Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2019 года

Обзор вирусной активности для мобильных устройств в феврале 2019 года

1 марта 2019 года

Последний зимний месяц этого года для пользователей Android-устройств оказался неспокойным. В середине февраля специалисты компании «Доктор Веб» обнаружили в каталоге Google Play порядка 40 троянцев семейства Android.HiddenAds. Злоумышленники распространяли их при помощи рекламы в популярных социальных сетях и онлайн-сервисах. Кроме того, владельцам Android-смартфонов и планшетов угрожали троянцы Android.FakeApp, которых киберпреступники применяли в мошеннических схемах, троянцы-загрузчики, а также другие вредоносные и нежелательные приложения.

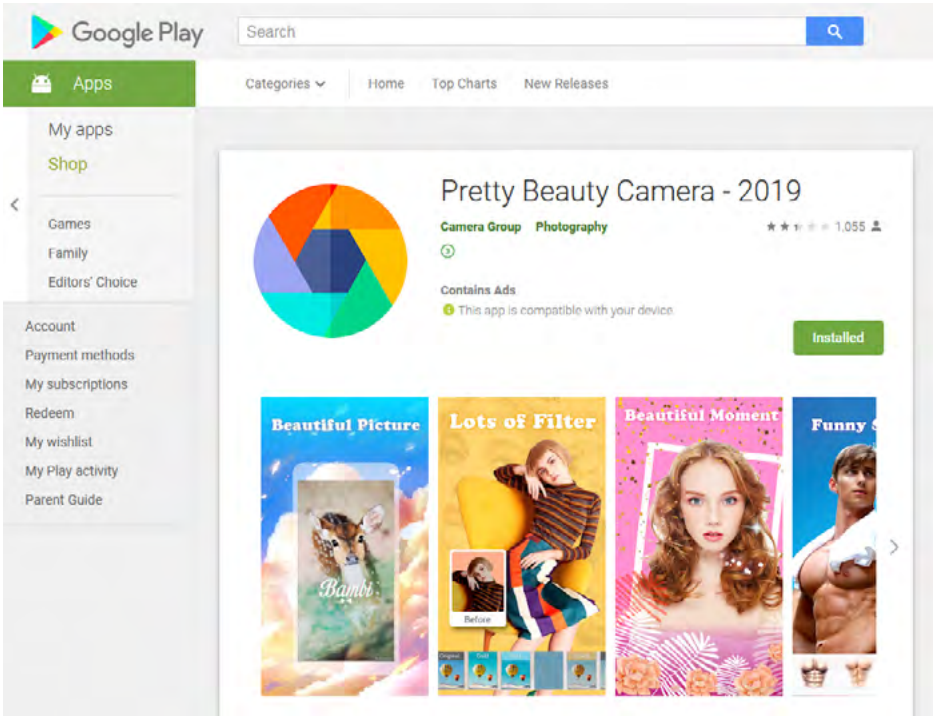
Главные тенденции февраля

- Обнаружение вредоносных программ в каталоге Google Play

Обзор вирусной активности для мобильных устройств в феврале 2019 года

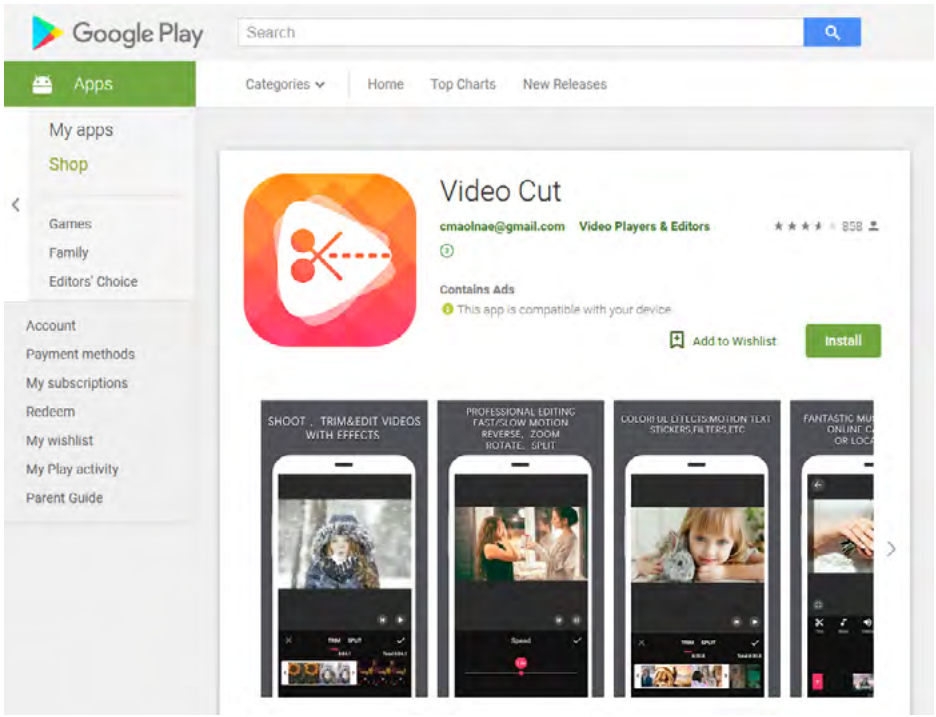
Мобильная угроза месяца

В прошедшем месяце вирусные аналитики «Доктор Веб» выявили в каталоге Google Play 39 троянцев семейства Android.HiddenAds. Злоумышленники активно рекламировали троянцев в популярных онлайн-сервисах с многомиллионной аудиторией, таких как YouTube и WhatsApp. Киберпреступники предлагали установить мощные программы для редактирования фотографий и видео, однако на самом деле владельцы смартфонов и планшетов инсталлировали троянцев с минимальным набором функций. Жертвами злоумышленников стали порядка 10 000 000 пользователей.

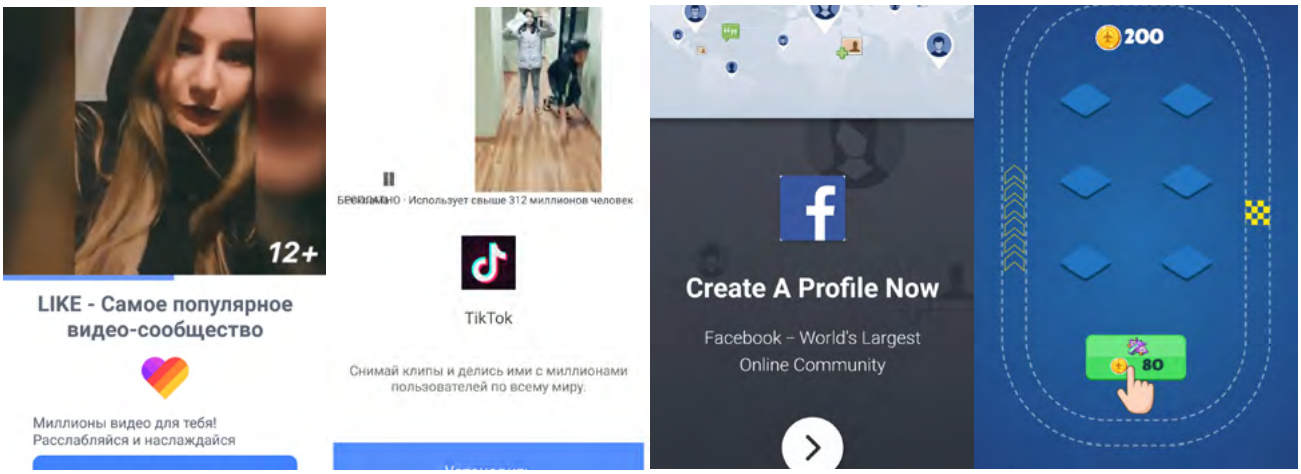


Обзор вирусной активности для мобильных устройств в феврале 2019 года

Мобильная угроза месяца



Эти троянцы постоянно показывали рекламу, перекрывая баннерами интерфейс других программ и даже самой операционной системы. В результате работать с зараженными устройствами становилось очень неудобно.



Подробнее об этих вредоносных приложениях рассказано в новостной публикации на нашем сайте.

Обзор вирусной активности для мобильных устройств в феврале 2019 года

По данным антивирусных продуктов Dr.Web для Android

Android.Backdoor.682.origin

Android.Backdoor.2080

Троянцы, которые выполняют команды злоумышленников и позволяют им контролировать зараженные мобильные устройства.

Android.RemoteCode.197.origin

Вредоносное приложение, предназначенное для загрузки и выполнения произвольного кода.

Android.HiddenAds.261.origin

Android.HiddenAds.659

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

Обзор вирусной активности для мобильных устройств в феврале 2019 года

По данным антивирусных продуктов Dr.Web для Android

Adware.Zeus.1

Adware.Patacore.1.origin

Adware.Patacore.168

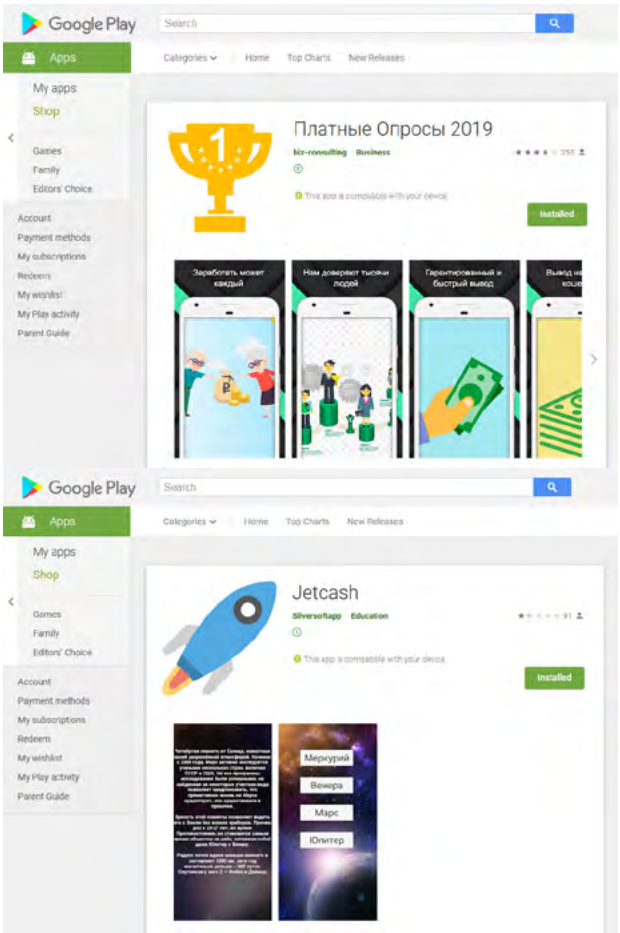
Adware.Jiubang.2

Adware.Toofan.1.origin

Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

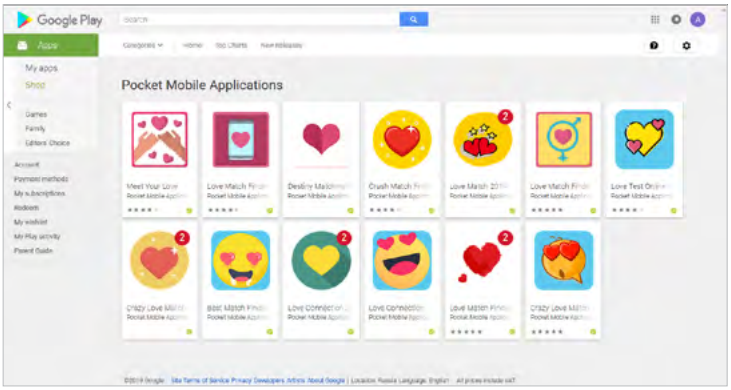
Угрозы в Google Play

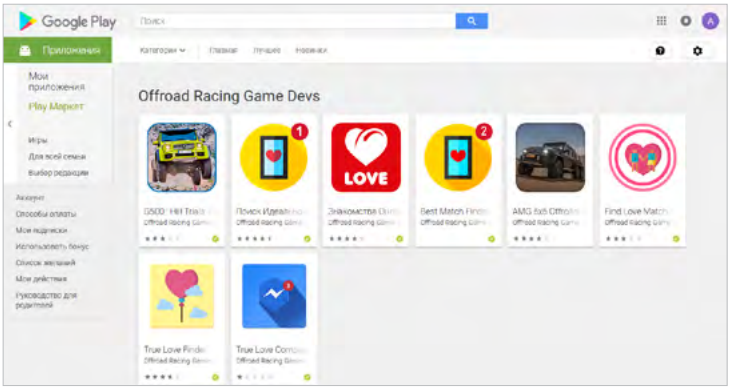
Наряду с троянцами Android.HiddenAds в Google Play были найдены и другие вредоносные программы. Среди них — очередные троянцы семейства Android.FakeApp, такие как Android.FakeApp.155, Android.FakeApp.154, Android.FakeApp.158. Интернет-жулики использовали их для мошенничества. Пользователям предлагалось установить приложения для прохождения онлайн-опросов, за которые якобы положено большое денежное вознаграждение. Троянцы загружали веб-сайты с такими «опросами», где после ответа на несколько простых вопросов у потенциальных жертв запрашивался некий проверочный платеж. Он якобы был необходим для перевода средств участнику опроса. Если пользователи соглашались на оплату, никакого вознаграждения они не получали.



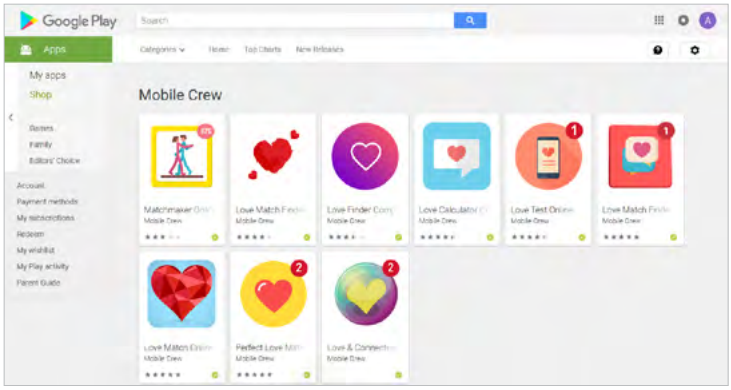
Также владельцам Android-устройств угрожал троянец Android.RemoteCode.2958, который загружал другие вредоносные программы. Он распространялся под видом безобидных игр и приложений и скачивал из Интернета произвольный код.

Угрозы в Google Play



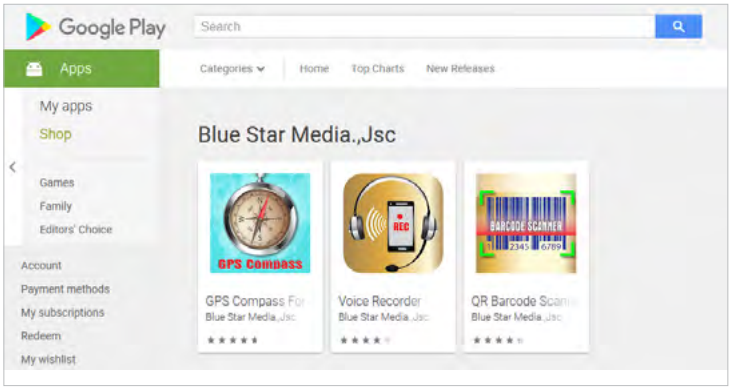


Другой троянец, получивший имя Android.Proxy.4, использовал зараженные устройства в качестве прокси-серверов, перенаправляя через них сетевой трафик киберпреступников. Как и другие вредоносные программы, он скрывался во внешне безобидных и полезных приложениях.

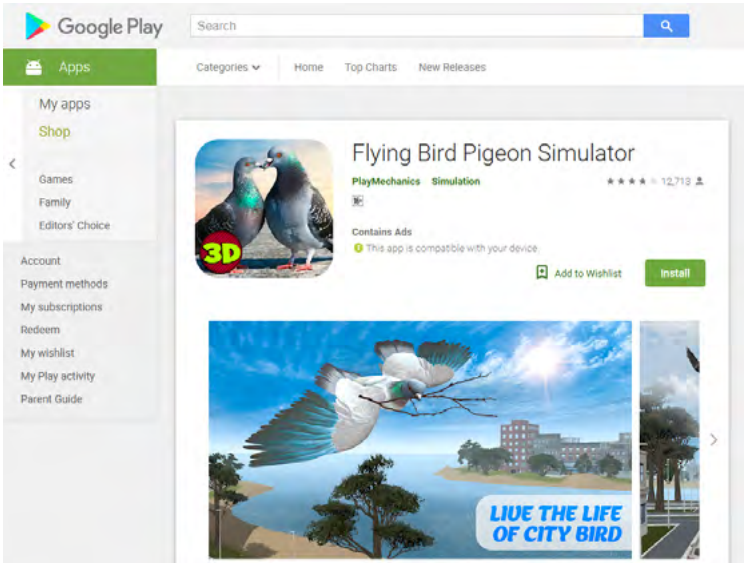


Угрозы в Google Play

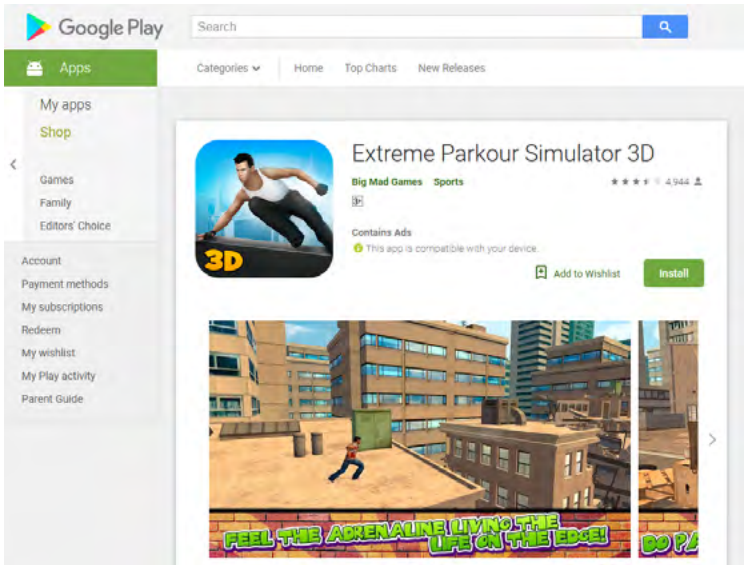
Кроме того, в вирусную базу Dr.Web была добавлена запись для детектирования приложений со встроенным нежелательным модулем Adware.Sharf.2. Он показывал рекламу, которая перекрывала окна программ и системный интерфейс. Вирусные аналитики «Доктор Веб» обнаружили Adware.Sharf.2 в различных программах — диктофоне, GPS-компасе и сканере QR-кодов.

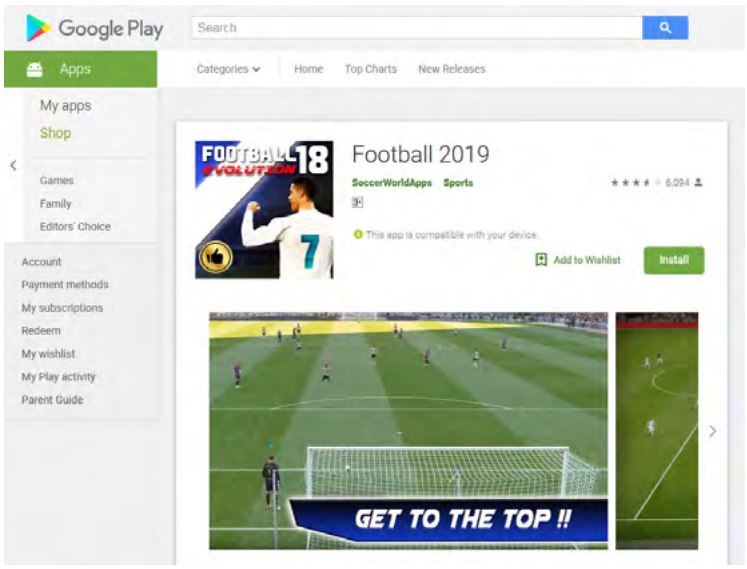


А в нескольких играх скрывались другие нежелательные рекламные модули, получившие по классификации Dr.Web имена Adware.Patacore.2 и Adware.Patacore.168. Они также показывали надоедливые баннеры.



Угрозы в Google Play





В каталоге Google Play выявляются все новые вредоносные и нежелательные приложения, поэтому владельцам мобильных Android-устройств необходимо устанавливать программы только от известных и проверенных разработчиков. Кроме того, следует обращать внимание на отзывы других пользователей. Для защиты смартфонов и планшетов следует установить антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных устройств в феврале 2019 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