



«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.

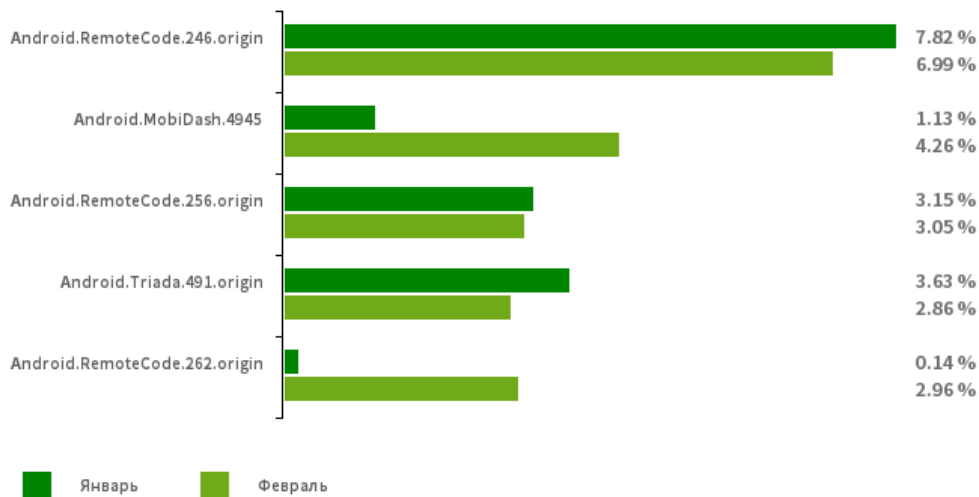
ГЛАВНЫЕ ТЕНДЕНЦИИ ФЕВРАЛЯ

- 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

Наиболее распространенные вредоносные программы
согласно статистике детектирований 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.

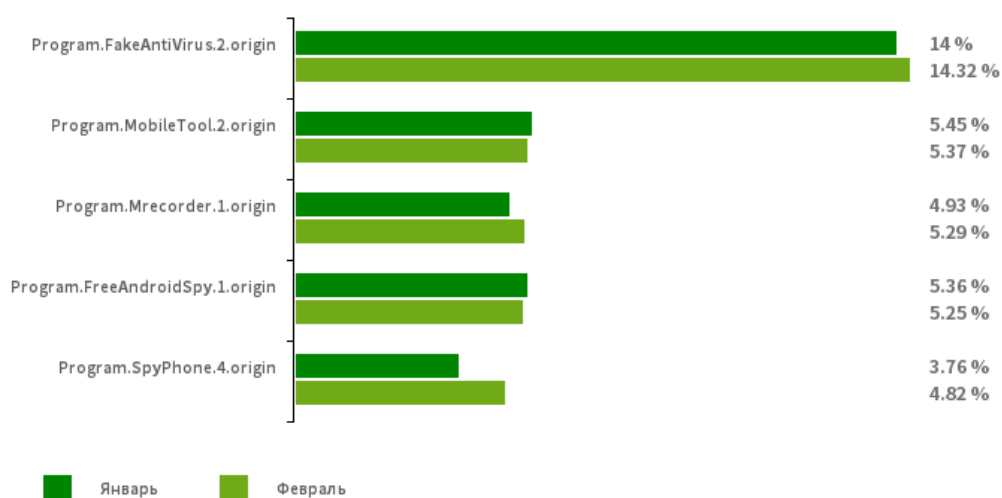
[Android.Triada.491.origin](#)

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

Наиболее распространенные нежелательные программы
согласно статистике детектирования 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](#)

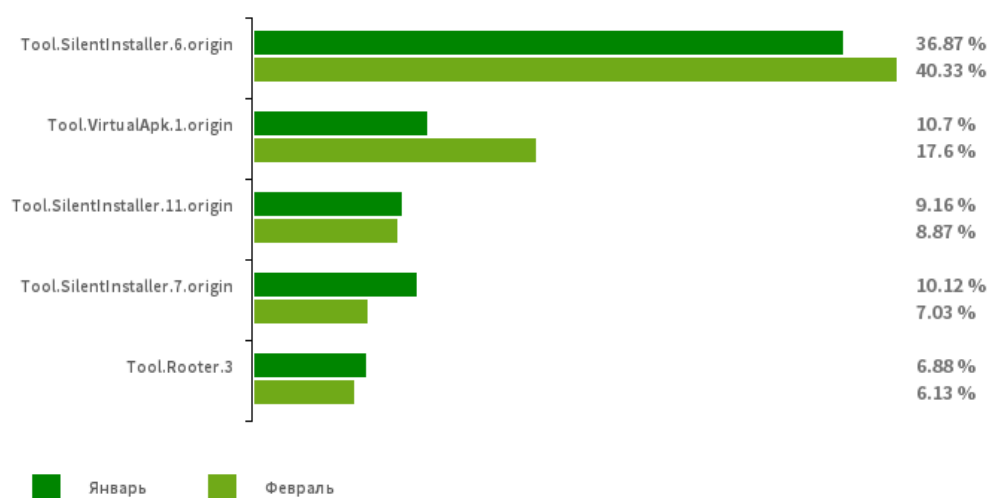
Приложения, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа.

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

По данным антивирусных продуктов Dr.Web для Android

Наиболее распространенные потенциально опасные программы

согласно статистике детектирования 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 арк-файлы без их установки.

Tool.Rooters.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:

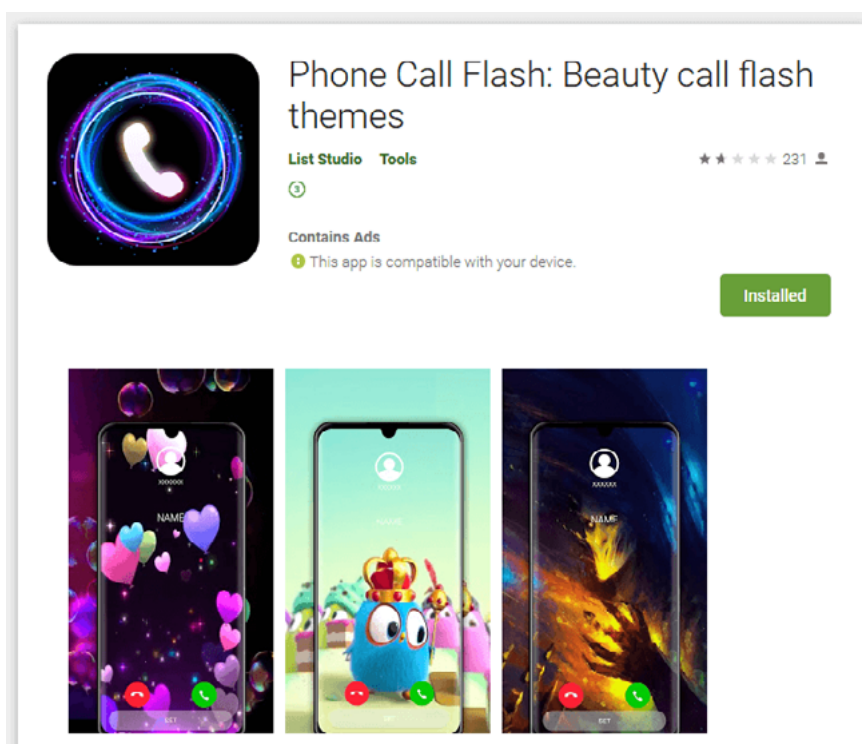
- Adware.Myteam.2.origin
- Adware.Mobby.5.origin
- Adware.Adpush.6547
- Adware.Toofan.1.origin
- Adware.Gexin.2.origin

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

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.

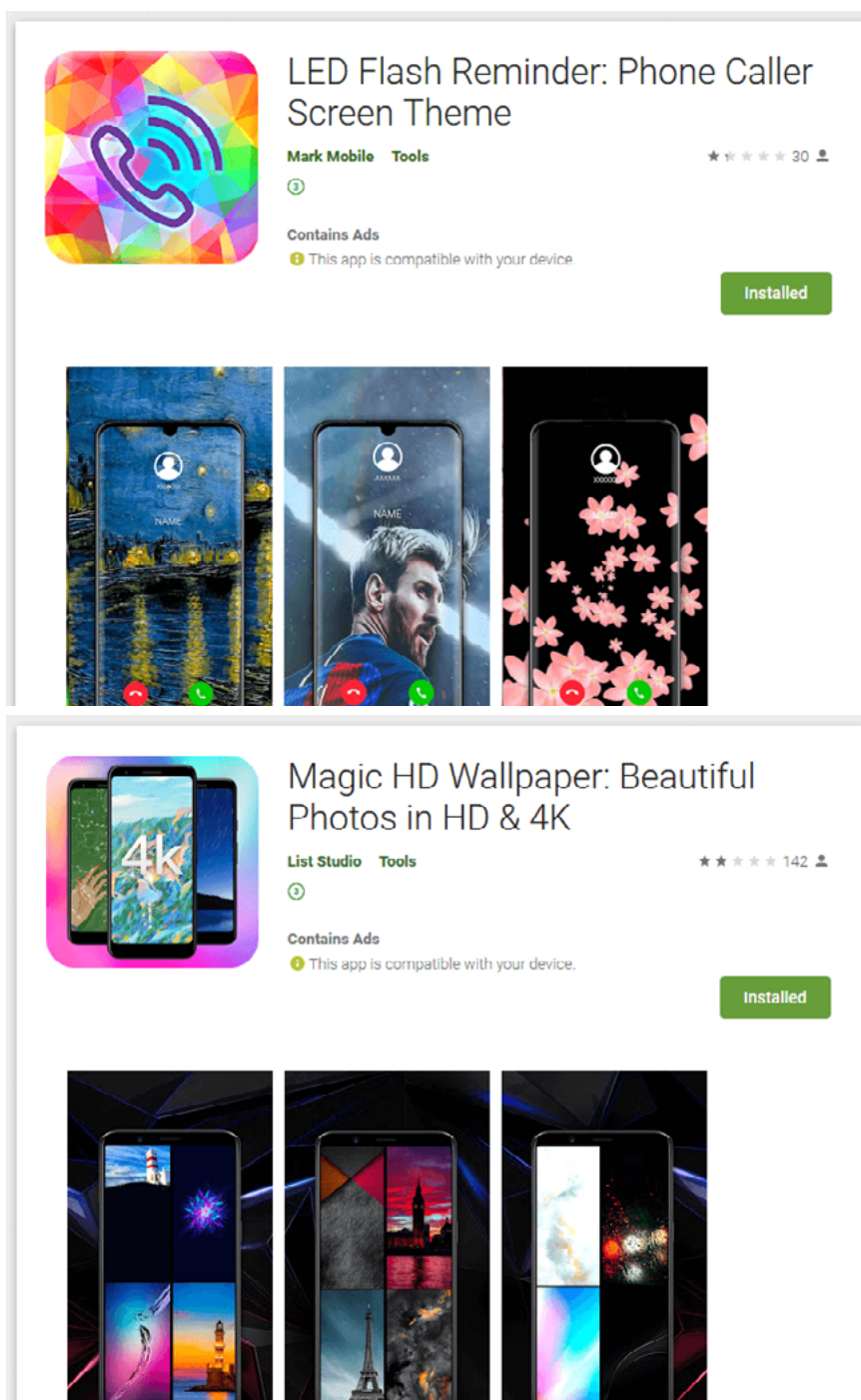


Узнайте больше

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

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

Угрозы в Google Play

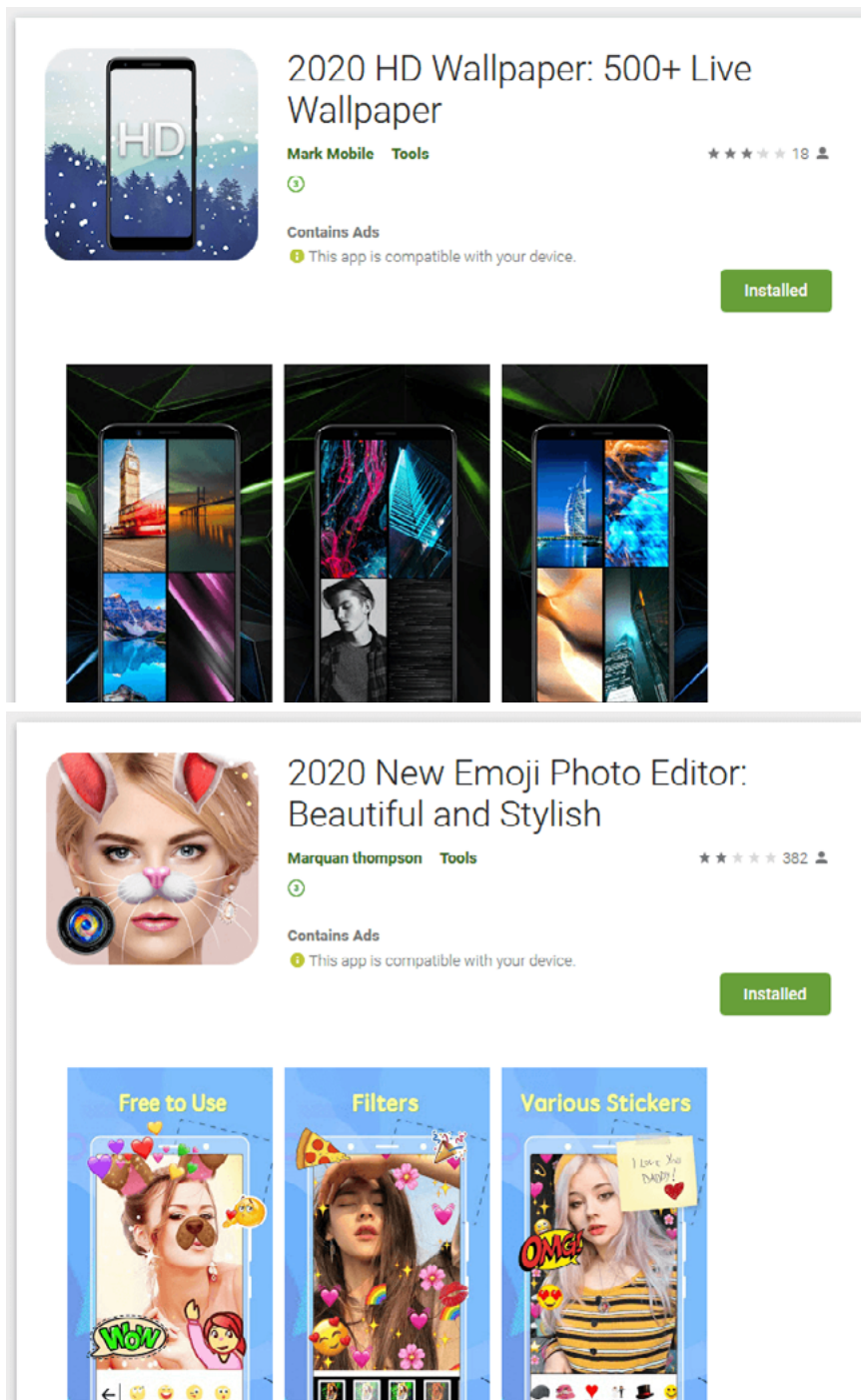


The screenshot displays two app listings from the Google Play Store. The first app, 'LED Flash Reminder: Phone Caller Screen Theme' by Mark Mobile, has a colorful geometric icon and a rating of 30 stars. The second app, 'Magic HD Wallpaper: Beautiful Photos in HD & 4K' by List Studio, has a 4K icon and a rating of 142 stars. Both apps include a 'Contains Ads' warning and a green 'Installed' button. Below each app listing are three preview images showing the app's interface on a smartphone screen.

Узнайте больше

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

Угрозы в Google Play



The screenshot displays two app listings from the Google Play Store. The first app, '2020 HD Wallpaper: 500+ Live Wallpaper', is developed by 'Mark Mobile Tools' and has a 5-star rating from 18 users. It is marked as 'Contains Ads' and is compatible with the device. The second app, '2020 New Emoji Photo Editor: Beautiful and Stylish', is developed by 'Marquan thompson Tools' and has a 5-star rating from 382 users. It is also marked as 'Contains Ads' and is compatible with the device. Both apps are shown as 'Installed'.

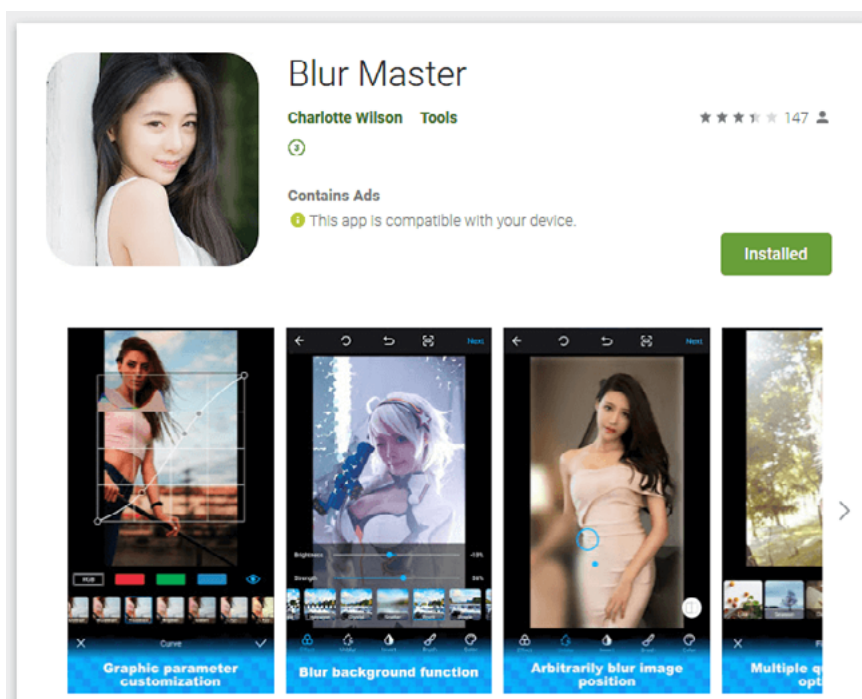
2020 HD Wallpaper: 500+ Live Wallpaper
Mark Mobile Tools ★★★★★ 18
Contains Ads
This app is compatible with your device. Installed

2020 New Emoji Photo Editor: Beautiful and Stylish
Marquan thompson Tools ★★★★★ 382
Contains Ads
This app is compatible with your device. Installed

Узнайте больше

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

Угрозы в Google Play



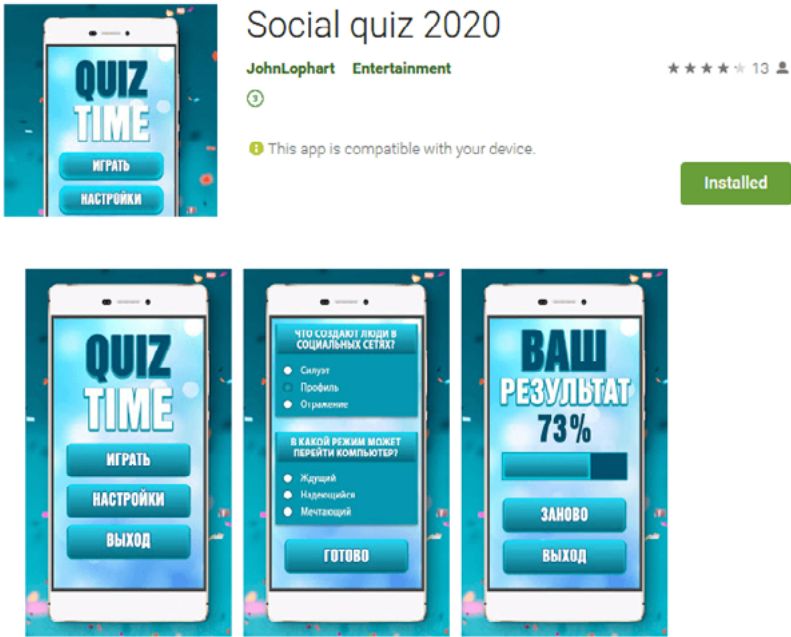
Кроме того, были выявлены новые вредоносные приложения семейства [Android.FakeApp](#), добавленные в вирусную базу Dr.Web как [Android.FakeApp.189](#), [Android.FakeApp.4.origin](#). Злоумышленники выдавали их за программы для заработка в Интернете. Трояны загружали мошеннические веб-сайты, где потенциальным 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.

Узнайте больше

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

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

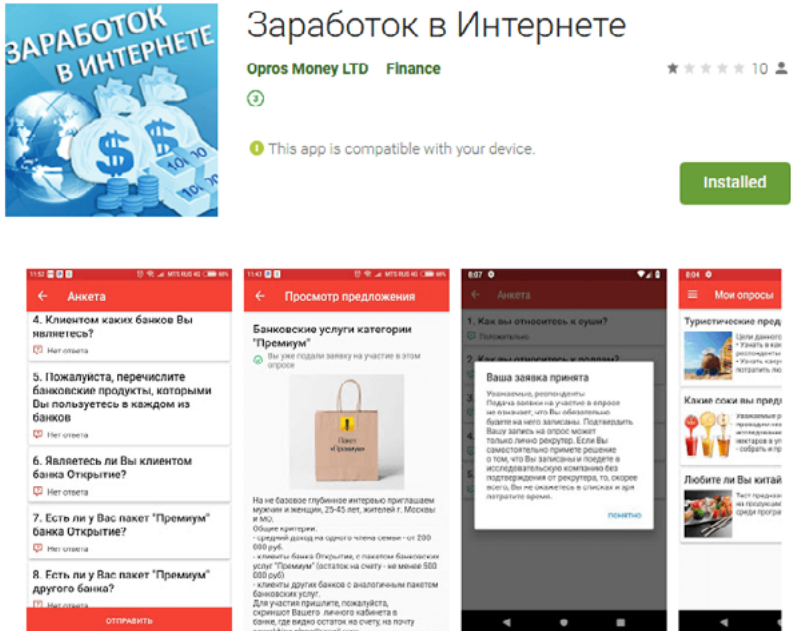
Угрозы в Google Play



Social quiz 2020
JohnLophart Entertainment ★★★★★ 1.0

This app is compatible with your device.

Installed



Заработок в Интернете
Opros Money LTD Finance ★★★★★ 1.0

This app is compatible with your device.

Installed

4. Клиентом каких банков Вы являетесь?
5. Пожалуйста, перечислите банковские продукты, которыми Вы пользуетесь в каждом из банков
6. Являетесь ли Вы клиентом банка Открытие?
7. Есть ли у Вас пакет "Премиум" банка Открытие?
8. Есть ли у Вас пакет "Премиум" другого банка?

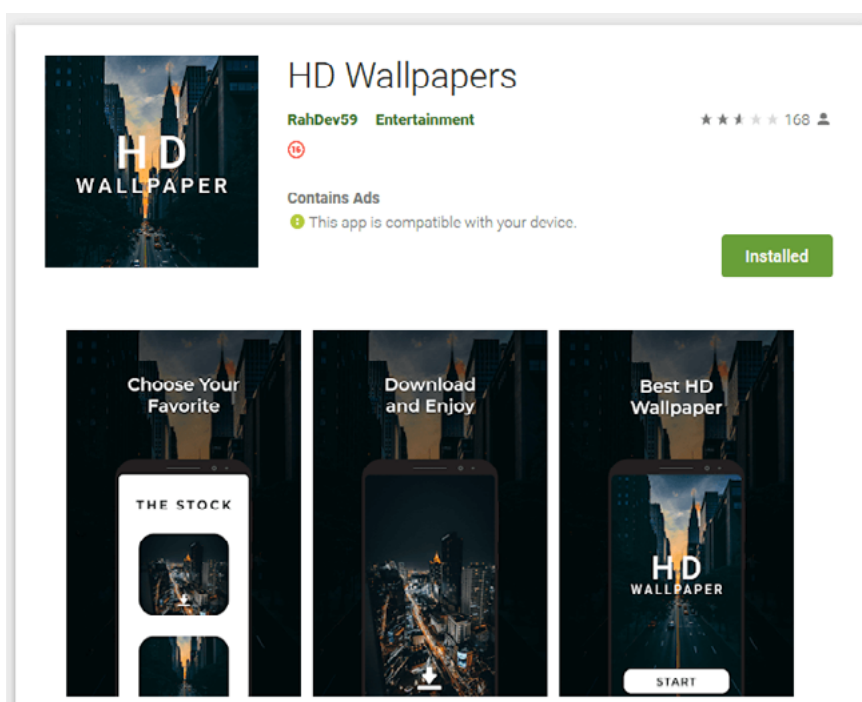
Ваша заявка принята
Уважаемые, рекомендовано...
1. Как вы относитесь к ушам?
2. Как вы относитесь к слепым?

Узнайте больше

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

Угрозы в Google Play

Кроме того, наши специалисты обнаружили трояна-кликера [Android.Click.878](#), распространявшегося под видом сборника изображений. После запуска он загружал в Google 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

[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»,
2003-2020

Узнайте больше

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