Dr.WEB®
с 1992 года

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

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

18 мая 2020 года

По сравнению с мартом в апреле количество выявленных угроз на Android-устройствах увеличилось на 16,46%. На 16,13% выросло число обнаруженных вредоносных программ, на 28,37% — нежелательных программ, на 20,83% — потенциально опасных и на 17,43% — рекламных приложений.

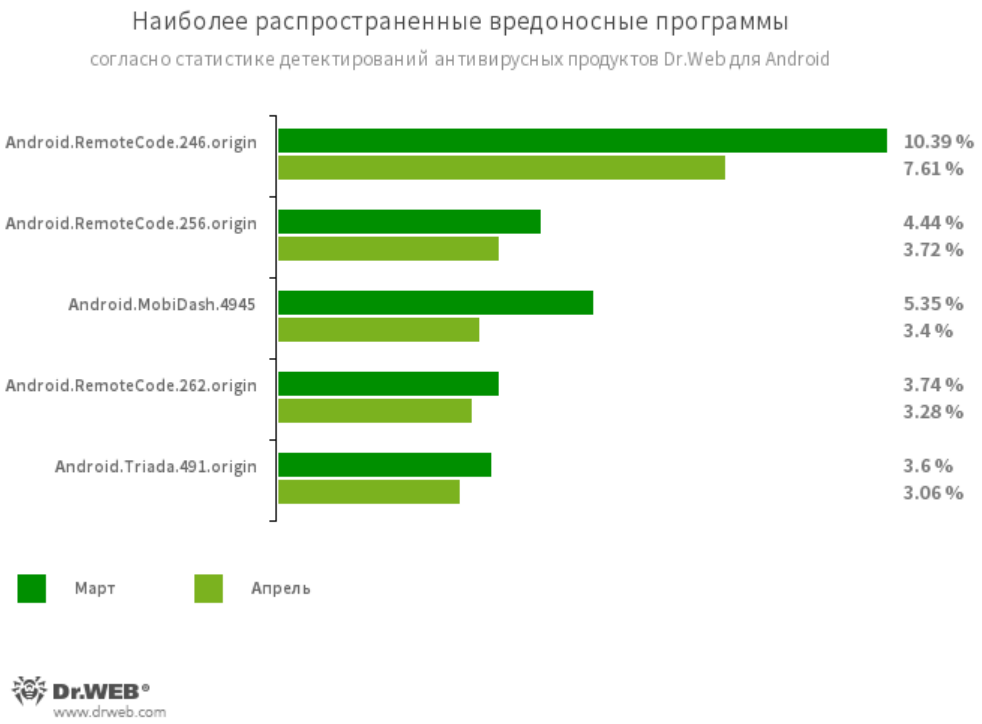
За последний месяц специалисты компании «Доктор Веб» зафиксировали несколько угроз в каталоге Google Play. Среди них были новые модификации опасных вредоносных приложений Android.Circle, способных выполнять команды злоумышленников. Кроме того, был найден рекламный троян Android.HiddenAds.2124, а также троян Android.Joker.164, который подписывал пользователей на платные услуги и мог выполнять произвольный код.

ГЛАВНЫЕ ТЕНДЕНЦИИ АПРЕЛЯ

- Увеличение числа угроз, выявленных на Android-устройствах
- Появление новых вредоносных программ в Google Play

«Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 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. 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.4945

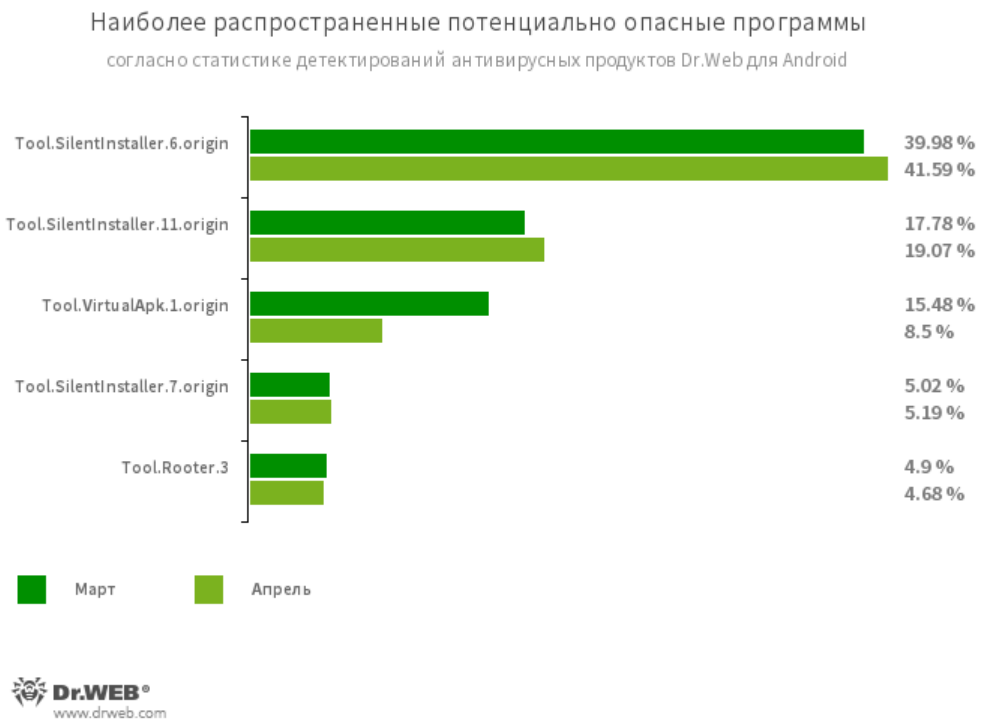
Троянская программа, показывающая надоедливую рекламу. Представляет собой программный модуль, который разработчики ПО встраивают в приложения.

Android.Triada.491.origin

Многофункциональный троян, выполняющий разнообразные вредоносные действия. Относится к семейству троянских приложений, проникающих в процессы всех работающих программ. Некоторые модификации этого семейства встречаются в прошивках Android-устройств, куда злоумышленники внедряют их на этапе производства.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 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. 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. Она может использоваться как пользователями Android-устройств, так и злоумышленниками и вредоносными программами.

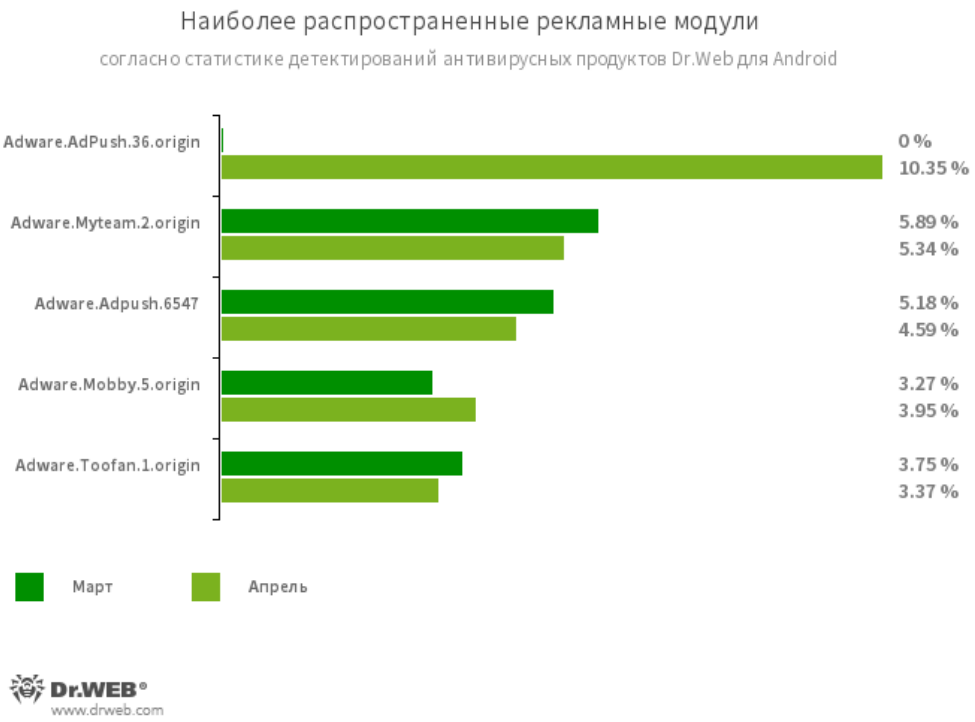
«Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2020 года

По данным антивирусных продуктов Dr.Web для Android

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.FreeAndroidSpy.1.origin
Program.Mrecorder.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.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.RemoteBot.1.origin
Приложение, предназначенное для дистанционного управления Android-устройствами. Программа позволяет перехватывать и отправлять СМС, выполнять и отслеживать телефонные вызовы, перехватывать содержимое уведомлений, контролировать местоположение устройства, выполнять прослушивание окружения, записывать видео, делать фотографии и т. п.

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

По данным антивирусных продуктов Dr.Web для Android

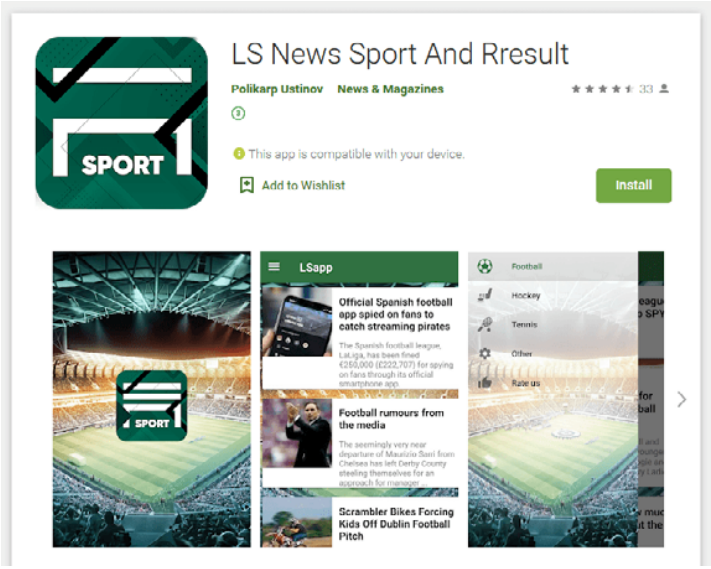


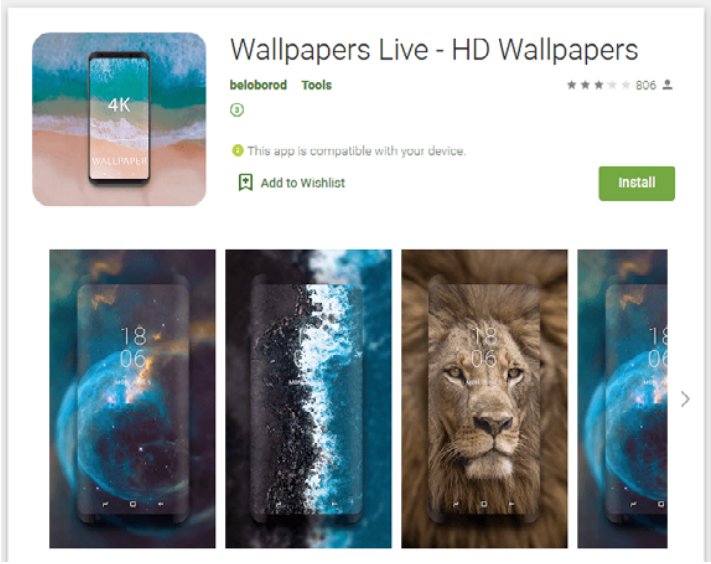
Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать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

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

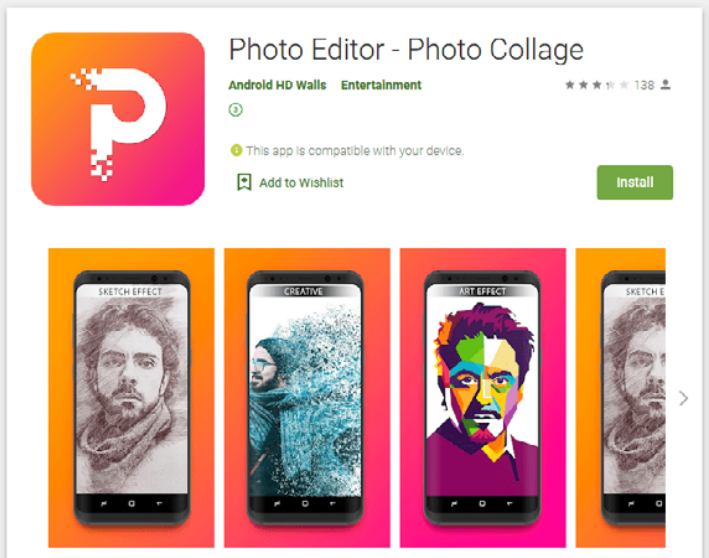
Угрозы в Google Play

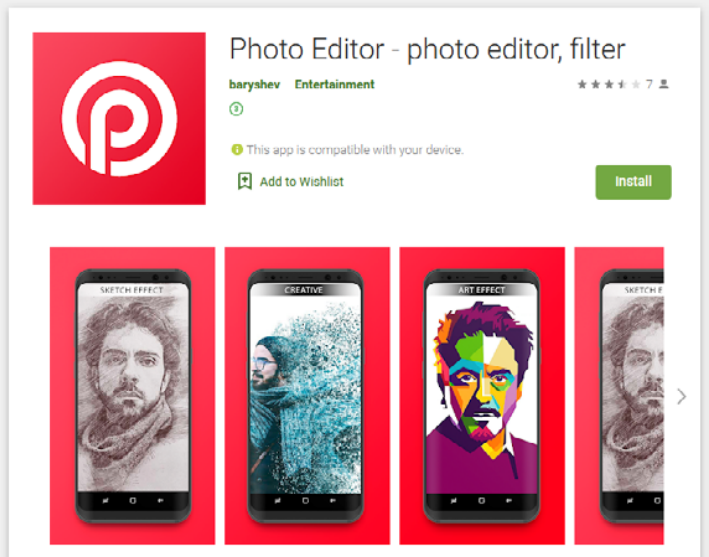
В апреле вирусные аналитики «Доктор Веб» выявили в каталоге Google Play сразу несколько вредоносных программ. Среди них были новые модификации троянов семейства Android.Circle — Android.Circle.**1.origin**, Android.Circle.**8** и Android.Circle.**14**. Они распространялись под видом безобидных приложений, таких как редакторы изображений и программы спортивной тематики. Трояны этого семейства исполняют скрипты с заданиями, используя для этого встроенную в них библиотеку с открытым исходным кодом BeanShell. По команде злоумышленников они могут показывать рекламу, а также выполнять другие действия.





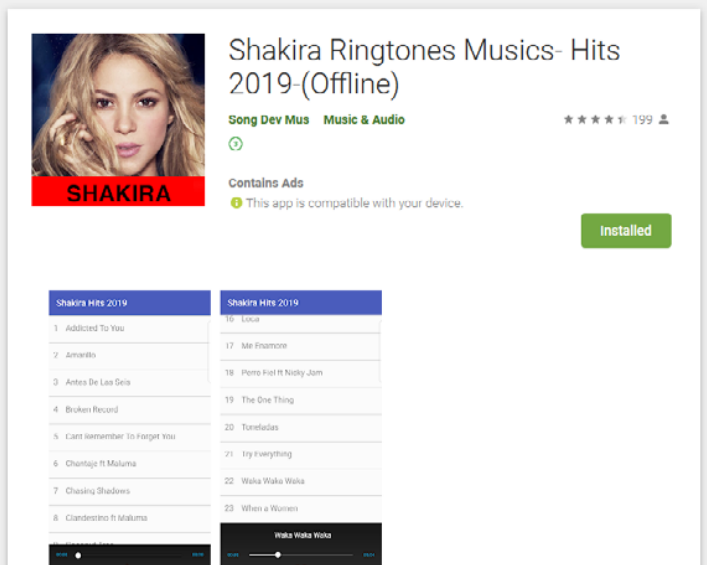
Угрозы в Google Play

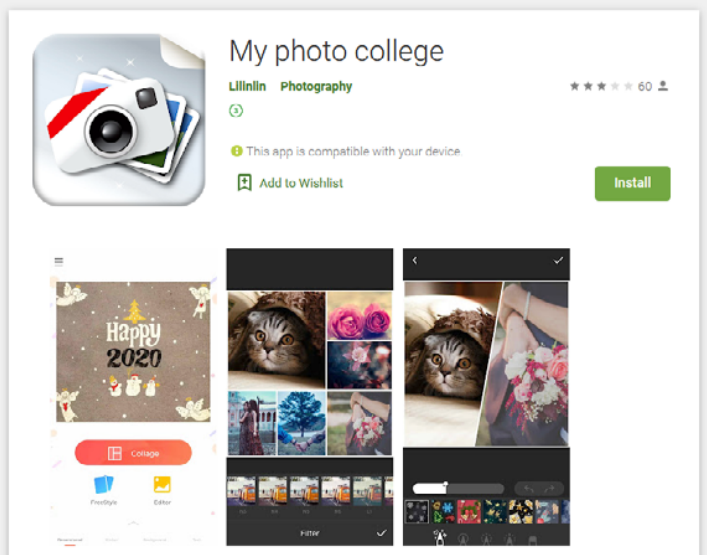




Вместе с этими вредоносными программами были обнаружены трояны Android.HiddenAds.2124 и Android.Joker.164. Первый показывал надоедливую рекламу и был встроен в приложения для прослушивания музыки. Второй — выполнял произвольный код и мог подписывать пользователей на дорогостоящие сервисы. Его злоумышленники распространяли под видом графического редактора.

Угрозы в Google Play





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 апреле 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