

«Доктор Веб»: обзор вирусной активности для мобильных устройств в июне 2018 года



Обзор вирусной активности для мобильных устройств в июне 2018 года

3 июля 2018 года

В июне 2018 года вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play более 30 приложений со встроенным рекламным модулем **Adware.Appalytic.1.origin**. Он показывал уведомления с предложением загрузить различное ПО, а также открывал в Google Play страницы рекламируемых программ. Кроме того, специалисты «Доктор Веб» обнаружили в официальном каталоге Android-приложений несколько новых троянцев семейства [Android.FakeApp](#), по команде злоумышленников загружавших веб-сайты. Помимо этого, в прошедшем месяце под видом эротической игры киберпреступники распространяли троянца [Android.Spy.461.origin](#), который шпионил за владельцами Android-смартфонов и планшетов. Также в июне пользователям мобильных устройств угрожал троянец [Android.SmsSend.1989.origin](#), отправлявший платные СМС-сообщения на премиум-номера.

Главные тенденции июня

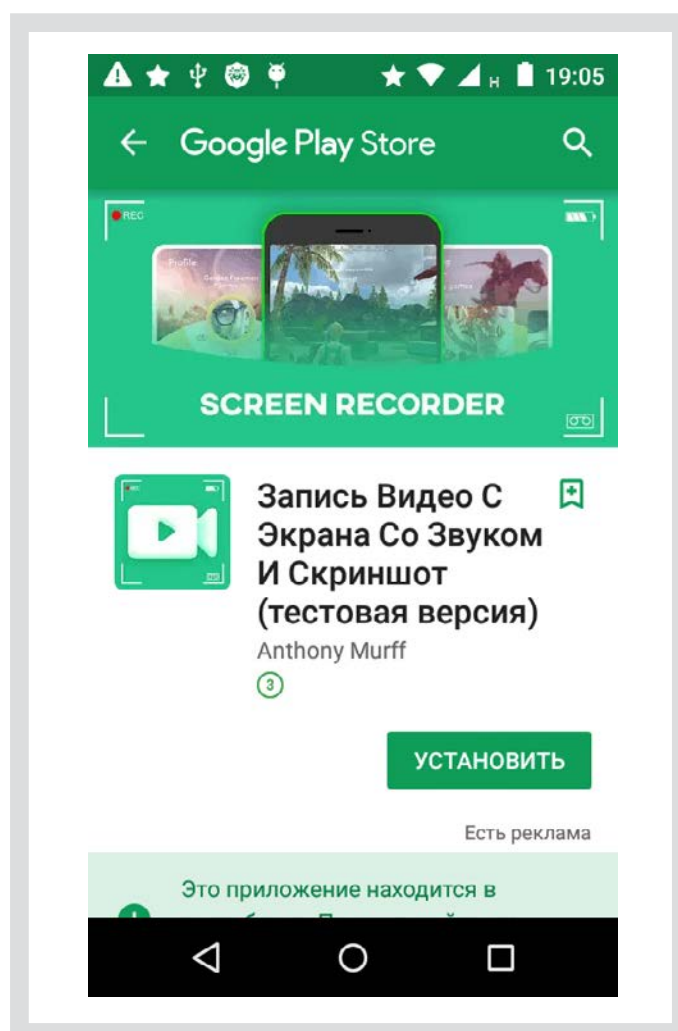
- Обнаружение в каталоге Google Play программ со встроенным нежелательным рекламным модулем
- Распространение троянца-шпиона

Обзор вирусной активности для мобильных устройств в июне 2018 года

Мобильная угроза месяца

В начале июня специалисты «Доктор Веб» обнаружили в каталоге Google Play 37 программ, в которых находился нежелательный рекламный модуль **Adware.Appalytic.1.origin**. Он настойчиво предлагал загрузить и установить различные приложения и игры. Кроме того, **Adware.Appalytic.1.origin** самостоятельно открывал в Google Play страницы рекламируемых программ.

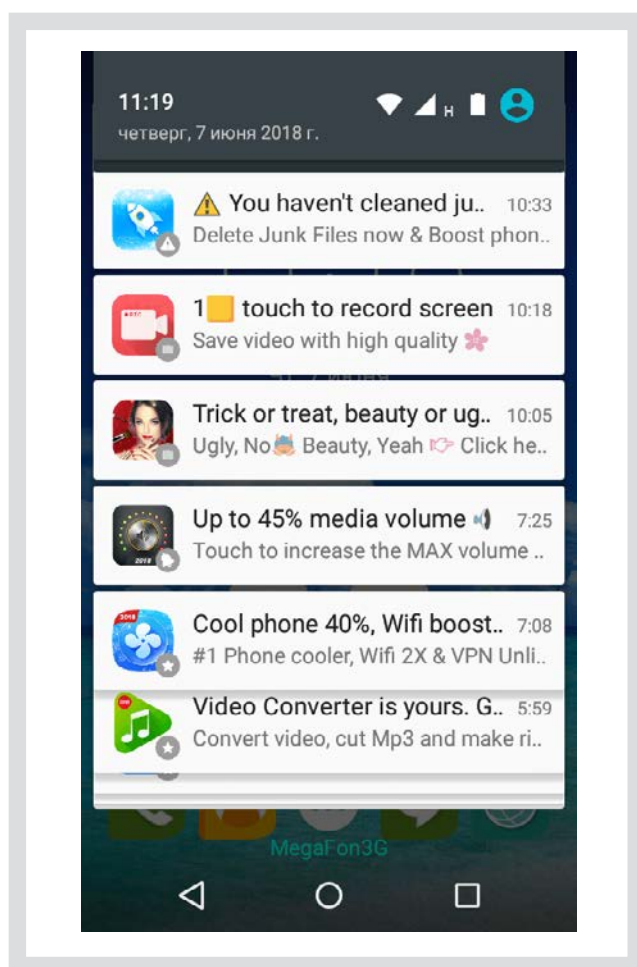
Пример рекламируемого приложения из каталога Google Play:



Обзор вирусной активности для мобильных устройств в июне 2018 года

Мобильная угроза месяца

Пример уведомлений, которые показывает этот модуль:



Особенности Adware.Appalytic.1.origin:

- встроен в безобидные приложения, распространяемые через Google Play;
- получает команды через облачный сервис Firebase;
- самостоятельно открывает каталог Google Play и загружает в нем страницы рекламируемых приложений;
- отображает в панели уведомлений надоедливые сообщения с предложением скачать и установить различные программы.

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

Обзор вирусной активности для мобильных устройств в июне 2018 года

По данным антивирусных продуктов Dr.Web для Android

Наиболее распространенные вредоносные программы согласно статистике детектирований антивирусных продуктов Dr.Web для Android



[Android.Mobifun.4](#)

Троянец, предназначенный для загрузки других Android-приложений.

[Android.HiddenAds.280.origin](#)

[Android.HiddenAds.288.origin](#)

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

[Android.SmsSend.1338.origin](#)

Вредоносная программа, отправляющая СМС на платные номера.

[Android.DownLoader.573.origin](#)

Троянец, предназначенный для загрузки других вредоносных приложений.

Обзор вирусной активности для мобильных устройств в июне 2018 года

По данным антивирусных продуктов Dr.Web для Android

Наиболее распространенные
нежелательные и потенциально опасные программы
согласно статистике детектирования антивирусных продуктов Dr.Web для Android



Adware.SalmonAds.3.origin

Adware.Jiubang.2

Adware.Appalytic.1.origin

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

Tool.SilentInstaller.1.origin

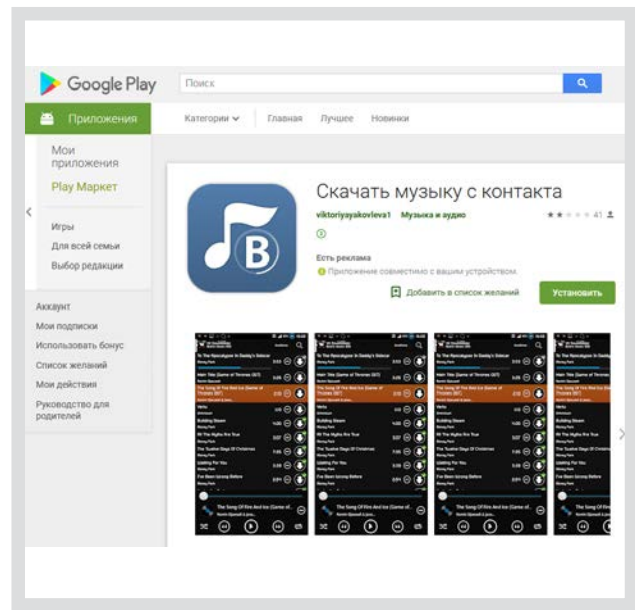
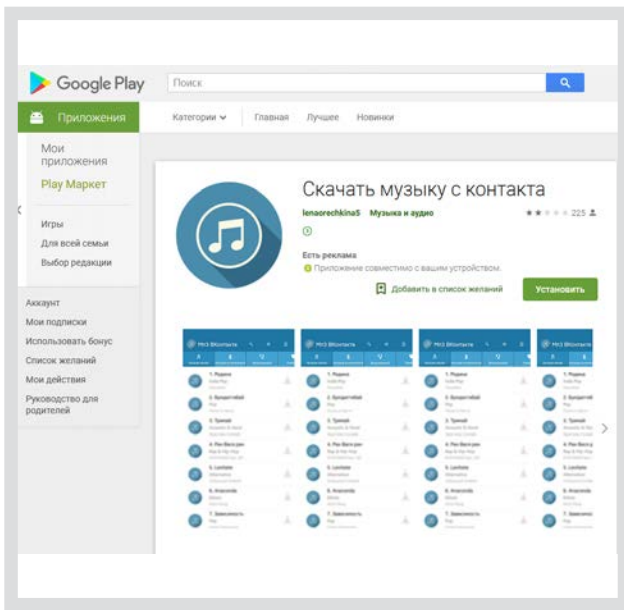
Потенциально опасная программа, предназначенная для незаметного запуска приложений без вмешательства пользователя.

Обзор вирусной активности для мобильных устройств в июне 2018 года

Троянцы в Google Play

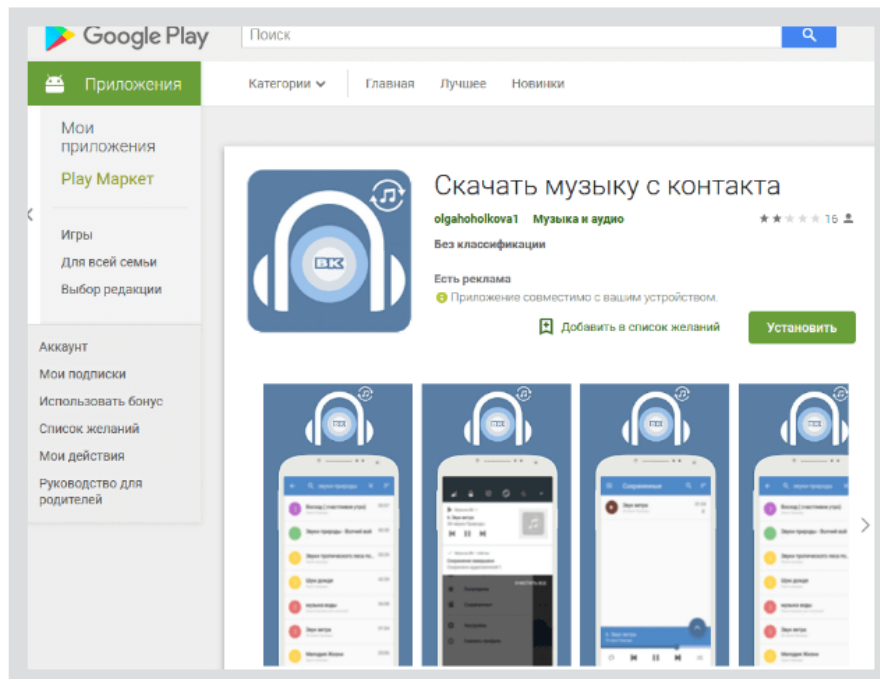
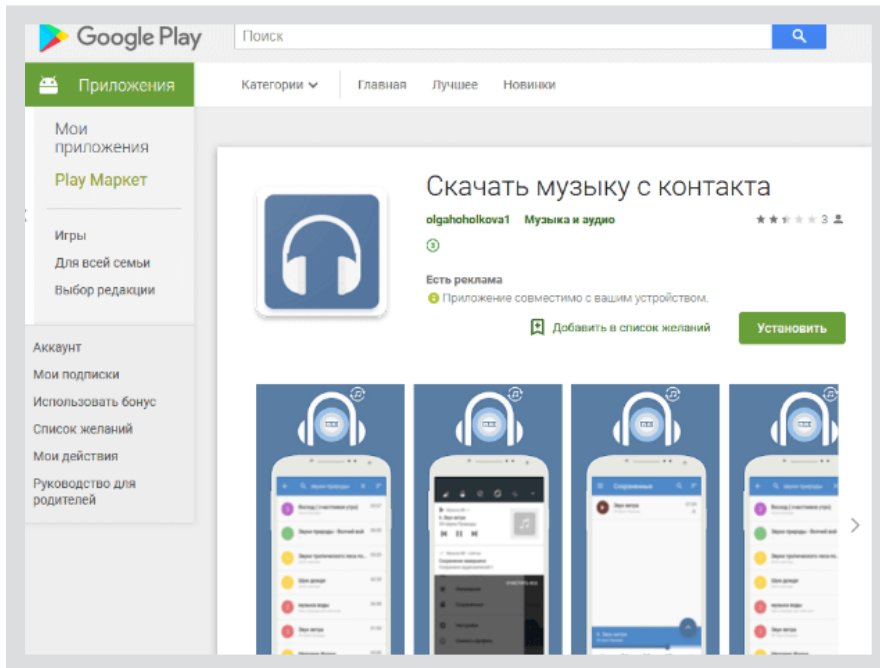
В конце июня специалисты «Доктор Веб» обнаружили в каталоге Google Play несколько новых троянцев семейства [Android.FakeApp](#). Как и ранее, эти вредоносные программы распространялись под видом полезных приложений – в частности, ПО для прослушивания музыки из социальной сети «ВКонтакте». Троянцы, добавленные в вирусную базу Dr.Web как [Android.FakeApp.89](#), [Android.FakeApp.90](#), [Android.FakeApp.91](#) и [Android.FakeApp.92](#), по команде злоумышленников переходили по заданным ими ссылкам и загружали различные веб-сайты, среди которых были мошеннические интернет-ресурсы.

На следующих изображениях показаны страницы загрузки обнаруженных в Google Play троянцев [Android.FakeApp](#):



Обзор вирусной активности для мобильных устройств в июне 2018 года

Троянцы в Google Play



Узнайте больше

Обзор вирусной активности для мобильных устройств в июне 2018 года

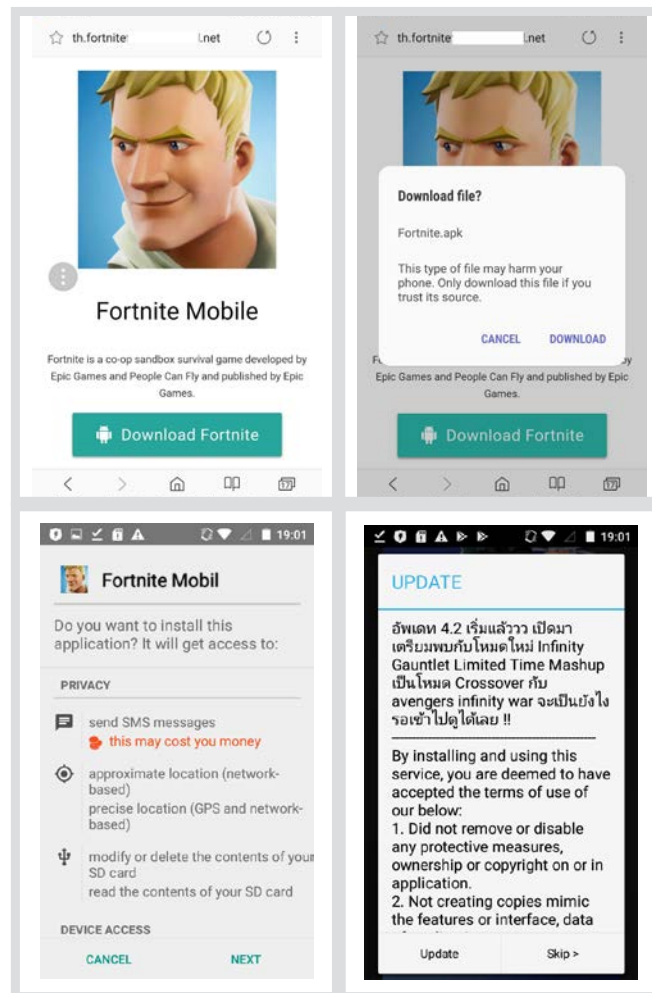
Android-шпион

В июне пользователям Android-смартфонов и планшетов угрожал троянец-шпион, которого злоумышленники распространяли под видом эротической игры. Эта вредоносная программа получила имя [Android.Spy.461.origin](#). Троянец похищал СМС-сообщения и контакты из телефонной книги, записывал окружение с использованием встроенного в мобильное устройство микрофона, получал список хранящихся на смартфоне или планшете файлов и мог загружать их на сервер злоумышленников. Кроме того, [Android.Spy.461.origin](#) крал данные из буфера обмена.

Обзор вирусной активности для мобильных устройств в июне 2018 года

СМС-троянец

В прошедшем месяце в злоумышленники распространяли СМС-троянца [Android.SmsSend.1989.origin](#), который отправлял сообщения на платные номера и подписывал пользователей на дорогостоящие услуги. Эта вредоносная программа скрывалась в приложении, которое киберпреступники выдавали за популярную игру Fortnite. При этом ее официальная версия для устройств под управлением ОС Android все еще находится в разработке и недоступна для игроков.



Злоумышленники по-прежнему атакуют мобильные устройства под управлением ОС Android и распространяют вредоносные и нежелательные программы не только с использованием различных веб-сайтов, но и через официальный каталог приложений Google Play. Для защиты смартфонов и планшетов пользователям необходимо установить антивирусные продукты Dr.Web для Android.

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

Обзор вирусной активности для мобильных устройств в июне 2018 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

[ВебиОметр](#) | [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](#)



© ООО «Доктор Веб»,
2003-2018

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)