Dr.WEB®
с 1992 года

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

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

21 июля 2020 года

В прошедшем месяце на Android-устройствах было выявлено на 17,2% меньше угроз по сравнению с маем. Количество вредоносных и рекламных программ снизилось за 17,6% и 19,84% соответственно. При этом число нежелательных приложений выросло на 2,6%, а потенциально опасных – на 14,52%.

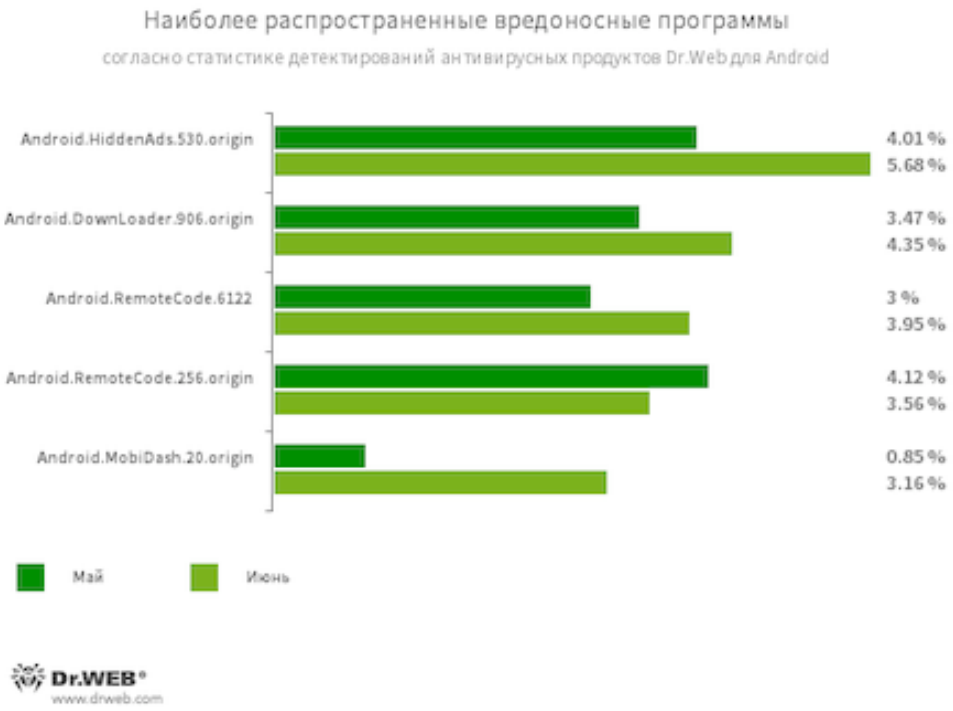
Наши вирусные аналитики обнаружили в каталоге Google Play новые угрозы. Среди них были рекламные трояны семейства Android.HiddenAds, а также многофункциональные вредоносные приложения семейства Android.Joker, которые подписывали пользователей на платные сервисы и могли выполнять произвольных код. Кроме того, злоумышленники распространяли через Google Play нового банковского трояна, использующего функции специальных возможностей ОС Android для установки своего вредоносного компонента.

ГЛАВНЫЕ ТЕНДЕНЦИИ ИЮНЯ

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

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

По данным антивирусных продуктов Dr.Web для Android



Android.HiddenAds.530.origin

Троян, предназначенный для показа навязчивой рекламы. Распространяется под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают их в системный каталог.

Android.DownLoader.906.origin

Троян, загружающий другие вредоносные программы и ненужное ПО. Может скрываться во внешне безобидных приложениях, которые распространяются через каталог Google Play или вредоносные сайты.

Android.RemoteCode.6122

Android.RemoteCode.256.origin

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.MobiDash.20.origin

Троянская программа, показывающая надоедливую рекламу. Представляет собой программный модуль, который разработчики ПО встраивают в приложения.

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

По данным антивирусных продуктов Dr.Web для Android

Program.FreeAndroidSpy.1.origin

Program.Mrecorder.1.origin

Program.Asgard.1.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

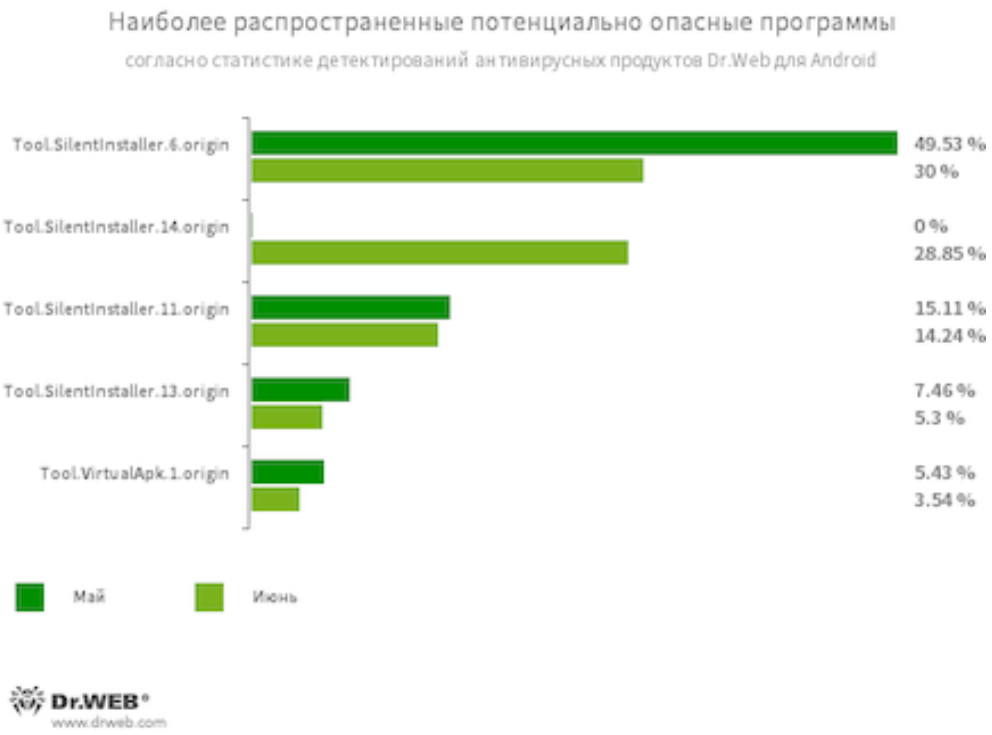
Детектирование программ, предназначенных для присвоения кредитного рейтинга на основании персональных данных пользователей. Такие приложения загружают на удаленный сервер СМС-сообщения, информацию о контактах из телефонной книги, историю вызовов, а также другие сведения.

Program.RiskMarket.1.origin

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

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

По данным антивирусных продуктов Dr.Web для Android

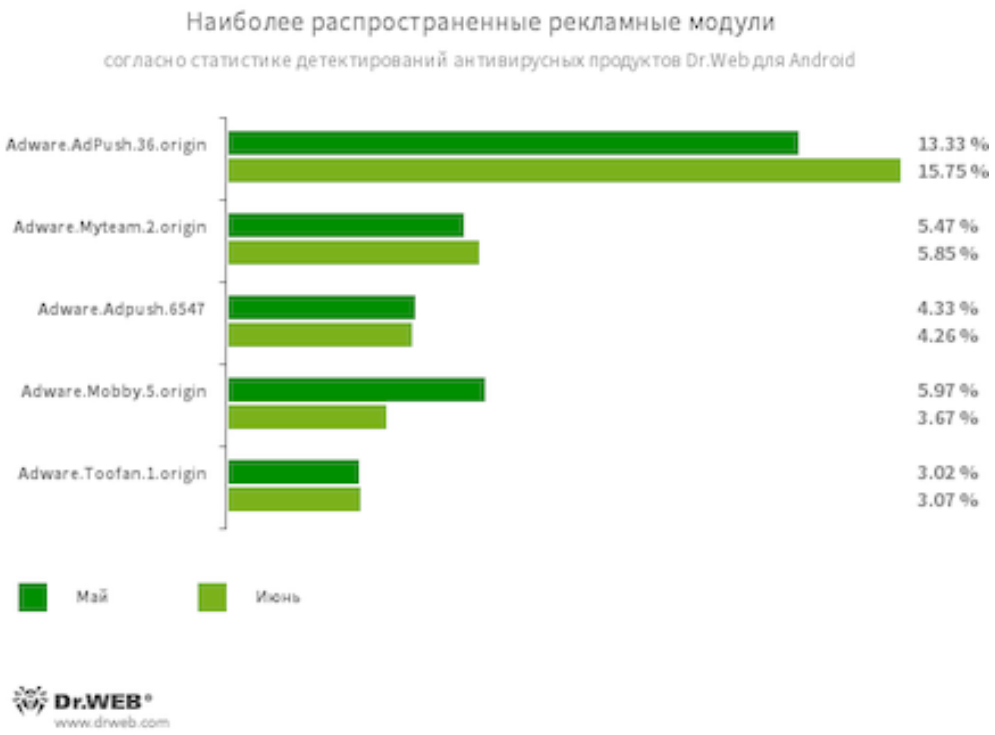


Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

Tool.SilentInstaller.6.origin
Tool.SilentInstaller.11.origin
Tool.SilentInstaller.13.origin
Tool.SilentInstaller.14.origin
Tool.VirtualApk.1.origin

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

По данным антивирусных продуктов Dr.Web для Android

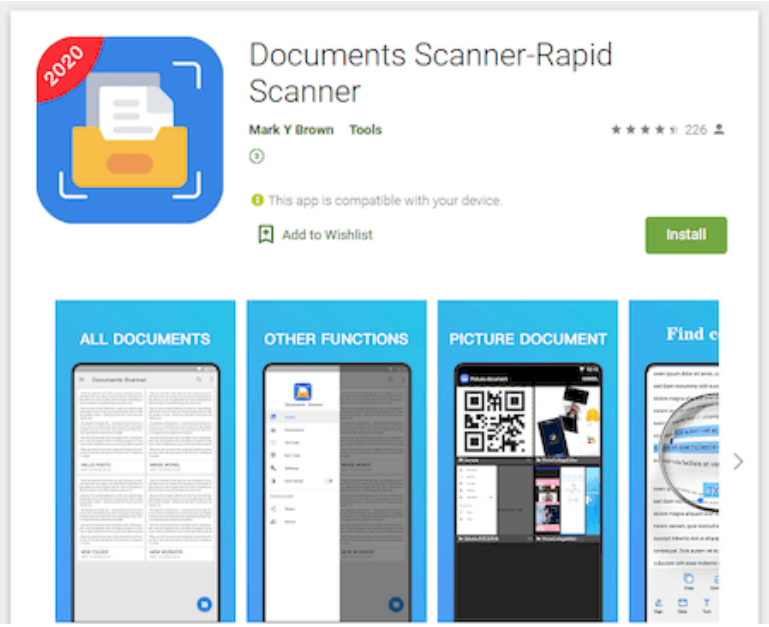


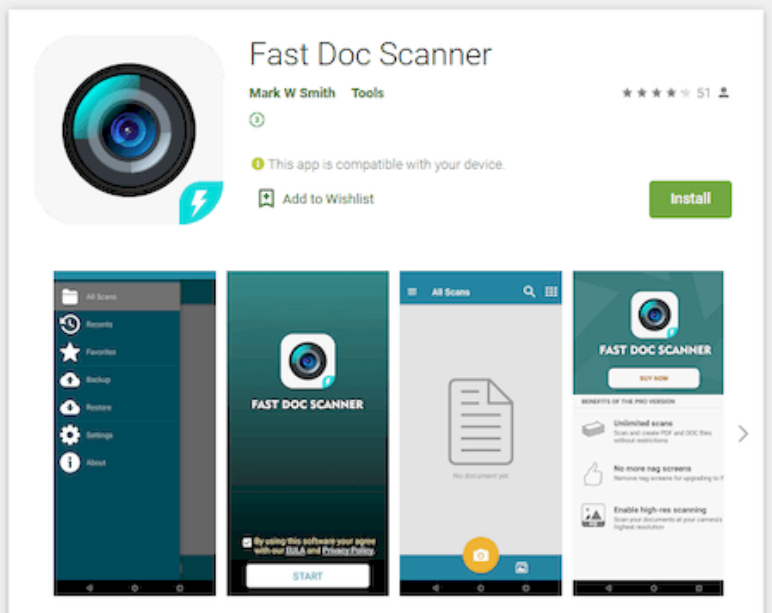
Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать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

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

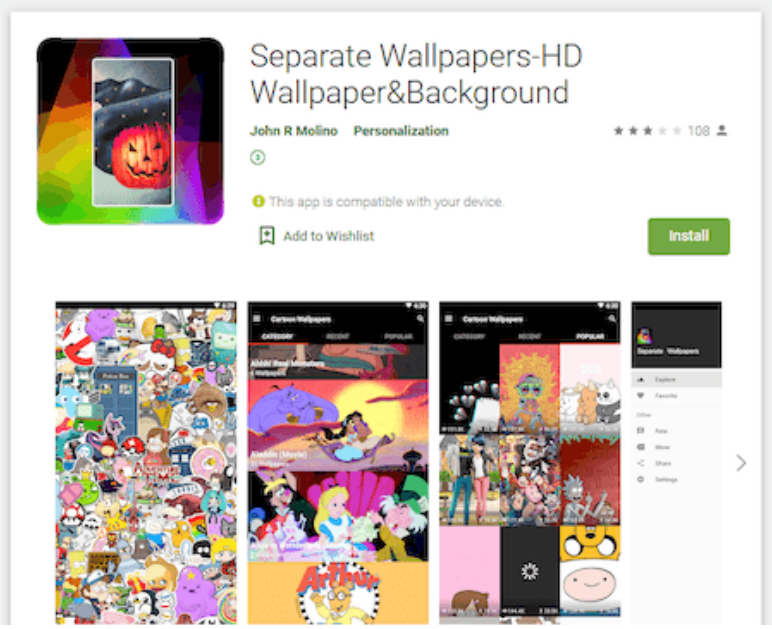
Угрозы в Google Play

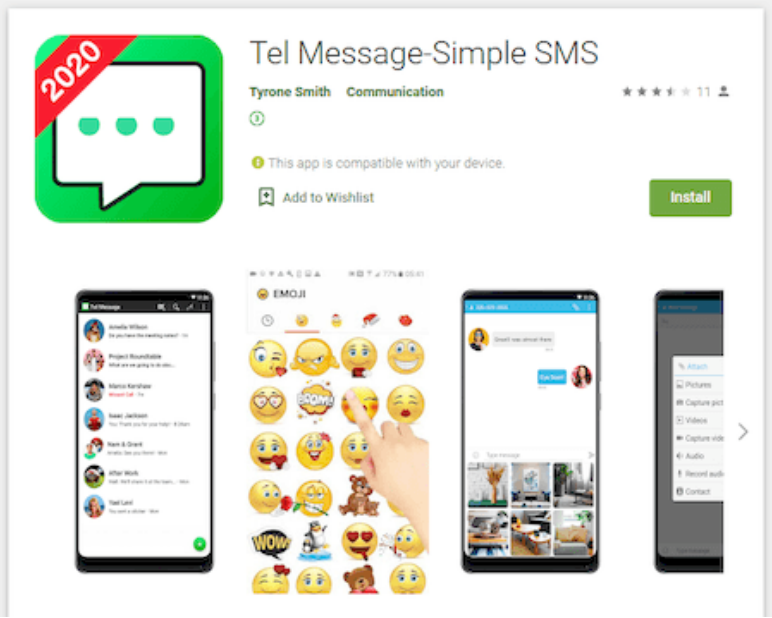
В июне в вирусную базу Dr.Web были добавлены записи для детектирования новых вредоносных программ семейства Android.Joker — Android.Joker.204, Android.Joker.209, Android.Joker.217 и Android.Joker.221. Злоумышленники встроили их в приложения для работы с документами, сборники изображений и мессенджеры.





Угрозы в Google Play

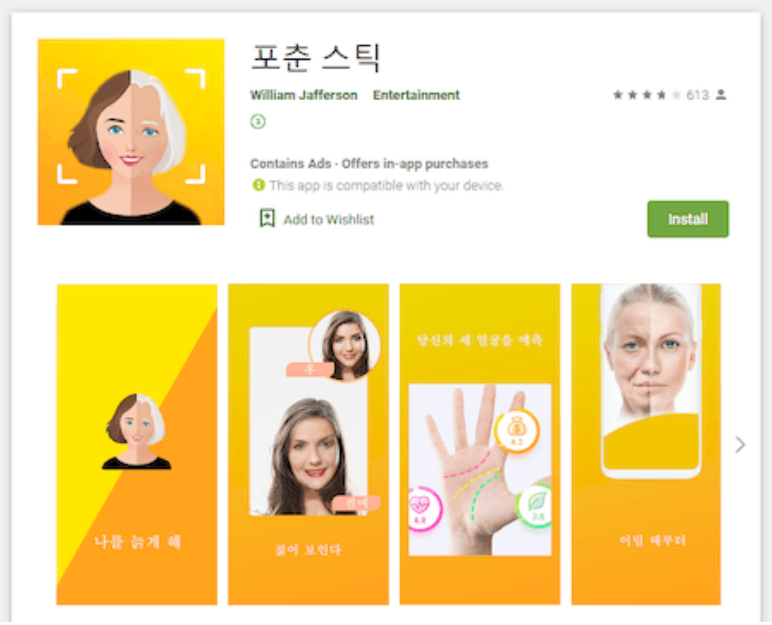


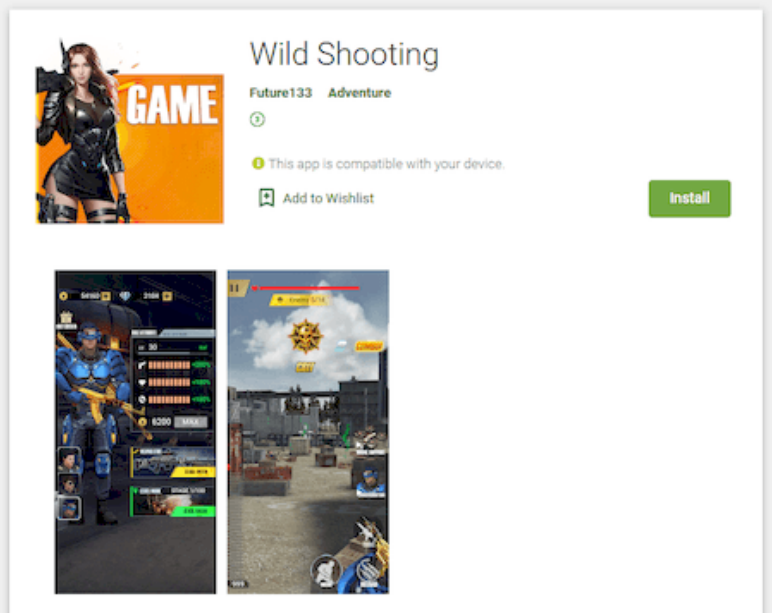


Эти трояны самостоятельно подписывали пользователей на дорогостоящие мобильные услуги, перехватывая уведомления с ПИН-кодами подтверждения, а также могли загружать и выполнять произвольный код.

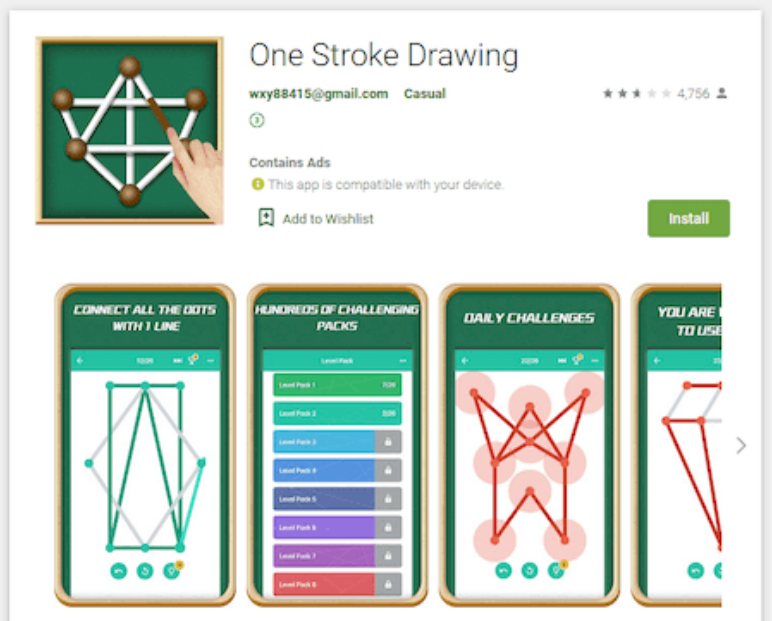
Угрозы в Google Play

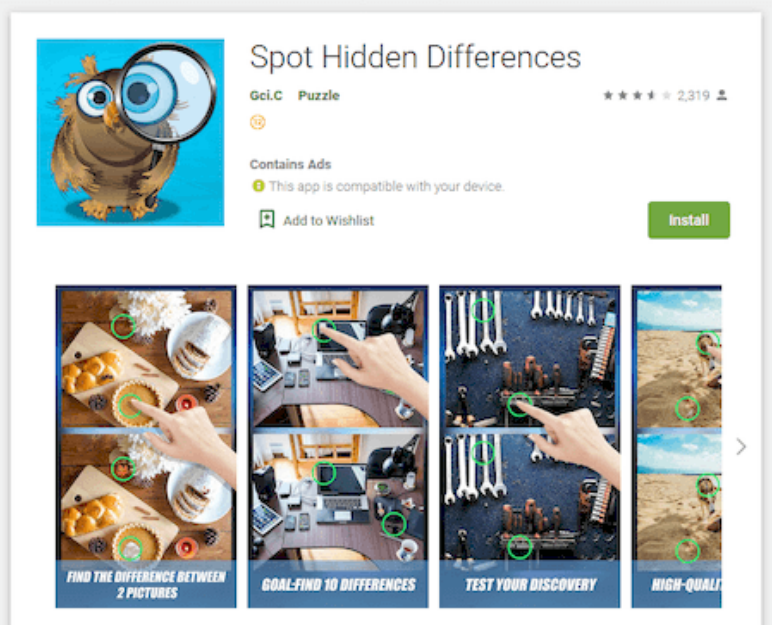
Кроме того, в Google Play были обнаружены очередные рекламные трояны семейства Android.HiddenAds, такие как Android.HiddenAds.548.origin и Android.HiddenAds.554.origin. Они распространялись под видом различных игр.





Угрозы в Google Play

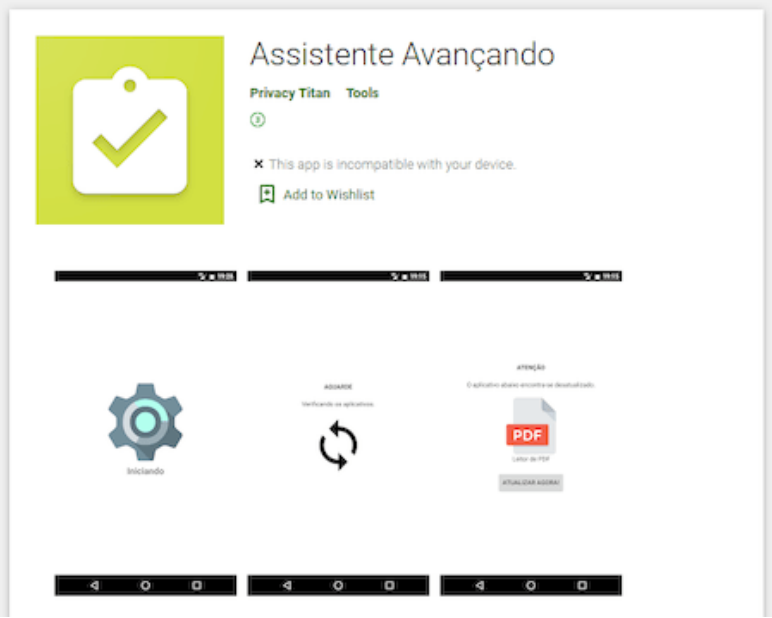




После запуска трояны скрывали свои значки из списка приложений в меню главного экрана и показывали баннеры поверх окон других приложений, мешая нормальной работе с Android-устройствами.

Угрозы в Google Play

Также наши вирусные аналитики выявили банковского трояна Android.BankBot.733.origin, которого вирусописатели распространяли под видом приложения для установки системных обновлений и обеспечения защиты мобильных устройств. В действительности это вредоносное приложение незаметно загружало вспомогательный компонент, который затем пыталась установить через сервис специальных возможностей (Accessibility Service).



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 июне 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