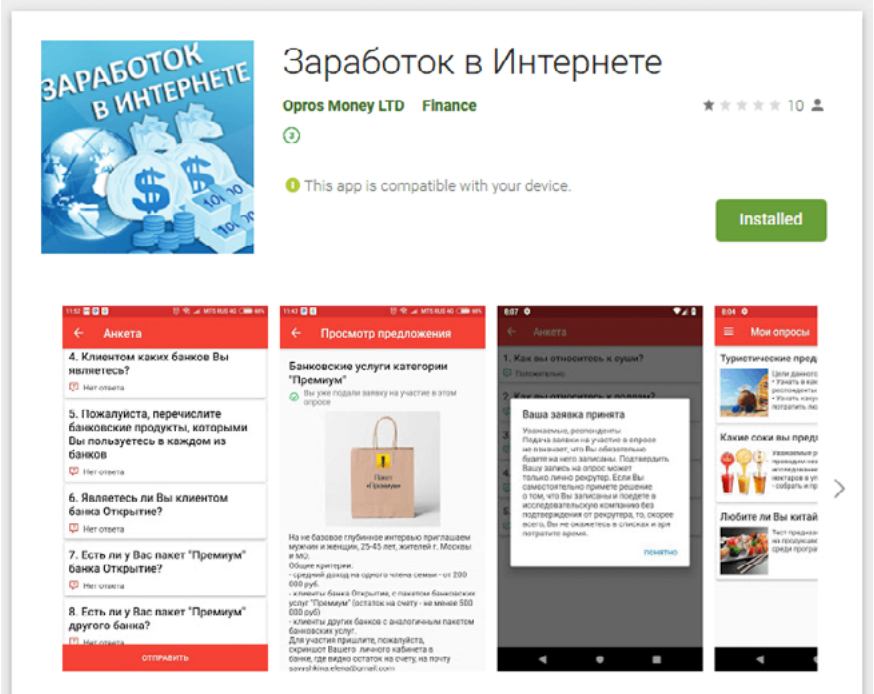
Угрозы в Google Play



Кроме того, были выявлены новые вредоносные приложения семейства Android.FakeApp, добавленные в вирусную базу Dr.Web как Android.FakeApp.189, Android.FakeApp.4.origin. Злоумышленники выдавали их за программы для заработка в Интернете. Трояны загружали мошеннические веб-сайты, где потенциальным жертвам за «вознаграждение» предлагалось принять участие в различных опросах. Для получения гонорара от них требовалось подтвердить свою личность или оплатить комиссию, предоставив данные банковской карты, либо отправив деньги на указанный мошенниками онлайн-кошелек. В результате пользователи могли не только потерять запрошенную сумму, но и лишиться всех средств на банковском счете.

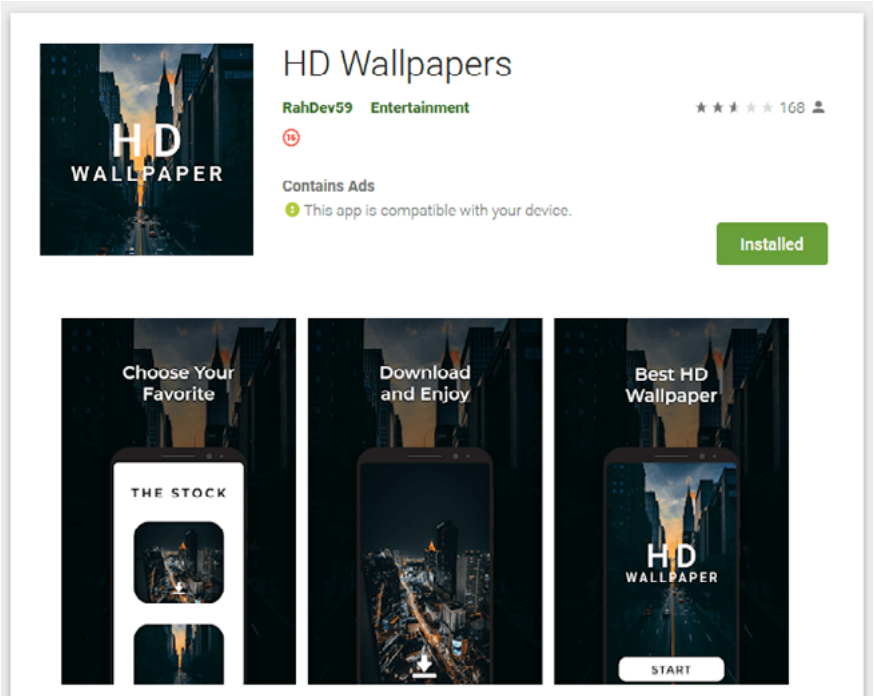
Угрозы в Google Play





Угрозы в Google Play

Кроме того, наши специалисты обнаружили трояна-кликера Android.Click.878, распространявшегося под видом сборника изображений. После запуска он загружал в Gogle Chrome различные веб-сайты, среди которых были и мошеннические. Чтобы скрыться от пользователя, Android.Click.878 убирал свой значок из списка приложений в меню главного экрана. После этого найти трояна можно было только в списке установленных программ в меню операционной системы, где кликер выдавал себя за системное приложение с именем Settings и значком шестеренки.



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

«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2020 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.drweb.ru | www.антивирус.рф | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах