Dr.WEB®
с 1992 года

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

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

19 июня 2020 года

В мае на Android-устройствах было обнаружено на 3,35% больше угроз по сравнению с апрелем. Число выявленных вредоносных программ выросло на 3,75%, потенциально опасных программ — на 8,77%, а рекламных приложений — на 1,62%. При этом количество нежелательных программ, проникших на устройства, снизилось на 1,77%.

В конце месяца компания «Доктор Веб» предупредила о распространении трояна Android.FakeApp.176, которого мошенники выдавали за мобильную версию игры Valorant. С помощью этой вредоносной программы вирусописатели зарабатывали, участвуя в различных партнерских программах.

В каталоге Google Play были найдены новые модификации троянов семейства Android.Joker, которые выполняли произвольный код и могли подписывать владельцев Android-устройств на платные мобильные услуги. Там же вирусные аналитики обнаружили несколько новых модификаций вредоносных программ семейства Android.HiddenAds, предназначенных для показа рекламы. Были найдены приложения с несколькими нежелательными рекламными модулями и очередной троян из семейства Android.Circle. Последний также показывал рекламу, мог выполнять скрипты BeanShell и загружал различные сайты, где нажимал на расположенные на них ссылки и баннеры. В течение месяца злоумышленники распространяли и другие угрозы.

ГЛАВНЫЕ ТЕНДЕНЦИИ МАЯ

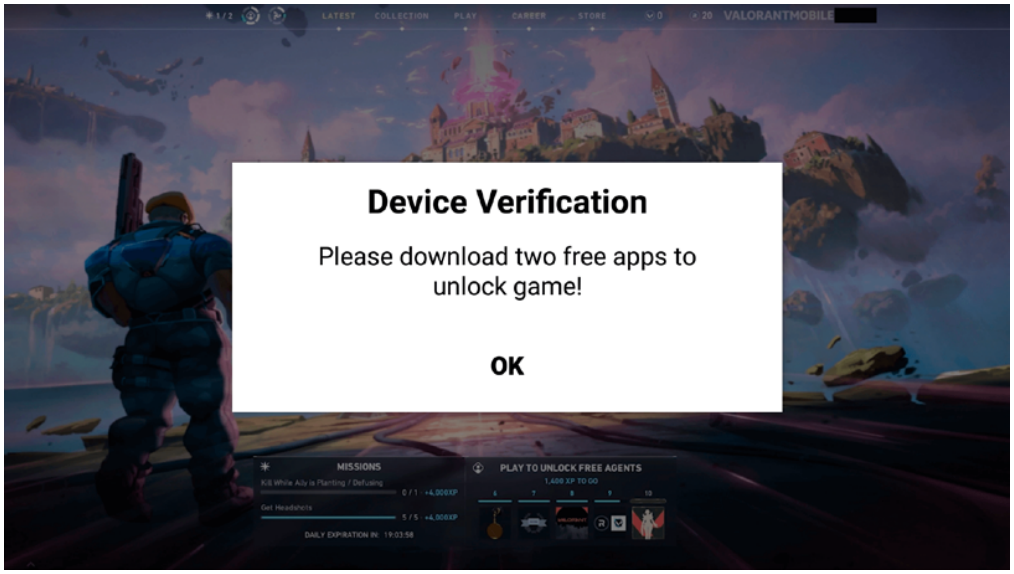
- Незначительный рост общего числа угроз, выявленных на Android-устройствах
- Появление новых угроз в каталоге Google Play

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

Угроза месяца

В мае компания «Доктор Веб» сообщила об обнаружении поддельной мобильной версии игры Valorant, которая на самом деле являлась одной из модификаций трояна Android.FakeApp.176. Злоумышленники уже давно распространяют его под видом известных приложений и используют для незаконного заработка от участия в различных партнерских программах.

Для получения полного доступа к игре троян предлагает потенциальным жертвам выполнить несколько заданий на сайте партнерского сервиса, например, установить и запустить другие игры. За каждое успешно выполненное задание мошенники получают вознаграждение, а обманутые пользователи не получают ничего.



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

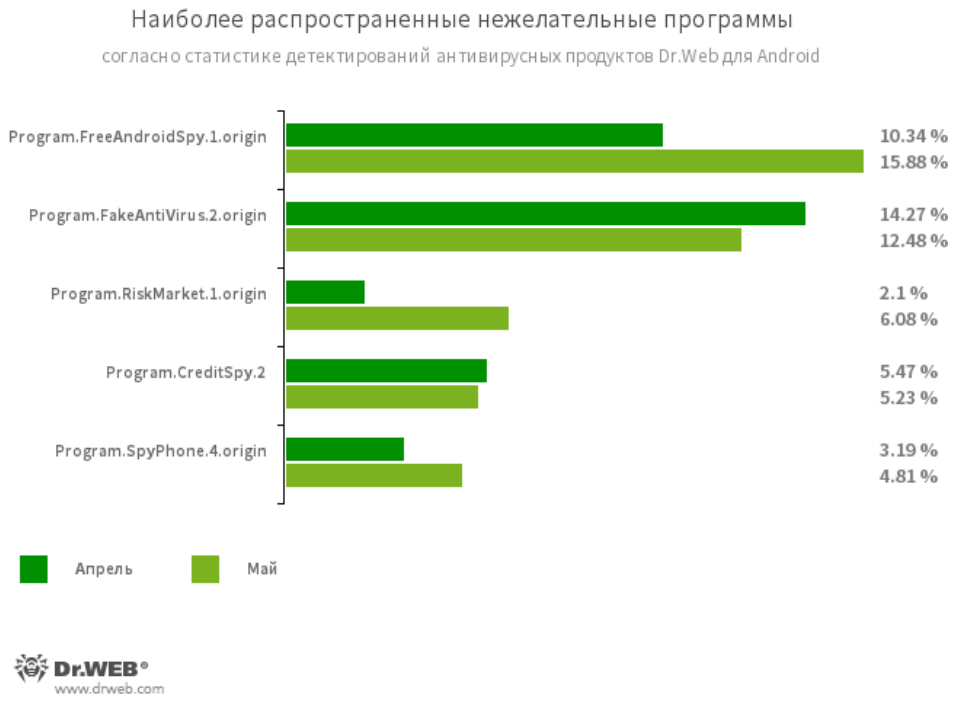
По данным антивирусных продуктов Dr.Web для Android

Android.RemoteCode.256.origin
Android.RemoteCode.6122
Вредоносные программы, которые загружают и выполняют произвольный код. В зависимости от модификации эти трояны могут загружать различные веб-сайты, переходить по ссылкам, нажимать на рекламные баннеры, подписывать пользователей на платные услуги и выполнять другие действия.
Android.HiddenAds.530.origin
Android.HiddenAds.1994

Трояны, предназначенные для показа навязчивой рекламы. Распространяются под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают их в системный каталог.
Android.DownLoader.906.origin

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

По данным антивирусных продуктов Dr.Web для Android



Program.FreeAndroidSpy.1.origin

Program.SpyPhone.4.origin

Приложения, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа. Они могут контролировать местоположение устройств, собирать данные об СМС-переписке, беседах в социальных сетях, копировать документы, фотографии и видео, выполнять прослушивание и т. п.

Program.FakeAntiVirus.2.origin

Детектирование рекламных программ, которые имитируют работу антивирусного ПО. Такие программы могут сообщать о несуществующих угрозах и вводить пользователей в заблуждение, требуя оплатить покупку полной версии.

Program.CreditSpy.2

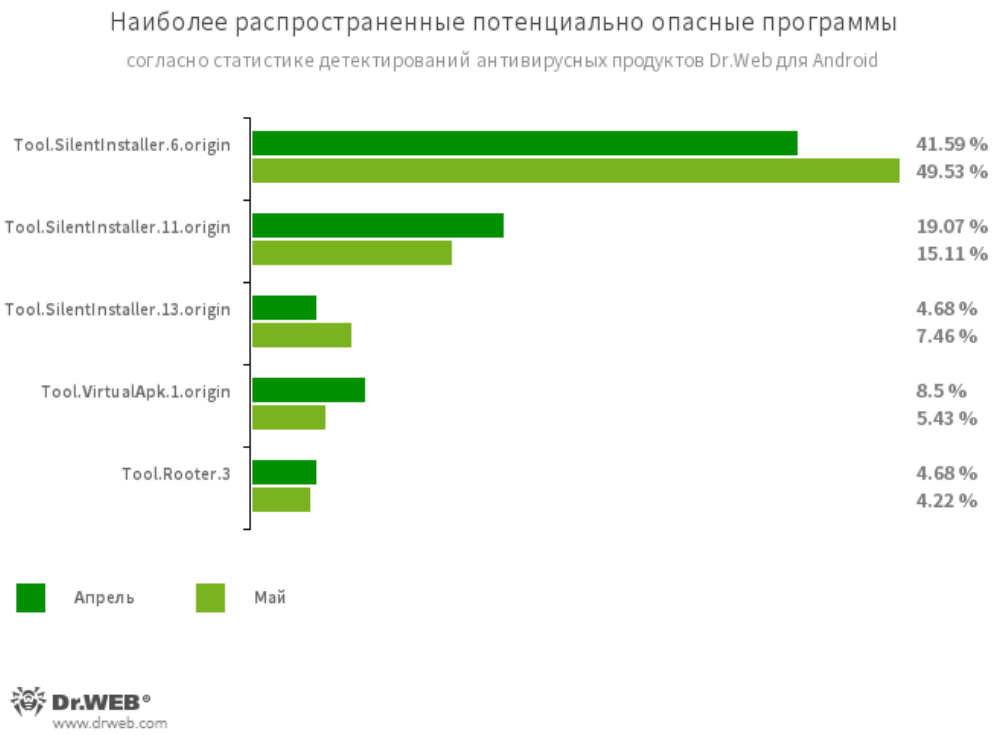
Детектирование программ, предназначенных для присвоения кредитного рейтинга на основании персональных данных пользователей. Такие приложения загружают на удаленный сервер СМС-сообщения, информацию о контактах из телефонной книги, историю вызовов, а также другие сведения.

Program.RiskMarket.1.origin

Магазин приложений, который содержит троянские программы и рекомендует пользователям их установку.

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

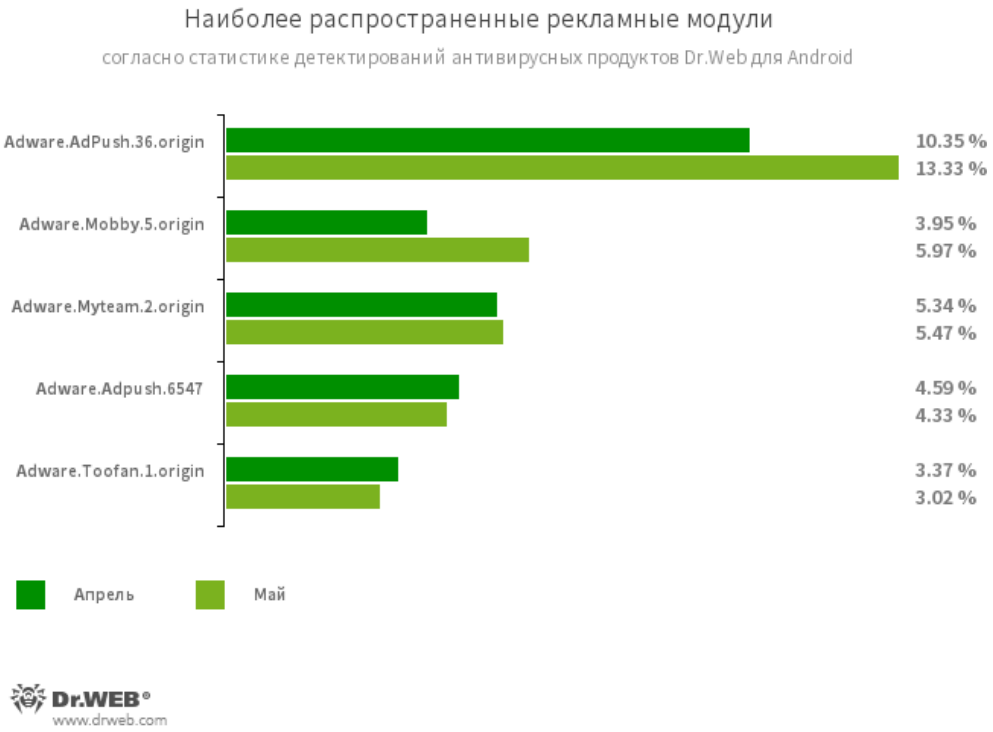
По данным антивирусных продуктов Dr.Web для Android



Tool.SilentInstaller.6.origin
Tool.SilentInstaller.11.origin
Tool.SilentInstaller.13.origin
Tool.VirtualApk.1.origin
Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.
Tool.Rooter.3
Утилита для получения root-полномочий на Android-устройствах, которая задействует различные эксплойты. Ее могут использовать как владельцы Android-устройств, так и злоумышленники и вредоносные программы.

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

По данным антивирусных продуктов Dr.Web для Android

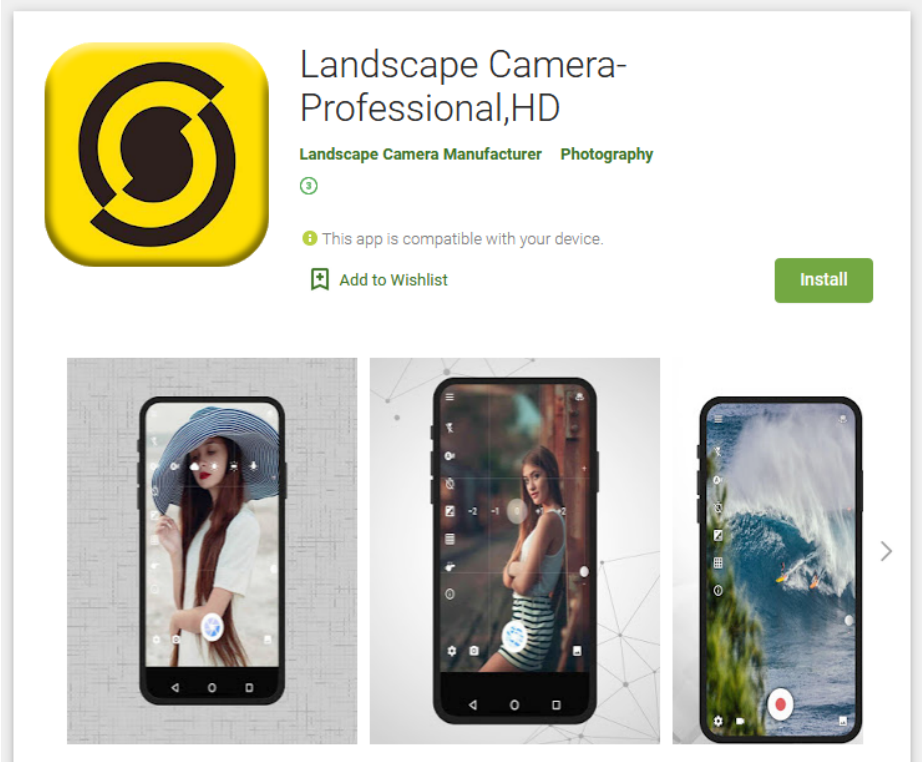


Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать ярлыки и загружать веб-сайты.

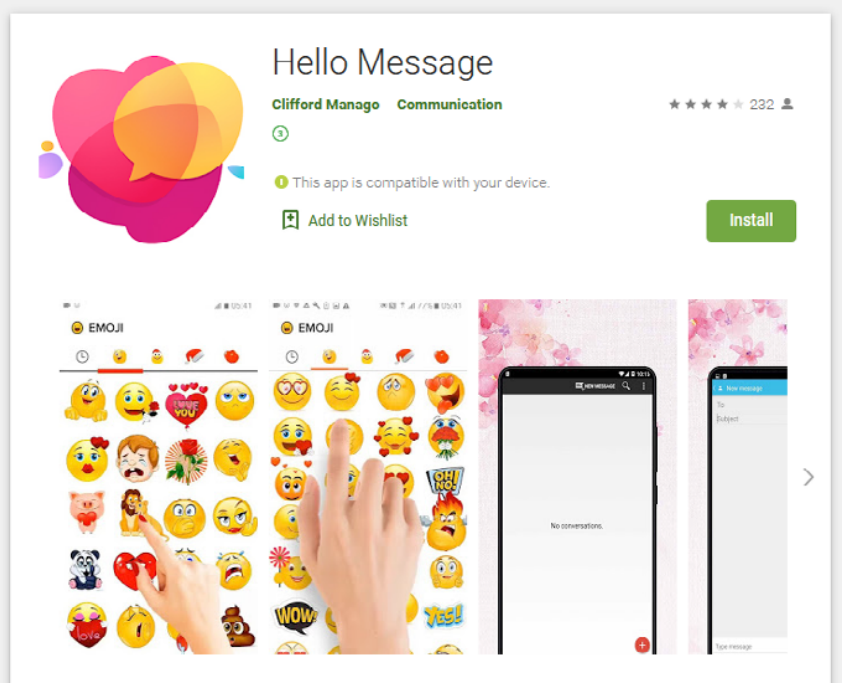
- Adware.Adpush.36.origin
- Adware.Adpush.6547
- Adware.Mobby.5.origin
- Adware.Myteam.2.origin
- Adware.Toofan.1.origin

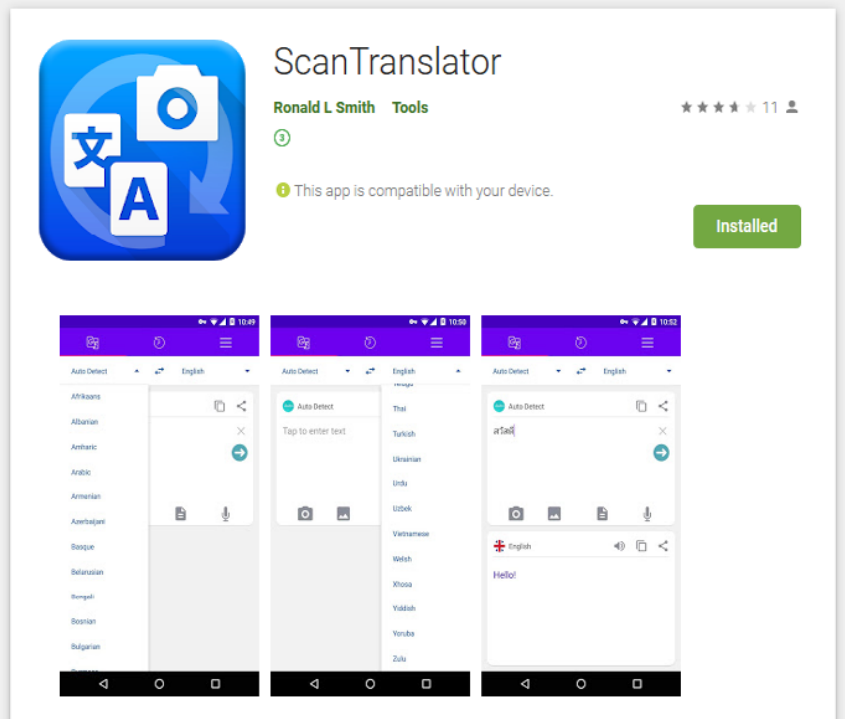
Угрозы в Google Play

В прошедшем месяце вирусные аналитики «Доктор Веб» обнаружили в каталоге Google Play множество новых модификаций троянов семейства Android.Joker, такие как Android.Joker.174, Android.Joker.182, Android.Joker.186, Android.Joker.138.origin, Android.Joker.190 и Android.Joker.199. Они были встроены в приложения для работы с документами, сборники изображений, программы для фотосъемки, системные утилиты, мессенджеры и другое ПО, которое выглядело безобидным. Однако после запуска эти трояны загружали и выполняли произвольный код, а также могли подписывать пользователей на дорогостоящие сервисы.

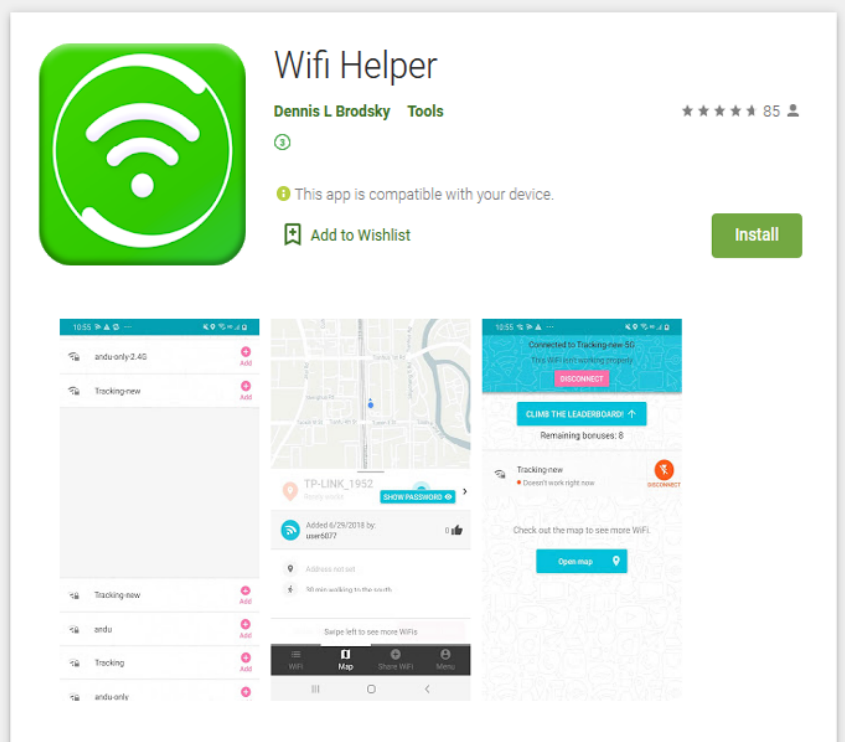


Угрозы в Google Play





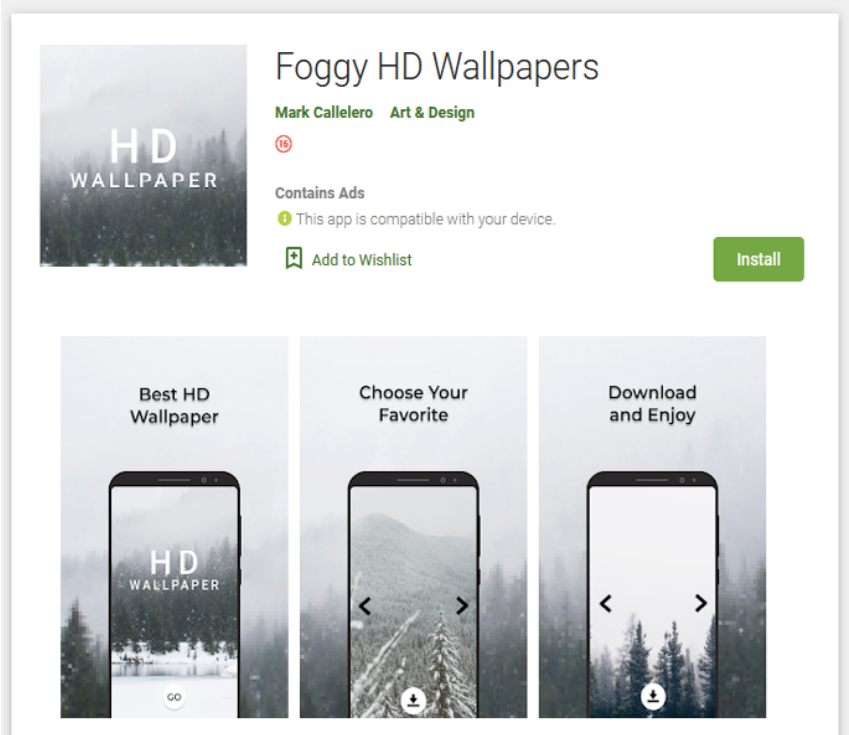
Угрозы в Google Play

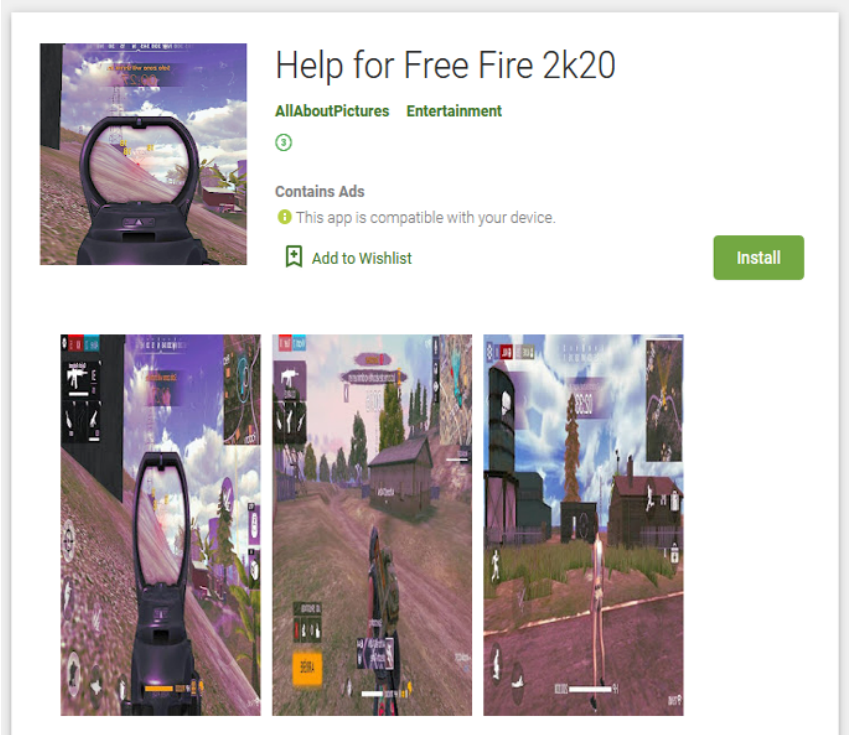


Кроме того, наши специалисты выявили трояна Android.Circle.15, который распространялся под видом утилиты для оптимизации работы системы. После запуска он показывал рекламу, загружал различные сайты и переходил по расположенным на них ссылкам и баннерам. Как и другие представители семейства Android.Circle, он мог выполнять скрипты BeanShell.

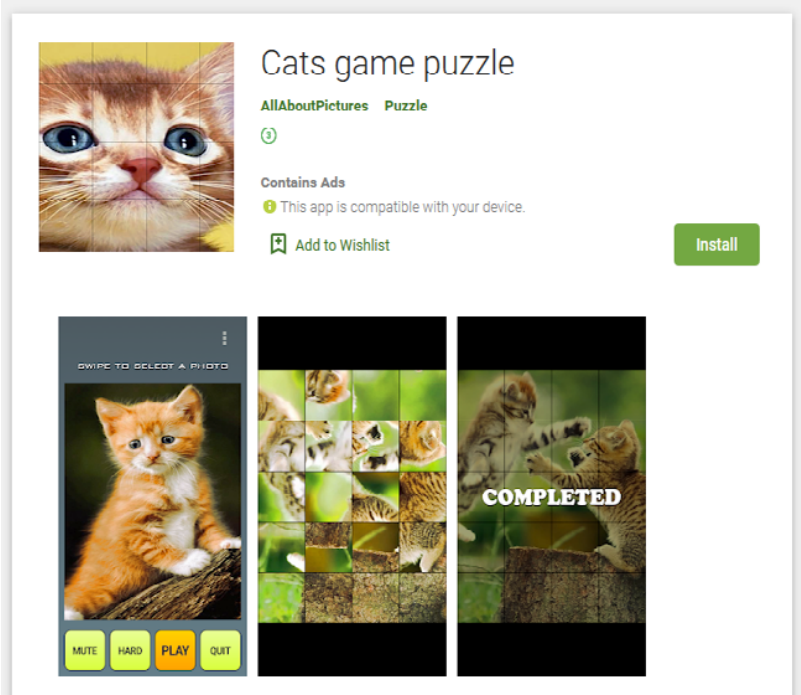
Среди найденных угроз были и новые рекламные трояны семейства Android.HiddenAds, такие как Android.HiddenAds.2134, Android.HiddenAds.2133, Android.HiddenAds.2146, Android.HiddenAds.2147, Android.HiddenAds.2048 и Android.HiddenAds.2150. Они распространялись под видом сборников стикеров для WhatsApp, игр, коллекций изображений и справочников. В общей сложности вирусные аналитики «Доктор Веб» обнаружили свыше 30 различных модификаций этих троянов, которые установили почти 160 000 пользователей.

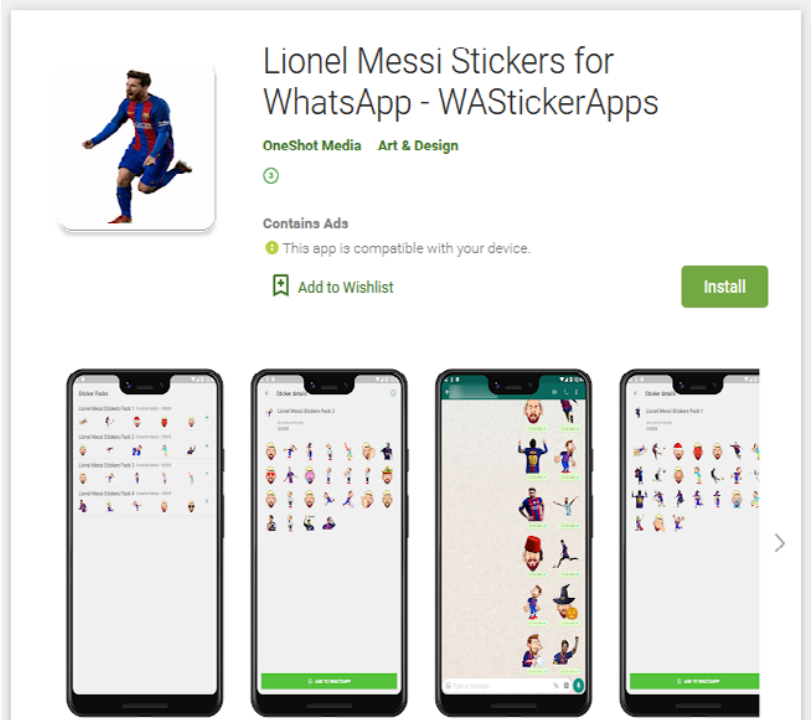
Угрозы в Google Play





Угрозы в Google Play

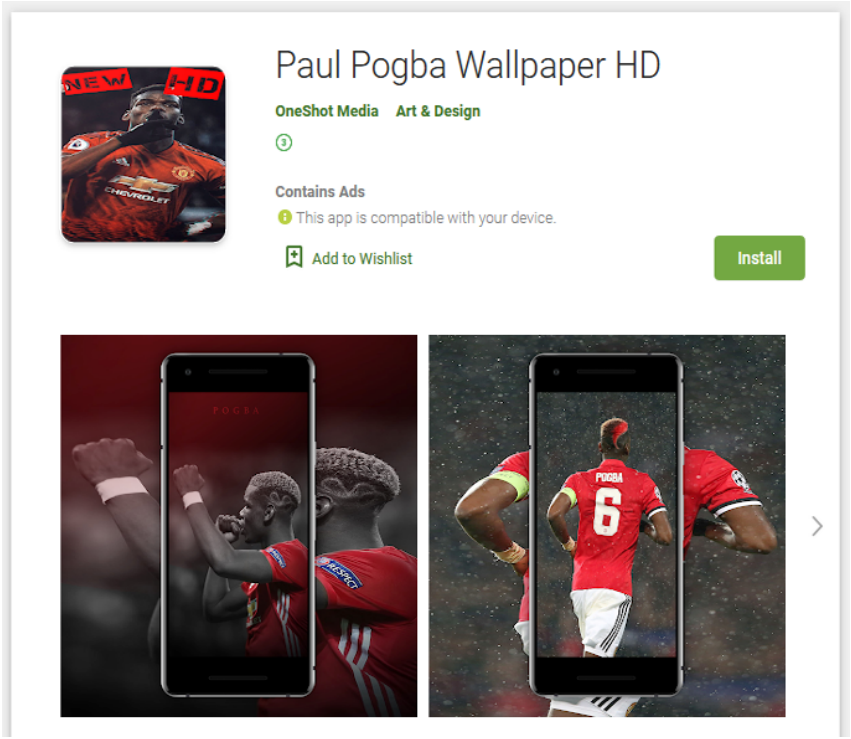




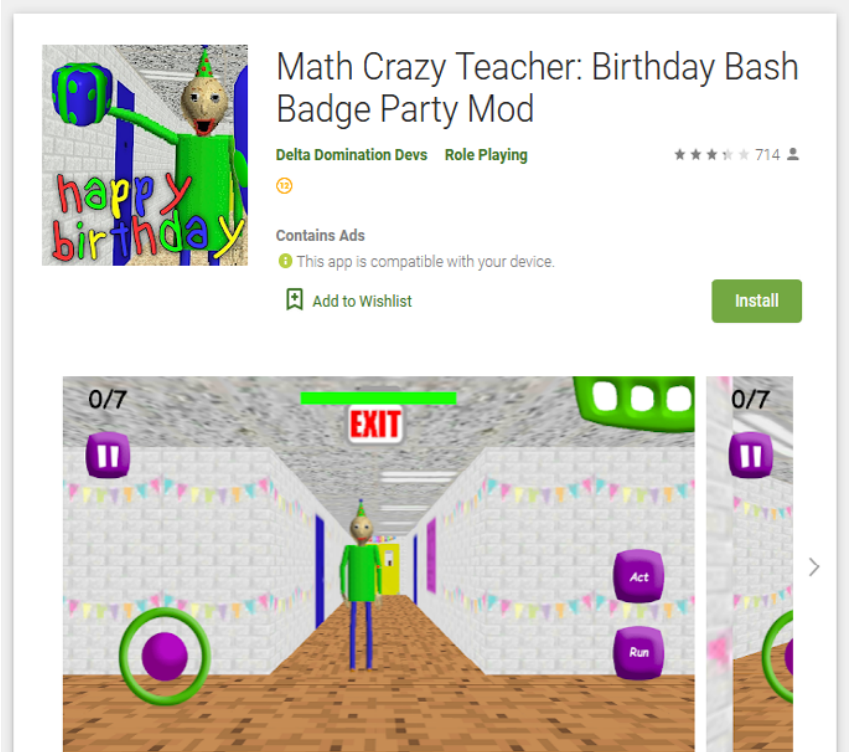
Угрозы в Google Play

После запуска эти вредоносные программы скрывали свой значок из списка приложений в меню главного экрана ОС Android и начинали показывать полноэкранные рекламные баннеры, которые мешали нормальной работе с устройствами.

Под видом безобидных программ, таких как игры и сборники изображений, также распространялись и новые рекламные модули, получившие имена **Adware.AdSpam.4**, **Adware.AdSpam.5** и **Adware.AdSpam.6**. Как и трояны семейства Android.HiddenAds, они показывали баннеры поверх других программ. Однако они не удаляли свои значки, поэтому пользователям было легче обнаружить источник рекламы и удалить приложения, в которые были встроены эти модули.



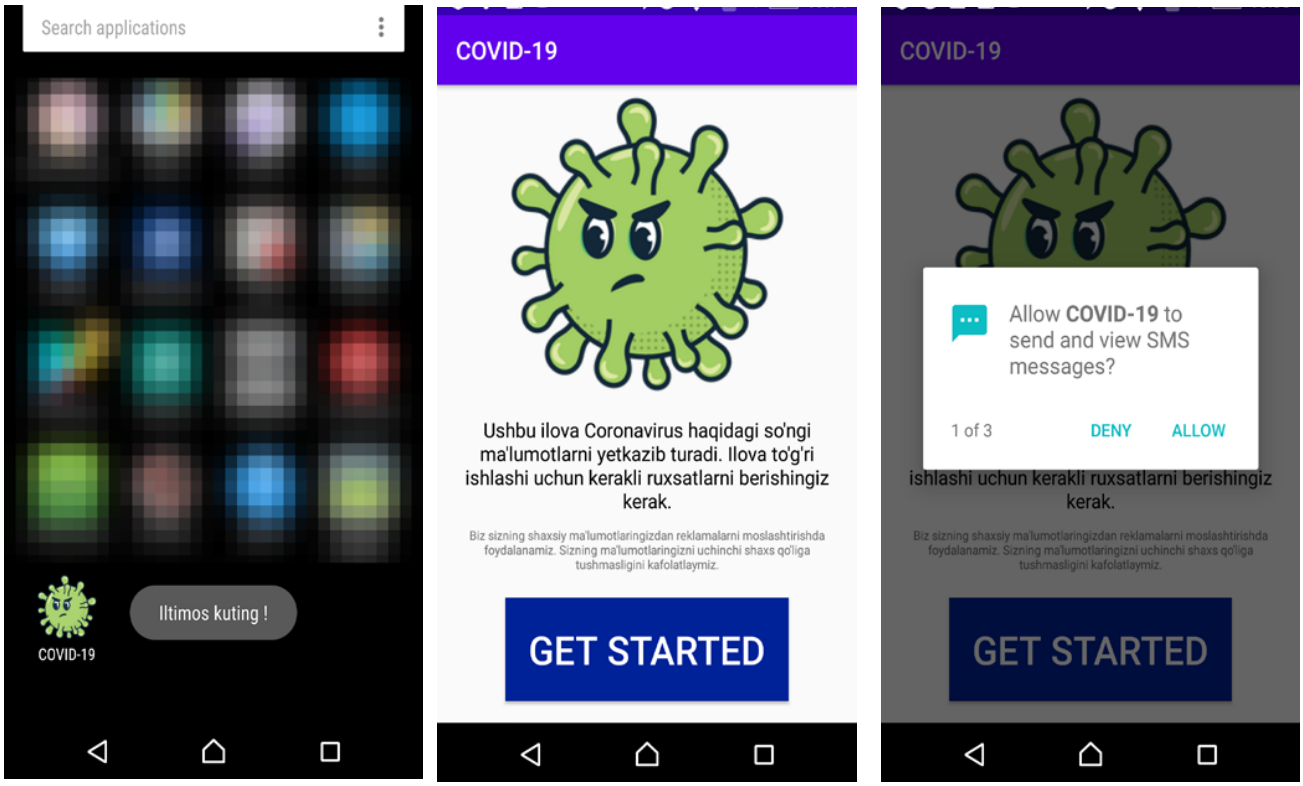
Угрозы в Google Play



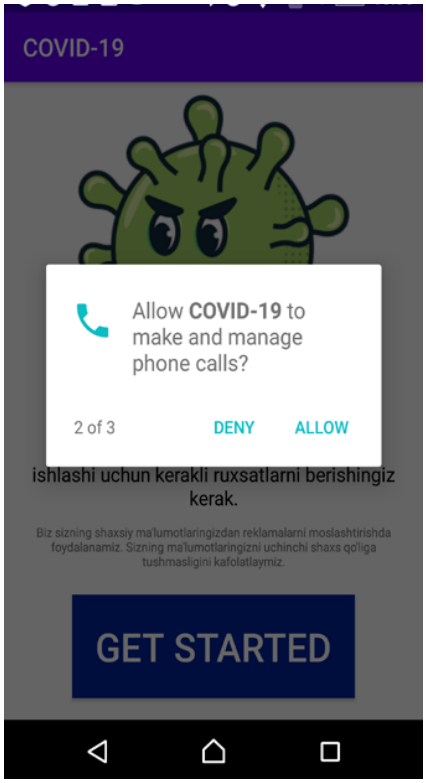
«Доктор Веб»: обзор вирусной активности для мобильных устройств в мае 2020 года

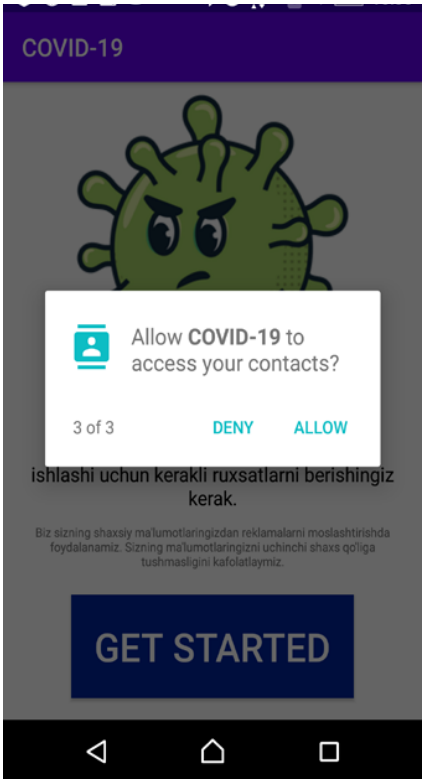
Прочие угрозы

Среди распространявшихся в мае вредоносных приложений оказался очередной троян, эксплуатирующий тему пандемии коронавируса SARS-CoV-2. Эта вредоносная программа, добавленная в вирусную базу Dr.Web как Android.Spy.660.origin, распространялась под видом утилиты, которая показывает число заболевших COVID-19. Однако истинной целью этого трояна был кибершпионаж. Главной мишенью Android.Spy.660.origin стали пользователи из Узбекистана. Троян похищал у них информацию об SMS, журнале телефонных вызовов, а также контактах из записной книги мобильного устройства. При запуске он запрашивал соответствующие системные разрешения, после чего демонстрировал статистику по заболеванию, чтобы не вызвать подозрений у своих жертв.



Прочие угрозы





Кроме того, злоумышленники продолжили атаковать пользователей с применением различных банковских троянов. Например, жителям Вьетнама угрожал банкер Android.Banker.388.origin, который загружался на Android-устройства при посещении поддельного сайта Министерства общественной безопасности страны. А жителям Японии вновь угрожали представители нескольких семейств банковских троянов, которые на протяжении долгого времени распространяются через поддельные сайты почтовых и курьерских служб.

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

Прочие угрозы

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 мае 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.антивирус.рф | www.drweb.ru | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах

Узнайте больше
Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека