Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2021 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2021 года

13 апреля 2021 года

В марте в числе наиболее активных угроз вновь оказались трояны и нежелательные приложения, демонстрировавшие рекламу. Кроме того, на Android-устройствах часто обнаруживались вредоносные программы, загружающие другое ПО и выполняющие произвольный код.

Среди угроз, выявленных в каталоге Google Play, было множество новых модификаций троянов Android.Joker, подписывающих жертв на премиум-сервисы, а также очередные мошеннические приложения Android.FakeApp.

ГЛАВНЫЕ ТЕНДЕНЦИИ МАРТА

- Распространение новых угроз через каталог Google Play
- Активность троянов, подписывающих жертв на платные мобильные услуги
- Распространение мошеннических приложений

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2021 года

По данным антивирусных продуктов Dr.Web для Android

Android.HiddenAds.1994

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

Android.RemoteCode.284.origin

Android.RemoteCode.6122

Вредоносная программа, которая загружает и выполняет произвольный код. В зависимости от модификации она также может загружать различные веб-сайты, переходить по ссылкам, нажимать на рекламные баннеры, подписывать пользователей на платные услуги и выполнять другие действия.

Android.Triada.510.origin

Многофункциональный троян, выполняющий разнообразные вредоносные действия. Относится к семейству троянских приложений, проникающих в процессы всех работающих программ. Различные представители этого семейства могут встречаться в прошивках Android-устройств, куда злоумышленники внедряют их на этапе производства. Кроме того, некоторые их модификации могут эксплуатировать уязвимости, чтобы получить доступ к защищенным системным файлам и директориям.

Android.MobiDash.5135

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

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2021 года

По данным антивирусных продуктов Dr.Web для Android

Program.FreeAndroidSpy.1.origin

Program.Mrecorder.1.origin

Program.Reptilicus.7.origin

Приложения, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа. Они способны контролировать местоположение устройств, собирать данные об СМС-переписке, беседах в социальных сетях, копировать документы, фотографии и видео, прослушивать телефонные звонки и окружение 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.Gemius.1.origin

Программа, собирающая информацию о мобильных Android-устройствах и о том, как их используют их владельцы. Вместе с техническими данными она собирает конфиденциальные сведения — информацию о местоположении устройства, сохраненных в браузере закладках, истории посещенных сайтов, а также о вводимых интернет-адресах.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2021 года

По данным антивирусных продуктов Dr.Web для Android

Tool.SilentInstaller.6.origin

Tool.SilentInstaller.7.origin

Tool.SilentInstaller.13.origin

Tool.SilentInstaller.14.origin

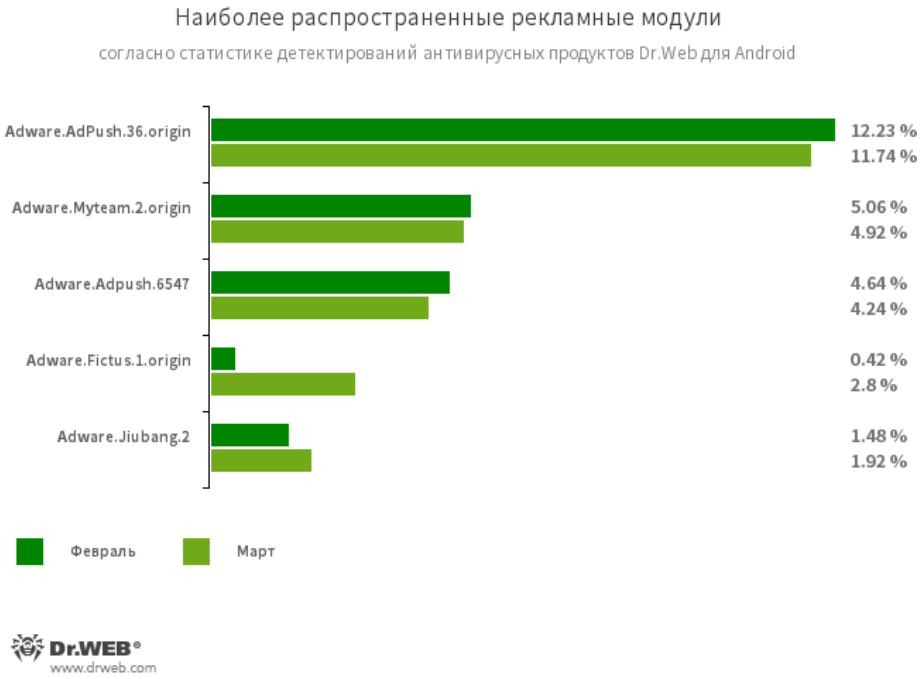
Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

Tool.Obfuscapk.1

Детектирование приложений, защищенных утилитой-обфускатором Obfuscapk. Эта утилита используется для автоматической модификации и запутывания исходного кода Android-приложений, чтобы усложнить их обратный инжиниринг. Злоумышленники применяют ее для защиты вредоносных и других опасных программ от обнаружения антивирусами.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2021 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

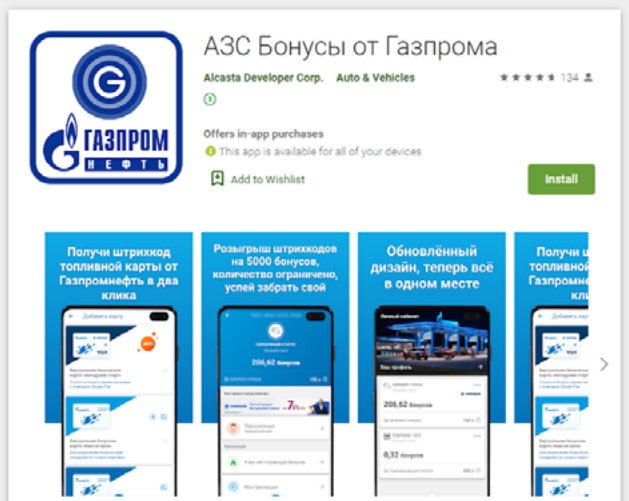
Adware.Fictus.1.origin

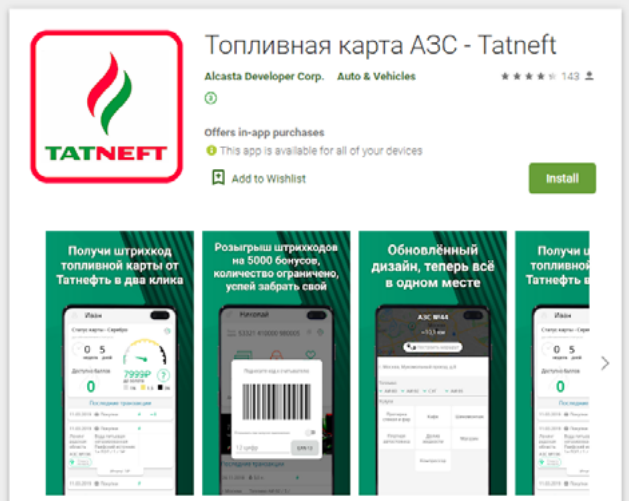
Adware.Jiubang.2

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2021 года

Угрозы в Google Play

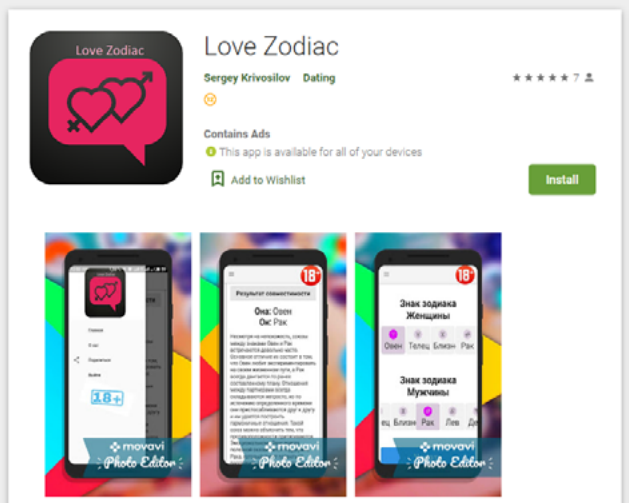
В прошедшем месяце специалисты компании «Доктор Веб» выявили в каталоге Google Play очередные мошеннические программы семейства Android.FakeApp. Среди них были новые модификации трояна Android.FakeApp.247, якобы предоставлявшего доступ к различным бонусам и скидкам от известных компаний и торговых сетей. В данном случае — бонусам при покупке топлива на популярных АЗС. Для получения «приза» потенциальным жертвам предлагалось оформить платную подписку стоимостью от 429 рублей в неделю. В итоге пользователи никаких скидок и бонусов не получали — троян лишь демонстрировал им бесполезный штрих-код.

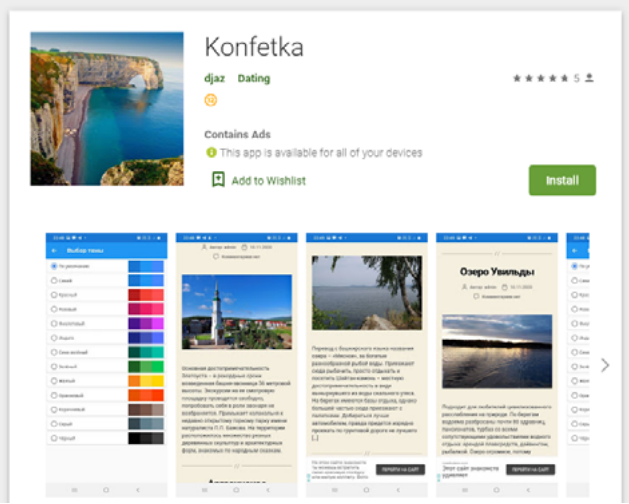


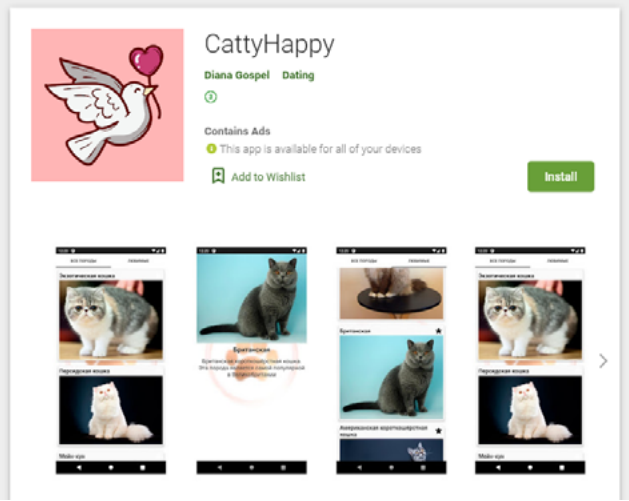


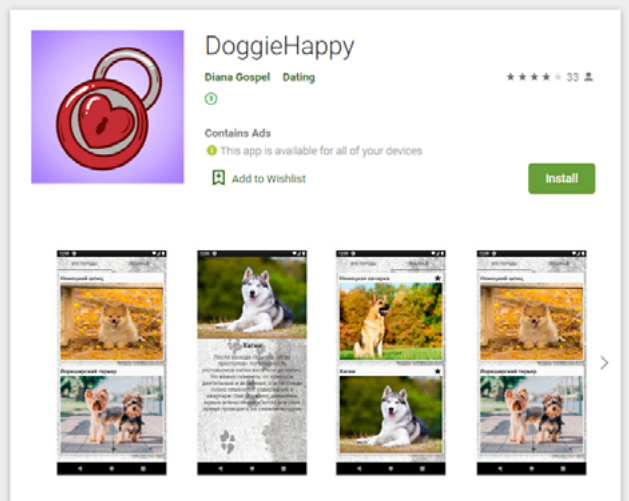
Другие вредоносные программы-подделки распространялись под видом разнообразных безобидных приложений — всевозможных справочников и пособий, программ для проверки совместимости людей и т. п. На самом деле они не выполняли заявленных функций и после запуска загружали сомнительные веб-сайты. Эти трояны были добавлены в вирусную базу Dr.Web как Android.FakeApp.244, Android.FakeApp.249 и Android.FakeApp.250.

Угрозы в Google Play





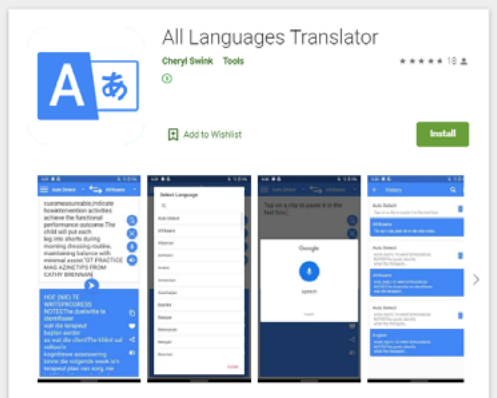


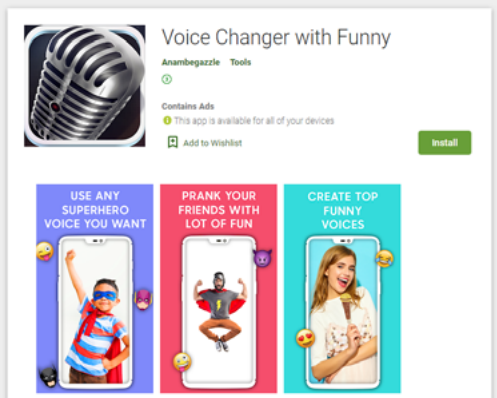


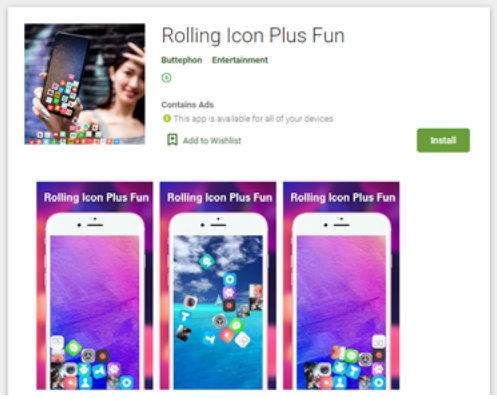
Кроме того, в течение марта вирусные аналитики «Доктор Веб» обнаружили множество новых троянов семейства Android.Joker, шпионящих за пользователями и подписывающих на дорогостоящие мобильные услуги, а также способных выполнять произвольный код. Эти многофункциональные трояны распространялись под видом программы-переводчика, приложения для записи голоса и создания различных звуковых эффектов, анимированных обоев, лончера (программы управления главным экраном), всевозможных редакторов изображений, а также утилиты для настройки и управления Android-устройствами. Они были добавлены в вирусную базу как Android.Joker.613, Android.Joker.614, Android.Joker.617, Android.Joker.618, Android.Joker.620, Android.Joker.622, Android.Joker.624, Android.Joker.630 и Android.Joker.632.

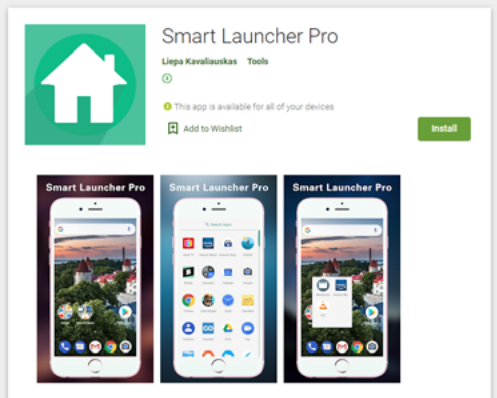
«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2021 года

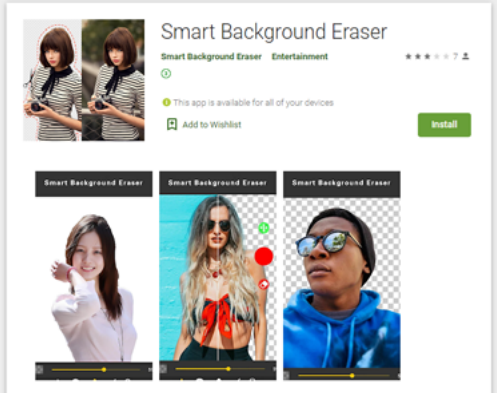
Угрозы в Google Play

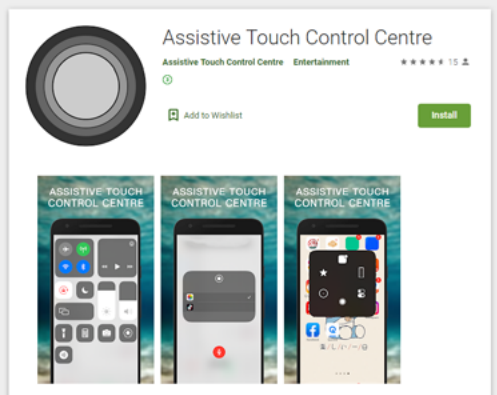












Для защиты Android-устройств от вредоносных и нежелательных программ пользователям следует установить антивирусные продукты Dr.Web для Android.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2021 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
125124, 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