Dr.WEB®
с 1992 года

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

Обзор вирусной активности для мобильных устройств в июне 2019 года

3 июля 2019 года

В середине июня вирусные аналитики «Доктор Веб» обнаружили в Google Play вредоносную программу Android.FakeApp.174, которая загружала веб-сайты, где пользователей Android-устройств подписывали на спам-уведомления. Кроме того, в течение месяца были найдены новые троянцы семейства Android.HiddenAds, предназначенные для показа рекламы, и троянцы-загрузчики Android.DownLoader, скачивавшие другие вредоносные приложения. Также были выявлены прочие Android-угрозы.

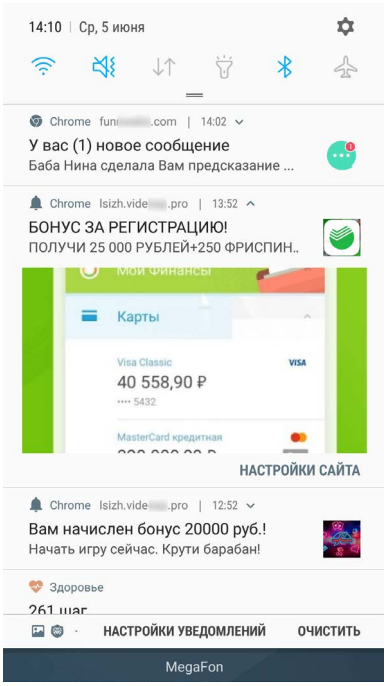
Главная тенденция июня

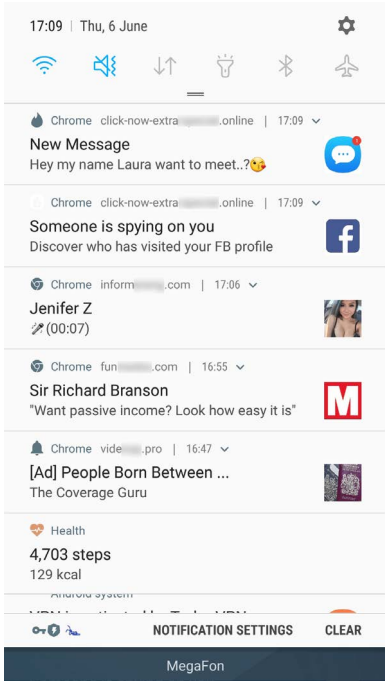
- Появление новых вредоносных и нежелательных программ в Google Play

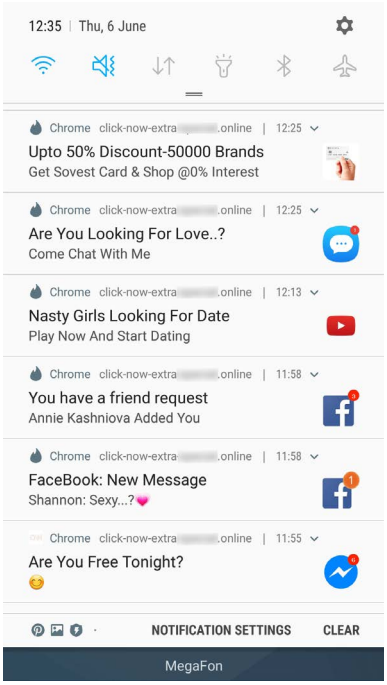
Обзор вирусной активности для мобильных устройств в июне 2019 года

Мобильная угроза месяца

14 июня компания «Доктор Веб» рассказала о троянце Android.FakeApp.174, загружавшем сомнительные веб-сайты. На них пользователям Android-устройств обманом предлагалось подписаться на получение уведомлений. В случае согласия жертвам начинали приходить десятки спам-сообщений, которые те могли принять за уведомления от установленных программ или операционной системы.







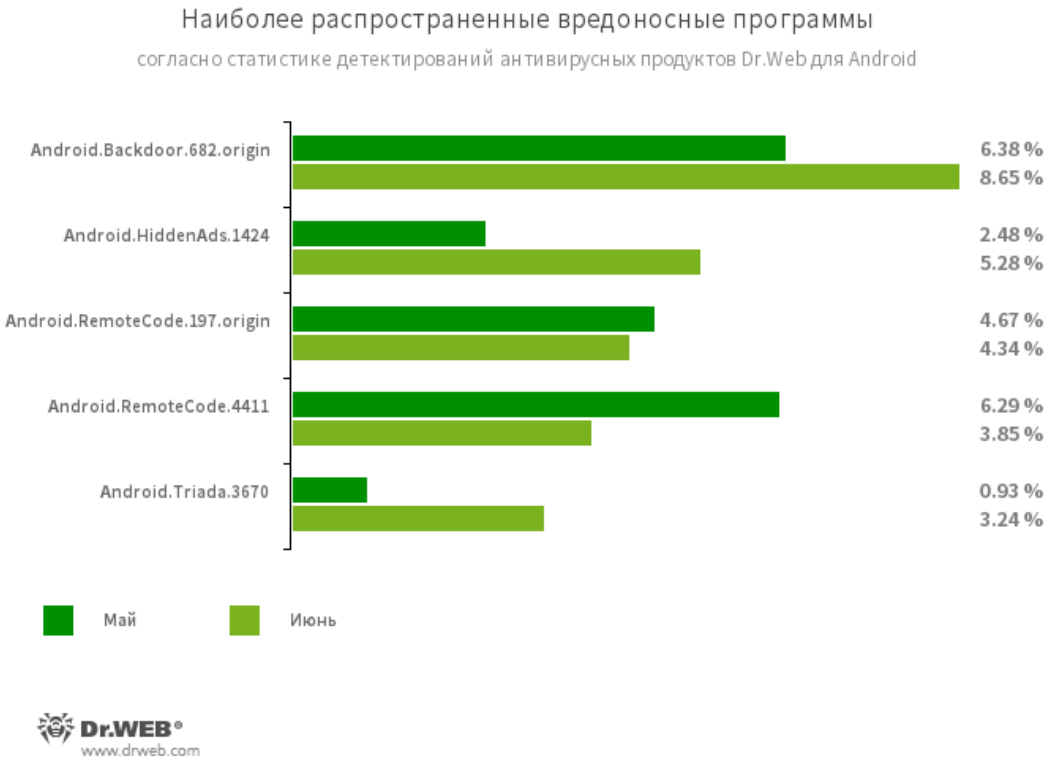
При нажатии на такое сообщение в браузере открывался один из рекламируемых сайтов. Многие из них были мошенническими.

Особенности Android.FakeApp.174:

- распространялся через Google Play под видом официальных программ известных брендов;
- уведомления с веб-сайтов, которые загружал троянец, приходили даже после его удаления.

Обзор вирусной активности для мобильных устройств в июне 2019 года

По данным антивирусных продуктов Dr.Web для Android



Android.Backdoor.682.origin

Троянец, который выполняет команды злоумышленников и позволяет им контролировать зараженные мобильные устройства.

Android.HiddenAds.1424

Троянец, предназначенный для показа навязчивой рекламы. Распространяется под видом популярных приложений.

Android.RemoteCode.197.origin

Android.RemoteCode.4411

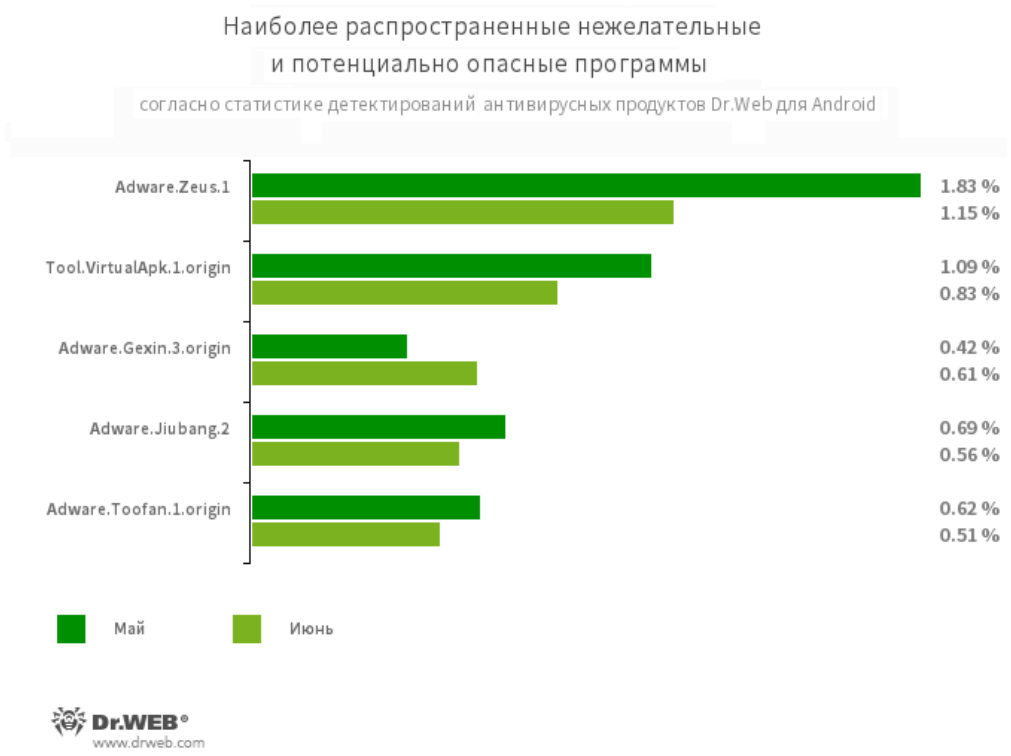
Вредоносные приложения, предназначенные для загрузки и выполнения произвольного кода.

Android.Triada.3670

Многофункциональный троянец, выполняющий разнообразные вредоносные действия.

Обзор вирусной активности для мобильных устройств в июне 2019 года

По данным антивирусных продуктов Dr.Web для Android



Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах:

Adware.Zeus.1

Adware.Jiubang.2

Adware.AdPush.33.origin

Adware.Toofan.1.origin

Потенциально опасная программная платформа, которая позволяет приложениям запускать apk-файлы без их установки:

Tool.VirtualApk.1.origin

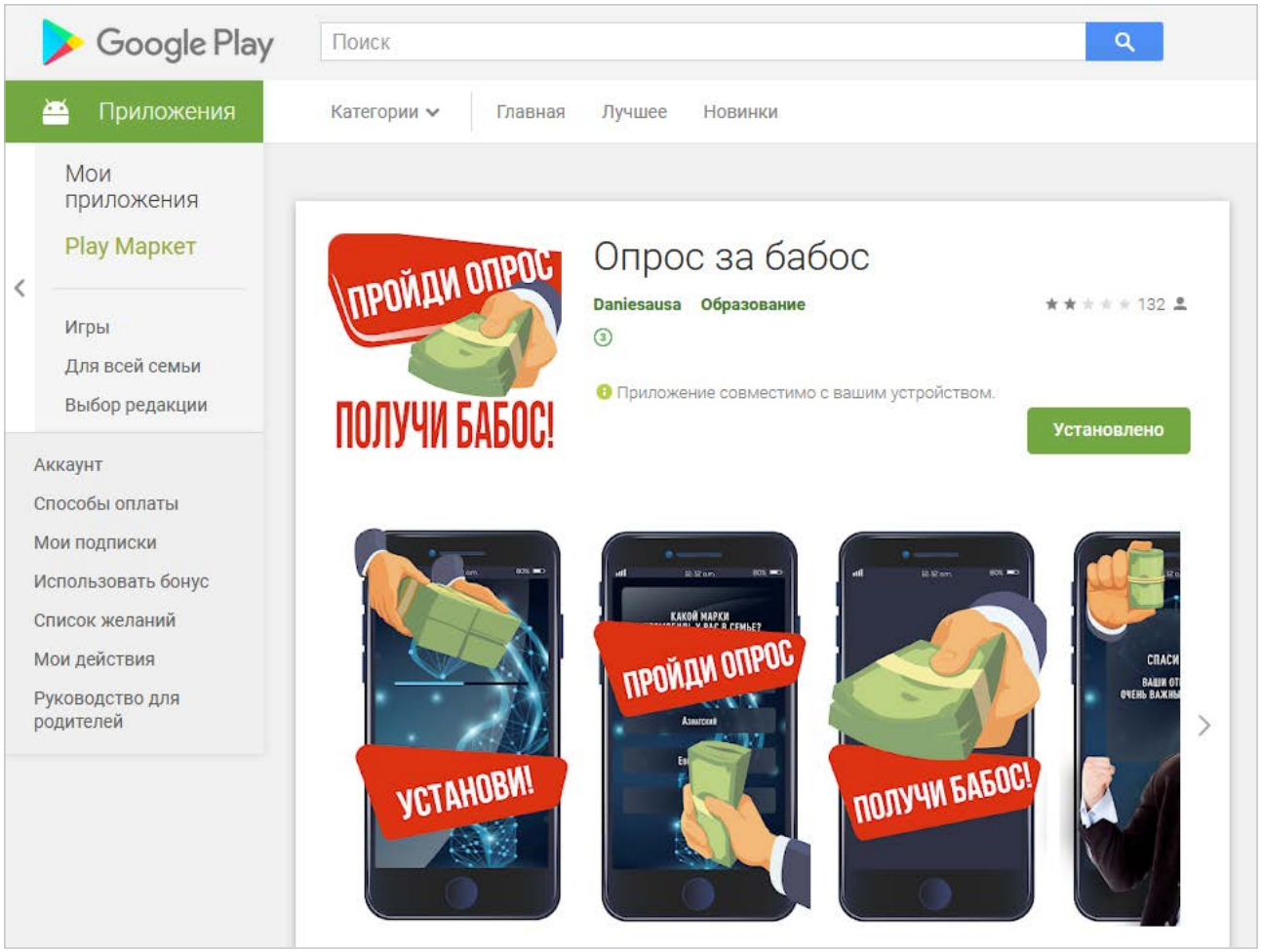
Новая угроза:

Adware.Patacore.253

Представитель семейства нежелательных модулей, показывающих рекламные баннеры на Android-устройствах.

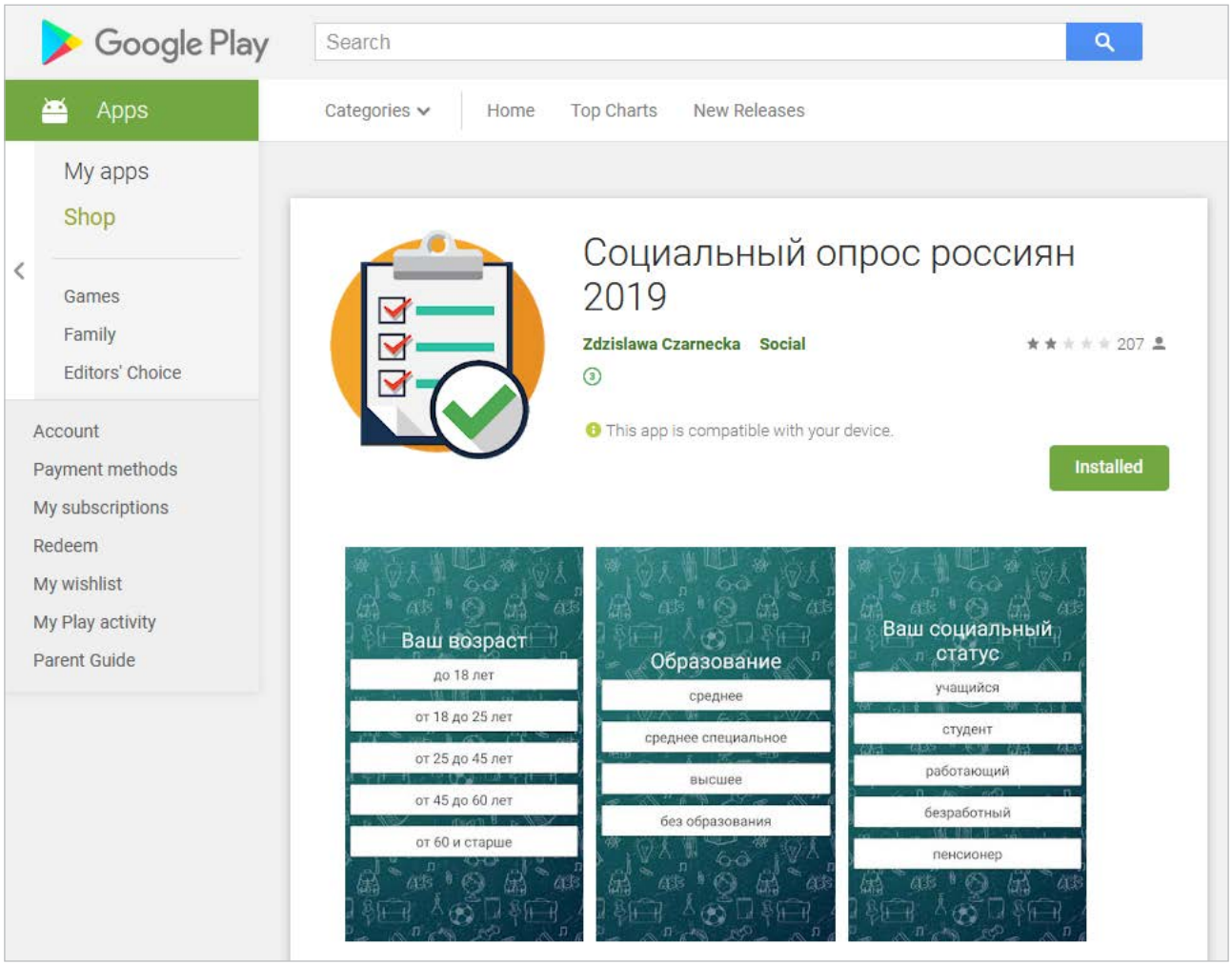
Угрозы в Google Play

Вместе с Android.FakeApp.174 в каталоге Google Play были найдены другие вредоносные и нежелательные программы. Среди них — троянцы того же семейства, получившие имена Android.FakeApp.151 и Android.FakeApp.173. Они распространялись под видом программ для заработка на онлайн-опросах. При запуске вредоносные приложения загружали мошеннические веб-сайты, где потенциальным жертвам предлагалось ответить на несколько вопросов. Для получения «вознаграждения» от них требовалось заплатить некий налог или комиссию, однако никаких денег после этого они не получали.



Обзор вирусной активности для мобильных устройств в июне 2019 года

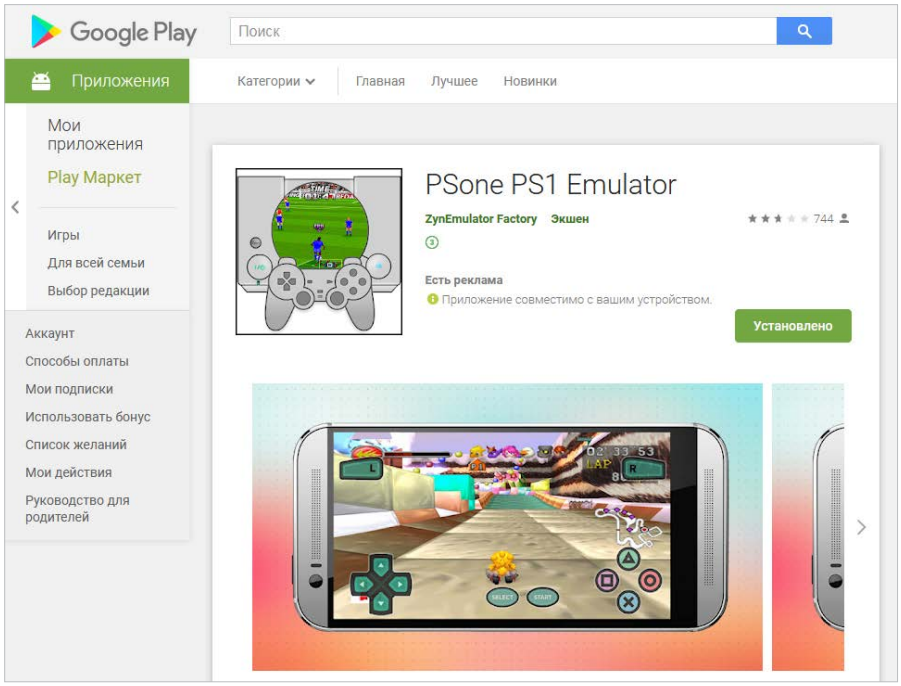
Угрозы в Google Play

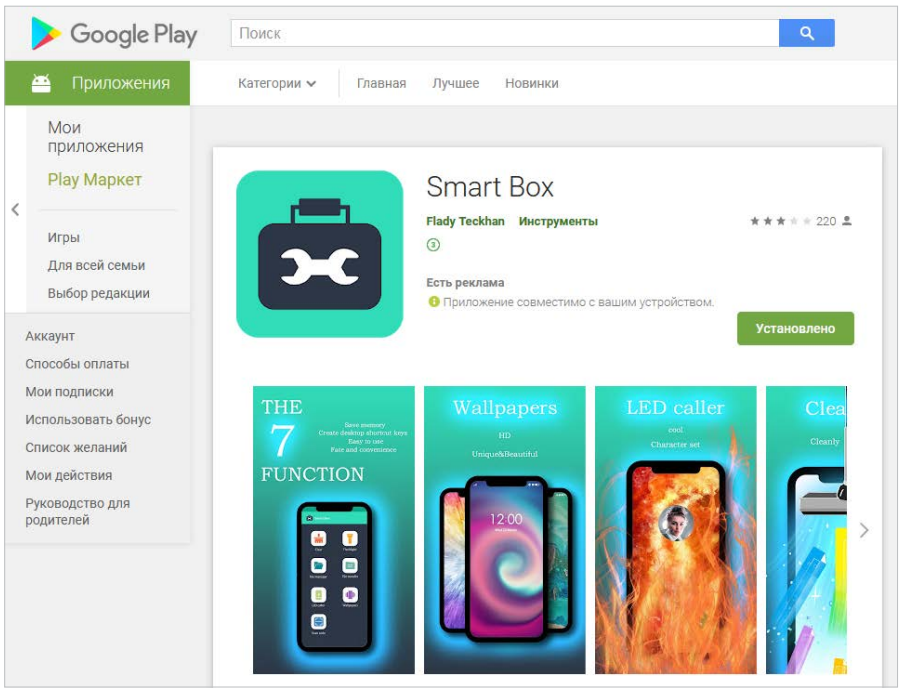


Также вирусные аналитики обнаружили множество новых троянцев Android.HiddenAds. Злоумышленники выдавали их за полезные приложения — различные игры и утилиты. В общей сложности их установили свыше 3 380 000 пользователей.

Обзор вирусной активности для мобильных устройств в июне 2019 года

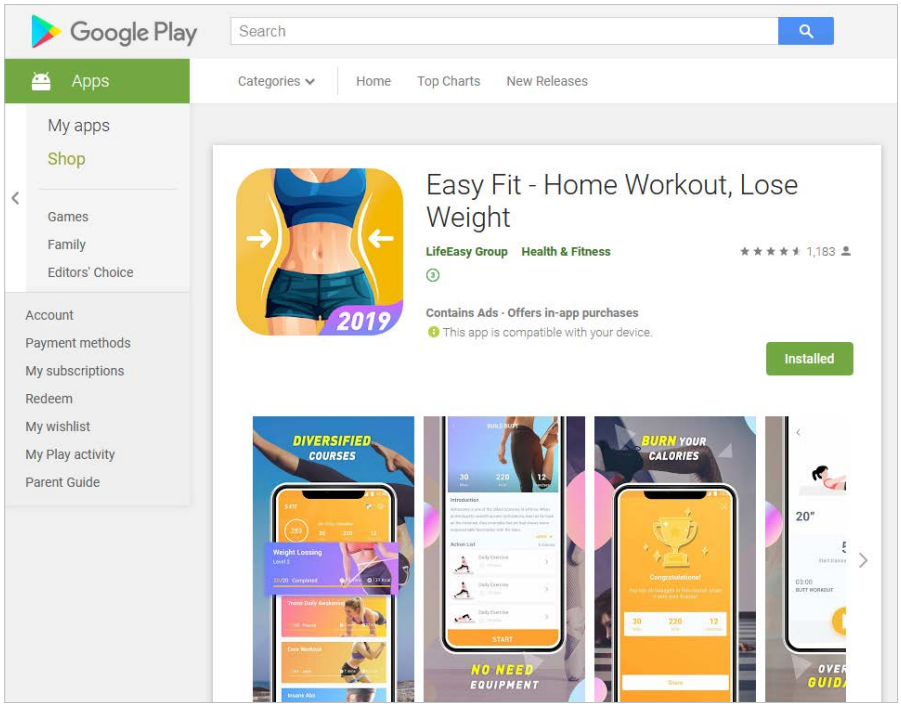
Угрозы в Google Play

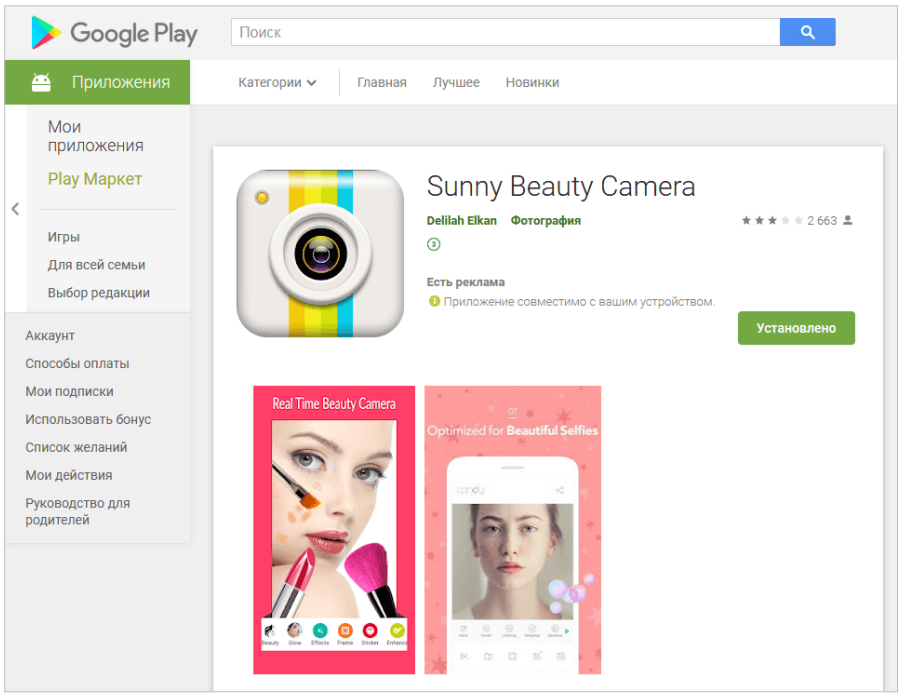




Обзор вирусной активности для мобильных устройств в июне 2019 года

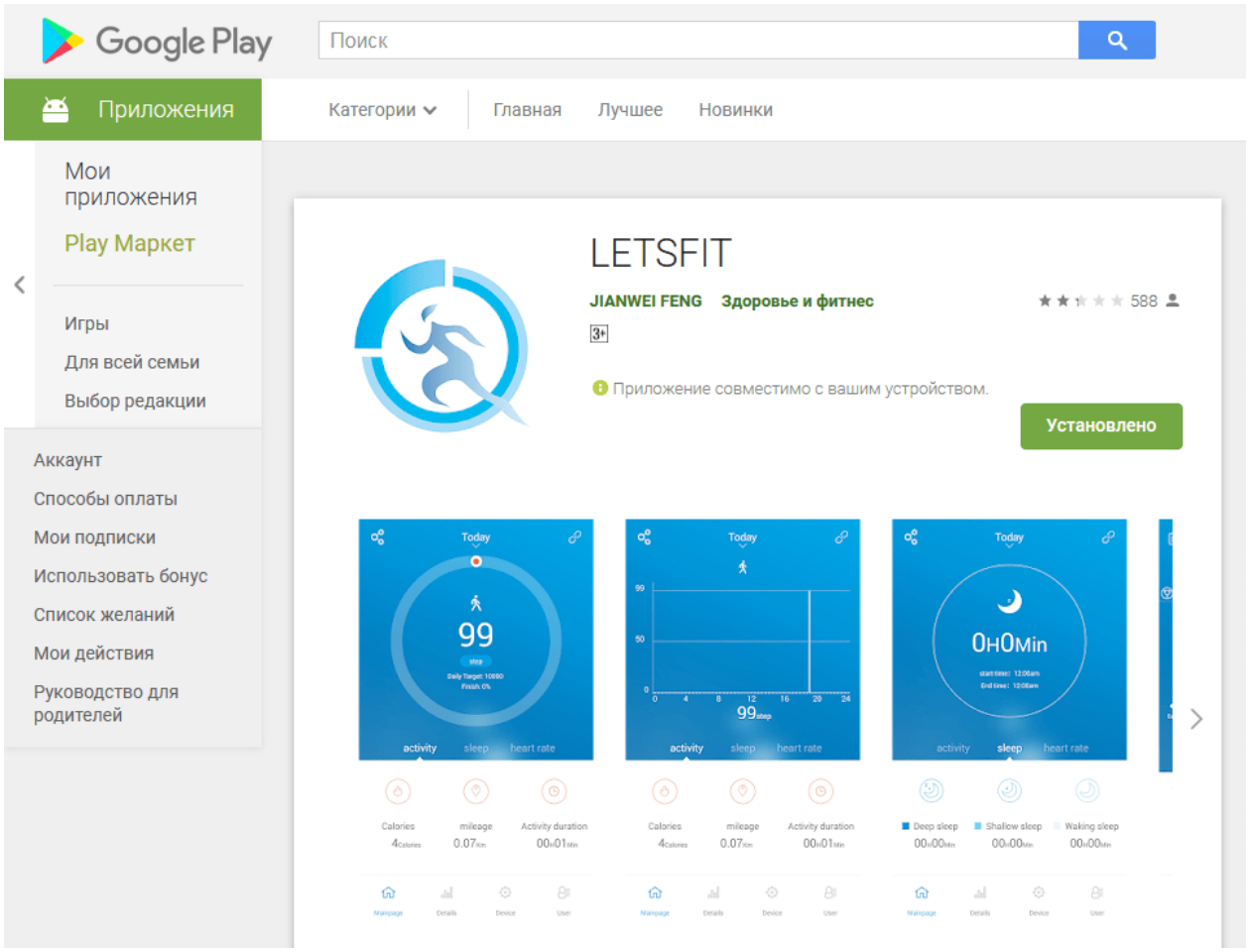
Угрозы в Google Play





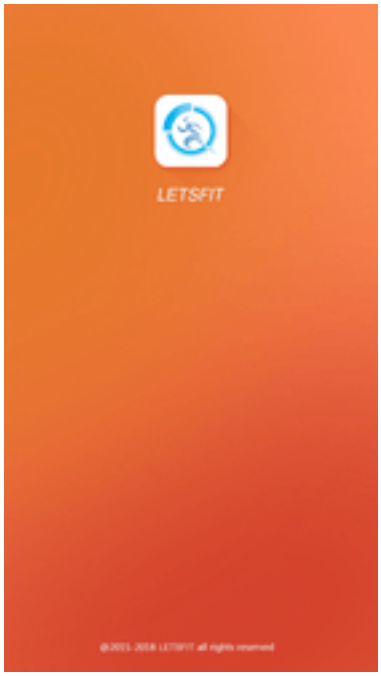
После установки и запуска эти вредоносные программы скрывали свои значки и начинали показывать рекламу.

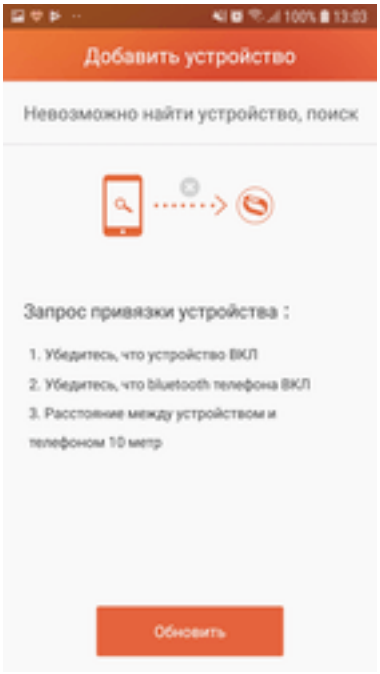
Другой троянец, обнаруженный в Google Play, получил имя Android.DownLoader.**3200**. Он был встроен в программу управления фитнес-браслетами LETSCOM Smart Bracelet, которую установили свыше 50 000 пользователей.



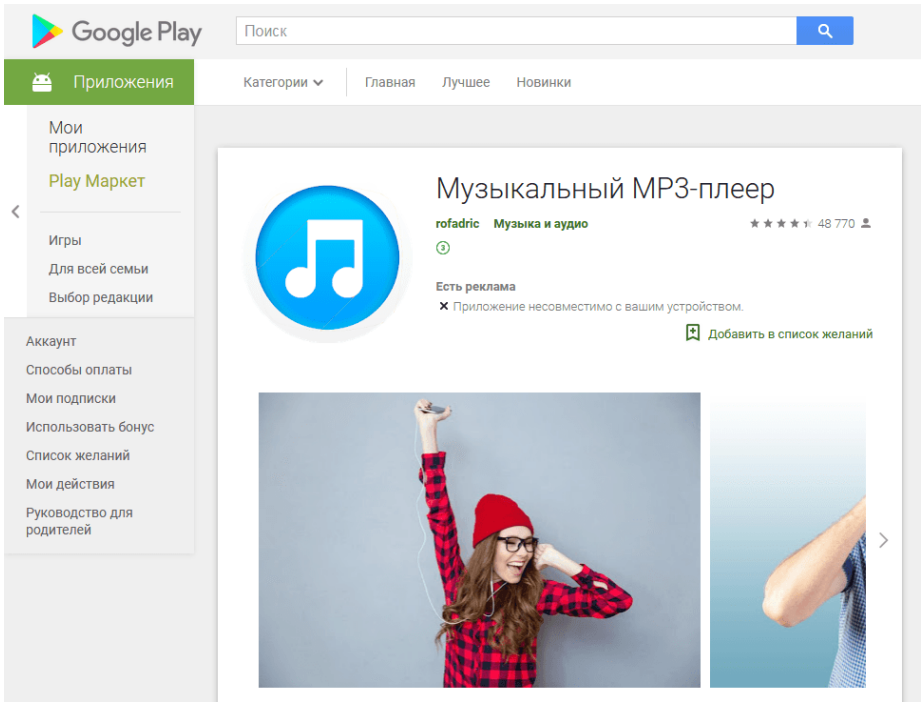
Первые версии этого приложения были безопасными, однако позднее, в версиях 1.1.0 и 1.1.4, у него появился троянский функционал. Android.DownLoader.**3200** скачивал на мобильные устройства других троянцев.

Обзор вирусной активности для мобильных устройств в июне 2019 года



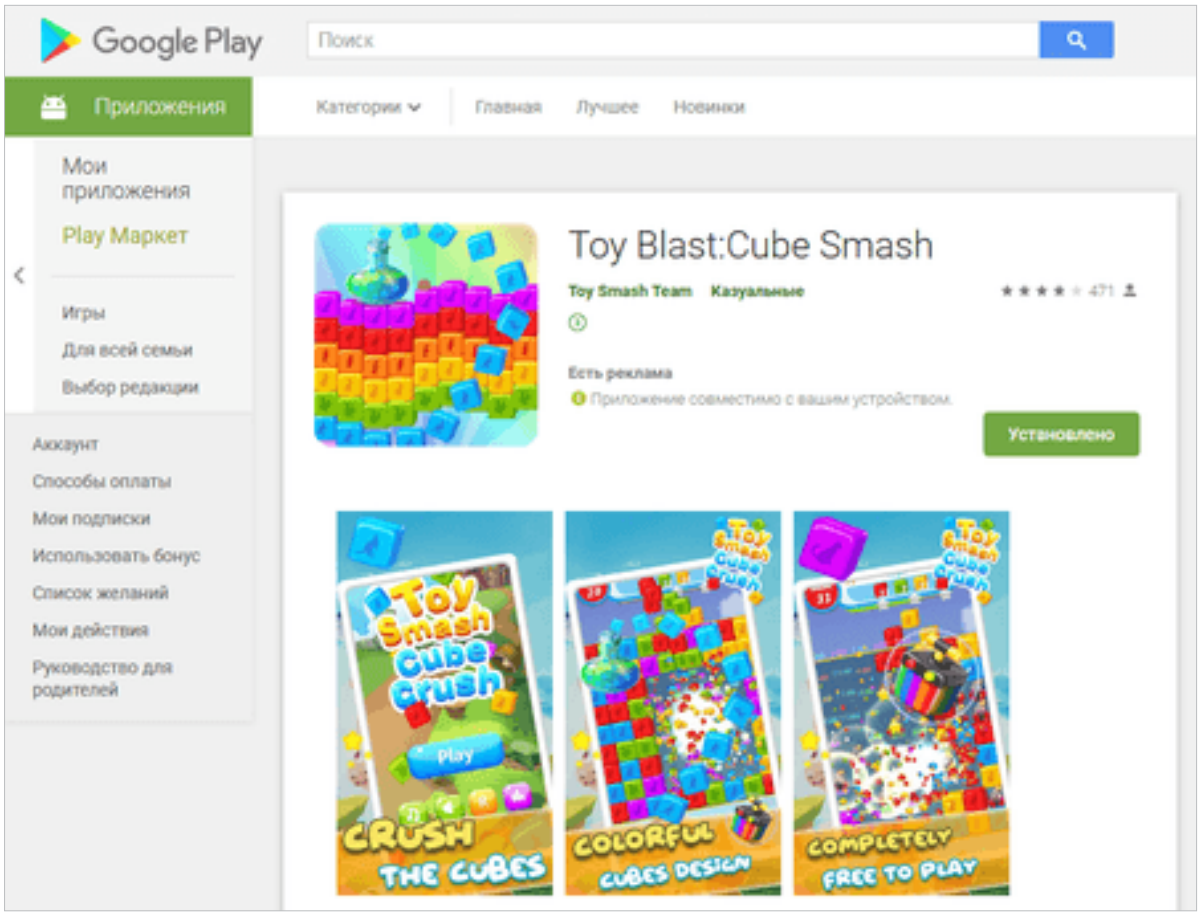


Еще один загрузчик получил имя Android.DownLoader.681.origin. Как и Android.DownLoader.3200, он распространялся под видом безопасной программы, в данном случае — аудиоплеера. Android.DownLoader.681.origin скачивал вредоносные приложения и пытался установить их.



Угрозы в Google Play

В конце июня в вирусную базу Dr.Web была добавлена запись для детектирования нежелательного программного модуля Adware.OneOceans.2.origin, предназначенного для показа рекламы. Он был встроен в игру Toy Blast: Cube Smash, которую загрузили более 100 000 пользователей.



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

Обзор вирусной активности для мобильных устройств в июне 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.drweb.ru | www.антивирус.рф | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах