



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



## Обзор вирусной активности для мобильных устройств в ноябре 2019 года

11 декабря 2019 года

В прошедшем ноябре вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play очередные угрозы. Среди них были новые модификации троянцев семейства [Android.Joker](#), подписывавшие пользователей на платные мобильные услуги. Киберпреступники вновь распространяли вредоносные программы семейства [Android.HiddenAds](#), которые показывали надоедливую рекламу. Кроме того, была обнаружена новая версия бэкдора [Android.Backdoor.735.origin](#), предназначенного для кибершпионажа.

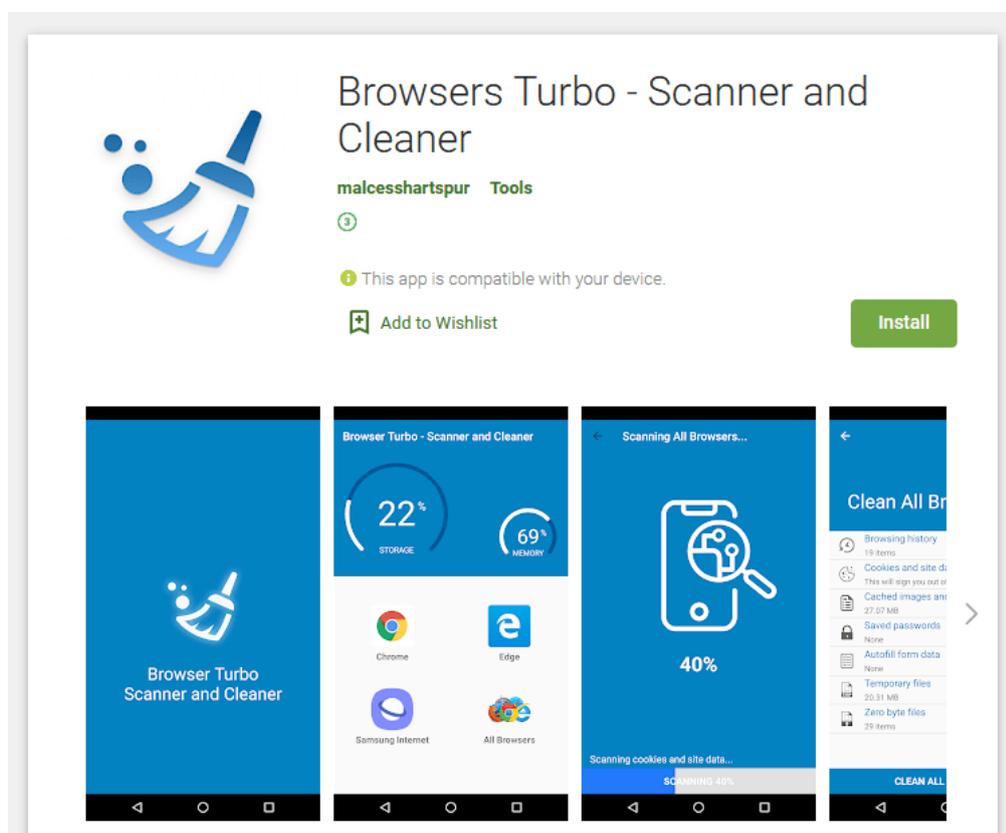
### Главные тенденции ноября

- Появление вредоносных программ в Google Play

# Обзор вирусной активности для мобильных устройств в ноябре 2019 года

## Мобильная угроза месяца

В ноябре специалисты «Доктор Веб» обнаружили в каталоге Google Play новую модификацию троянца [Android.Backdoor.735.origin](#) — компонента опасного бэкдора [Android.Backdoor.736.origin](#), о котором наша компания [сообщала](#) в июле. Эта вредоносная программа, также известная как PWNDROID1, распространялась под видом утилиты для настройки и ускорения работы браузера:

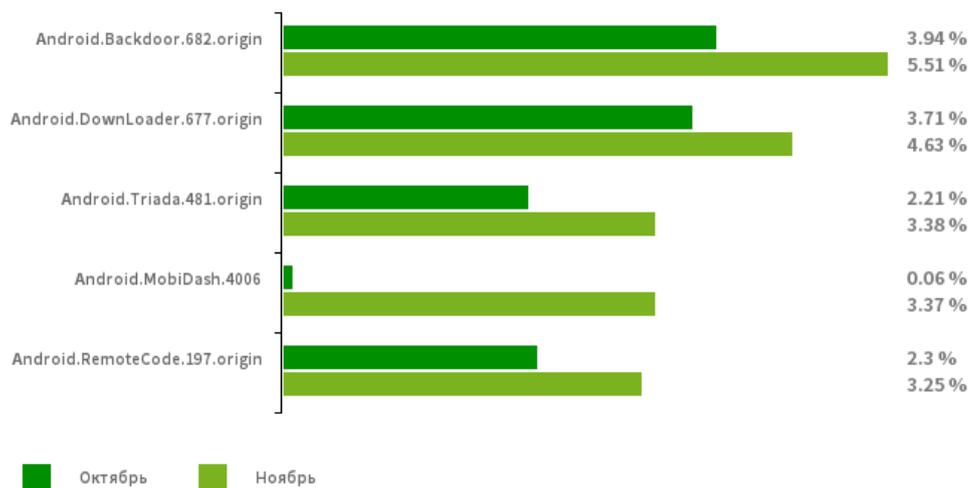


[Android.Backdoor.735.origin](#) выполняет команды злоумышленников, позволяет управлять зараженными Android-устройствами, шпионит за их владельцами и способен загружать и запускать дополнительные вредоносные компоненты.

# Обзор вирусной активности для мобильных устройств в ноябре 2019 года

## По данным антивирусных продуктов Dr.Web для Android

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



### [Android.Backdoor.682.origin](#)

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

### [Android.DownLoader.677.origin](#)

Загрузчик других вредоносных программ.

### [Android.Triada.481.origin](#)

Многофункциональный троянец, выполняющий разнообразные вредоносные действия.

### [Android.MobiDash.4006](#)

Троянская программа, показывающая надоедливую рекламу.

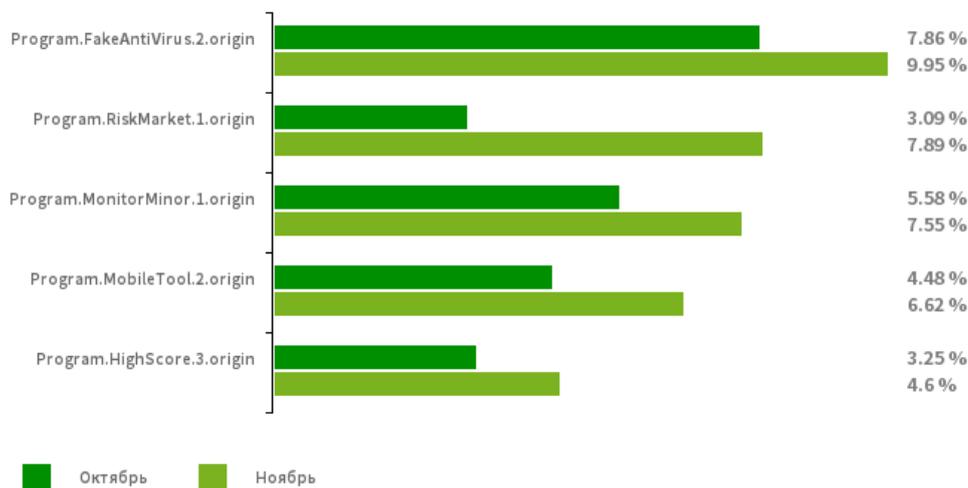
### [Android.RemoteCode.197.origin](#)

Вредоносное приложение, которое загружает и выполняет произвольный код.

# Обзор вирусной активности для мобильных устройств в ноябре 2019 года

## По данным антивирусных продуктов Dr.Web для Android

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



- **Program.FakeAntiVirus.2.origin**

Детектирование рекламных приложений, которые имитируют работу антивирусного ПО.

- **Program.RiskMarket.1.origin**

Магазин приложений, который содержит троянские программы и рекомендует пользователям их установку.

- **Program.HighScore.3.origin**

Каталог приложений, в котором через дорогостоящие СМС предлагается оплатить установку доступных в Google Play бесплатных программ.

- **Program.MonitorMinor.1.origin**

- **Program.MobileTool.2.origin**

Программы, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа.

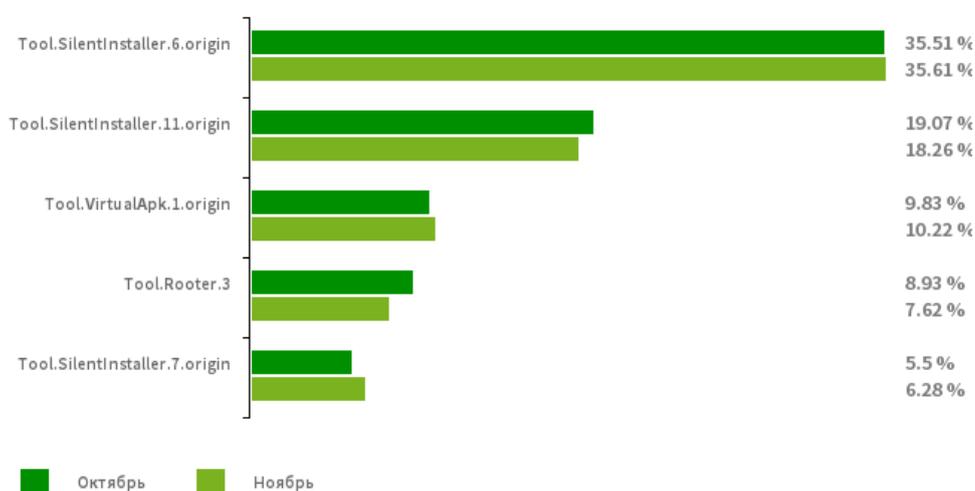
Узнайте больше

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

# Обзор вирусной активности для мобильных устройств в ноябре 2019 года

## По данным антивирусных продуктов Dr.Web для Android

Наиболее распространенные потенциально опасные программы  
согласно статистике детектирований 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 арк-файлы без их установки.

- **Tool.Rooter.3**

Утилита, предназначенная для получения root-полномочий на Android-устройствах. Может использоваться злоумышленниками и вредоносными программами.

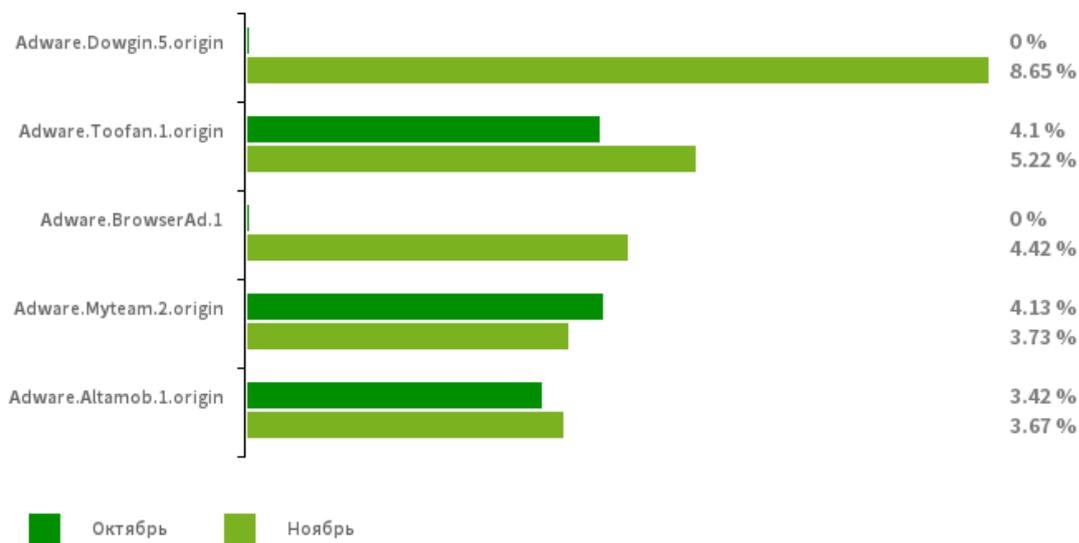
Узнайте больше

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

# Обзор вирусной активности для мобильных устройств в ноябре 2019 года

## По данным антивирусных продуктов Dr.Web для Android

Наиболее распространенные рекламные модули  
согласно статистике детектирования антивирусных продуктов Dr.Web для Android



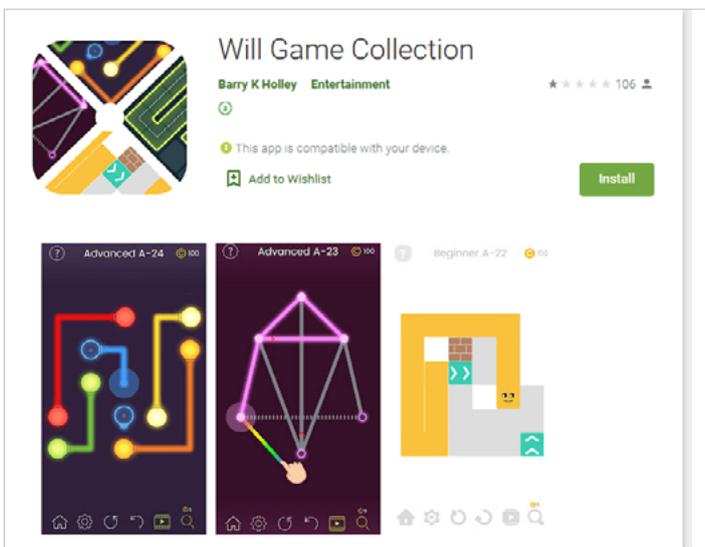
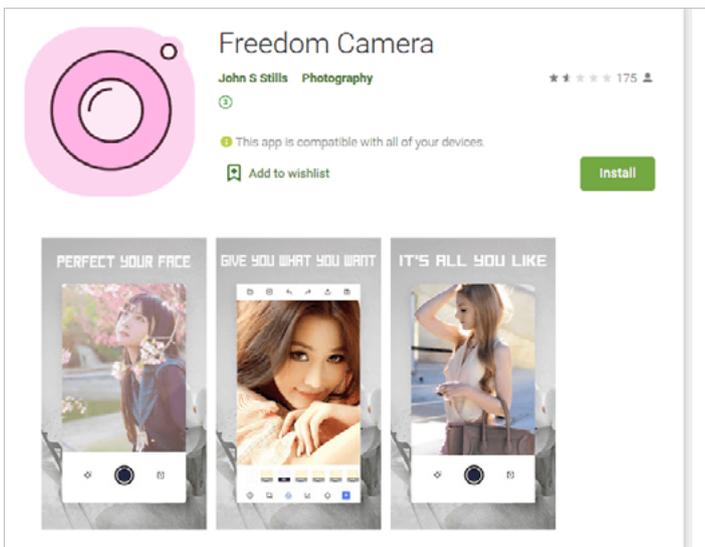
Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах:

- Adware.Dowgin.5.origin
- Adware.Toofan.1.origin
- Adware.BrowserAd.1
- Adware.Myteam.2.origin
- Adware.Altamob.1.origin

# Обзор вирусной активности для мобильных устройств в ноябре 2019 года

## Троянцы в Google Play

В течение месяца вирусные аналитики «Доктор Веб» обнаружили в Google Play несколько новых модификаций троянцев семейства [Android.Joker](#). Они скрывались в безобидных, на первый взгляд, программах — полезных утилитах для настройки мобильных устройств, играх, мессенджерах, сборниках изображений для рабочего стола и приложениях-фотокамерах. Эти вредоносные программы подписывают жертв на платные мобильные услуги, загружают и запускают вредоносные модули и могут выполнять произвольный код.

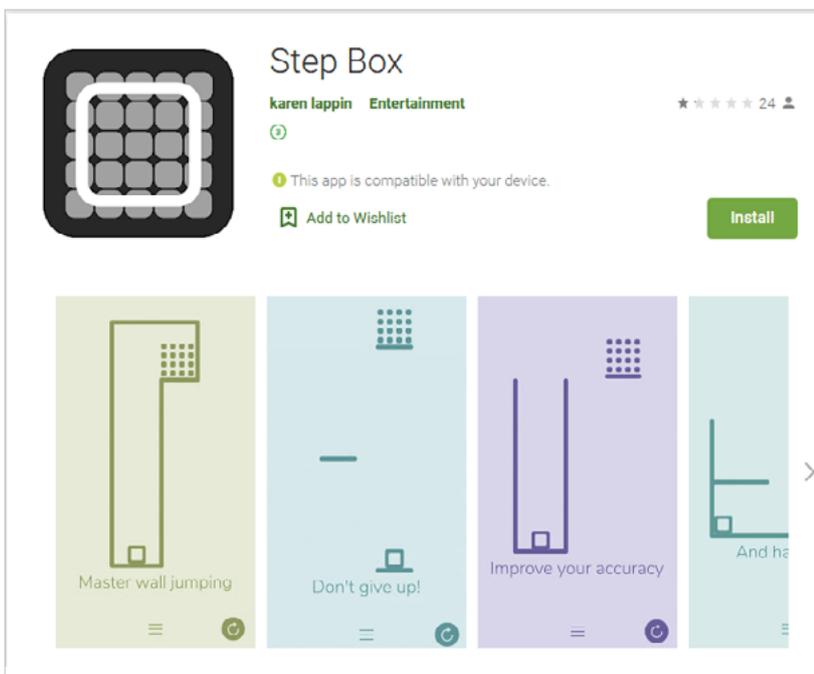
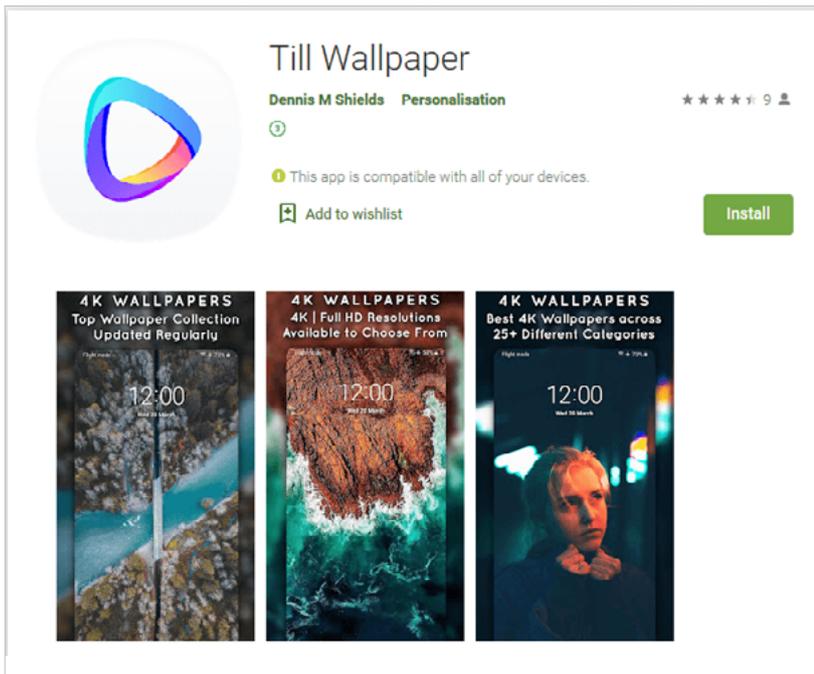


Узнайте больше

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

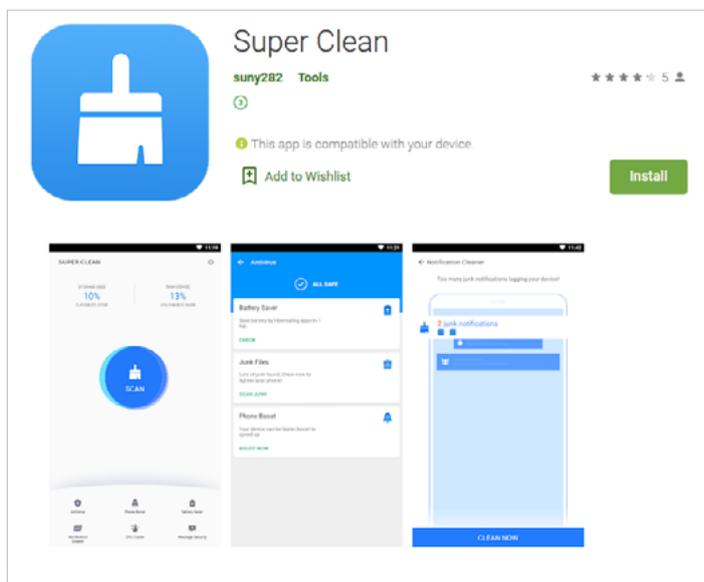
# Обзор вирусной активности для мобильных устройств в ноябре 2019 года

## Троянцы в Google Play



# Обзор вирусной активности для мобильных устройств в ноябре 2019 года

## Троянцы в Google Play



Также были выявлены новые рекламные троянцы [Android.HiddenAds](#). Злоумышленники распространяли их под видом игр, приложений-фотокамер, ПО для редактирования фотографий и других программ.



# Обзор вирусной активности для мобильных устройств в ноябре 2019 года

## Троянцы в Google Play

**MR Dinosaur: Run and eat**  
LIXGame Casual ★★★★★ 266

Contains Ads  
This app is compatible with your device.

Add to Wishlist **Install**

The screenshot shows a game interface with a dinosaur character running on a road, avoiding obstacles. It includes a 'PLAY' button and a stats panel with 'POWER', 'SPEED', and 'CASH' values.

**Sticker Maker**  
Popit Inc. Personalization ★★★★★ 47

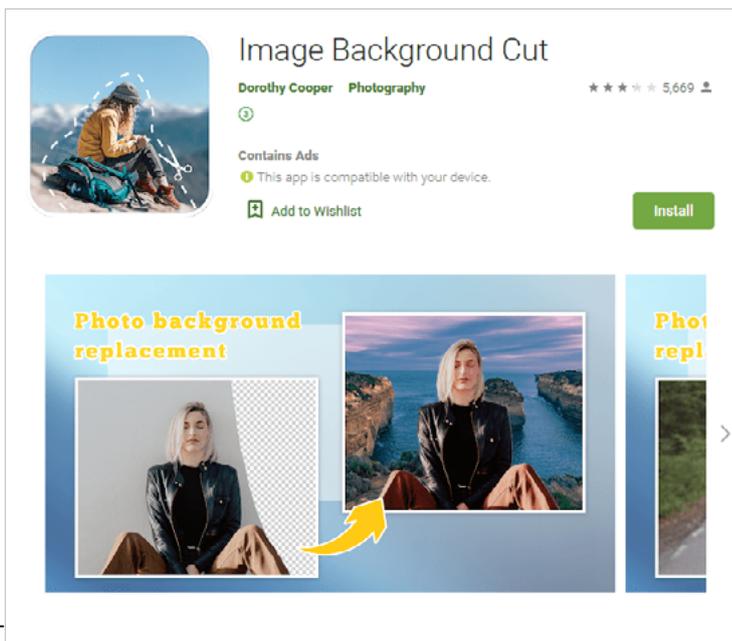
Contains Ads  
This app is compatible with your device.

Add to Wishlist **Install**

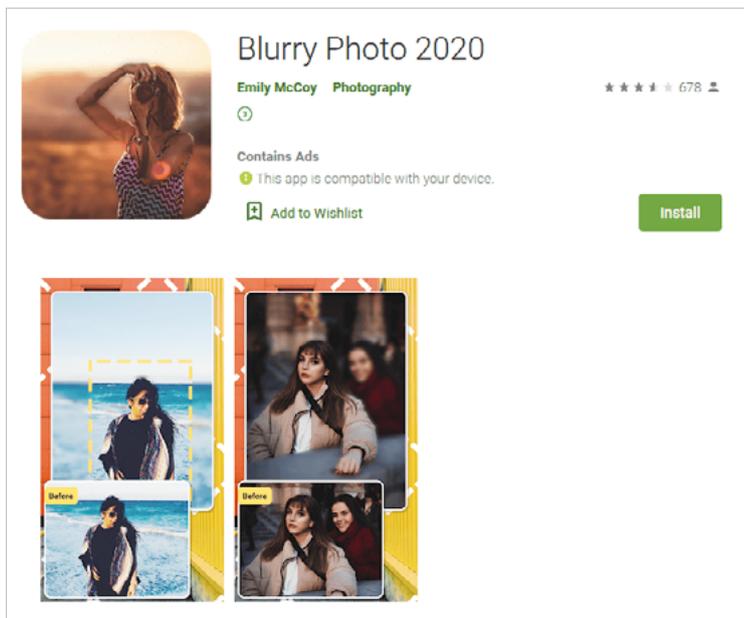
The screenshot shows two examples of stickers created in the app, featuring a person and a cat with speech bubbles.

# Обзор вирусной активности для мобильных устройств в ноябре 2019 года

## Троянцы в Google Play



T



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 ноябре 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

[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.drweb.ru](http://www.drweb.ru) | [www.антивирус.рф](http://www.антивирус.рф) | [free.drweb.ru](http://free.drweb.ru) | [www.av-desk.ru](http://www.av-desk.ru)

[«Доктор Веб» в других странах](#)



© ООО «Доктор Веб»,  
2003-2019

Узнайте больше

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