

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



## Обзор вирусной активности для мобильных устройств в мае 2018 года

31 мая 2018 года

В мае 2018 года вирусные аналитики компании «Доктор Веб» нашли в каталоге Google Play несколько приложений, в которые был встроен троянец [Android.Click.248.origin](#). Он загружал мошеннические веб-страницы, на которых пользователей подписывали на дорогостоящие мобильные услуги. Кроме того, в Google Play была обнаружена вредоносная программа [Android.FakeApp](#), распространявшаяся под видом известного ПО. Она переходила по заданным злоумышленниками ссылкам и накручивала счетчик посещений веб-сайтов. Среди других угроз, встретившихся в официальном каталоге приложений ОС Android, оказались троянцы семейства [Android.HiddenAds](#), предназначенные для показа рекламы. Также в уходящем месяце специалисты по информационной безопасности выявили троянцев [Android.Spy.456.origin](#) и [Android.Spy.457.origin](#), которых злоумышленники использовали для кибершпионажа. А в конце мая в вирусную базу Dr.Web была добавлена запись для детектирования новой версии коммерческой программы-шпиона [Program.Onespy](#).

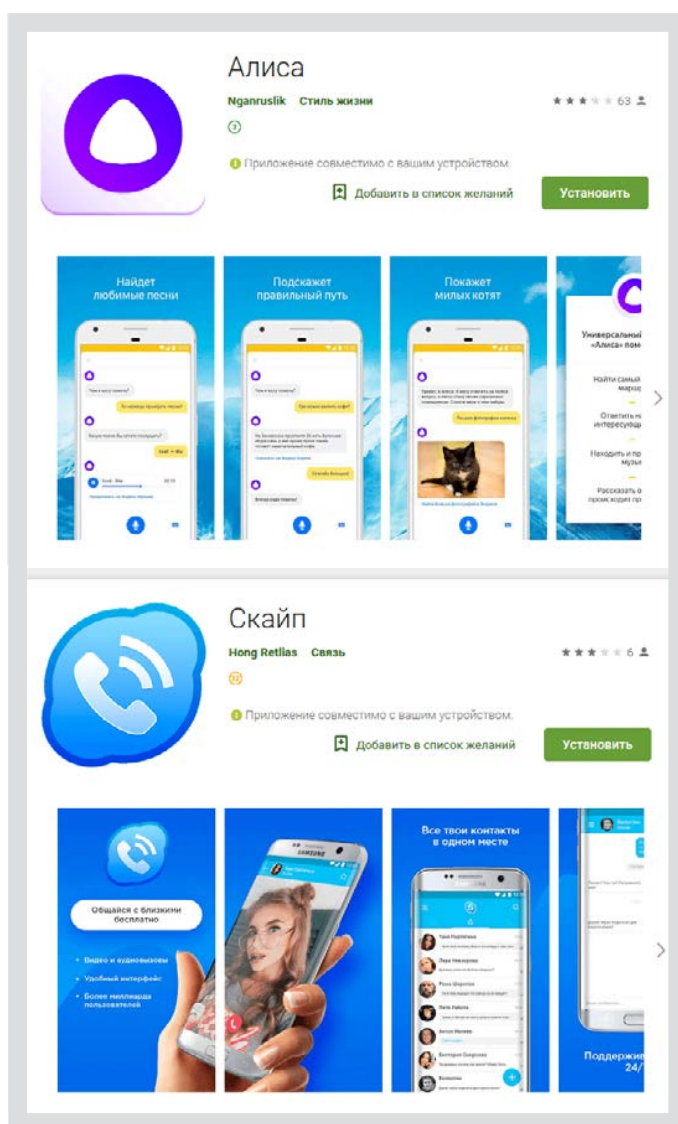
### Главные тенденции мая

- Обнаружение в каталоге Google Play очередных троянцев
- Выявление новой версии программы-шпиона для ОС Android

# Обзор вирусной активности для мобильных устройств в мае 2018 года

## Мобильная угроза месяца

В уходящем месяце специалисты «Доктор Веб» выявили в каталоге Google Play троянца [Android.Click.248.origin](#), которого злоумышленники распространяли под видом таких известных программ как Skype и Алиса (голосовой помощник от компании «Яндекс», в действительности недоступный в виде отдельного приложения).



Троянец загружал мошеннические веб-сайты, на которых пользователей подписывали на платные услуги. Об аналогичных вредоносных приложениях компания «Доктор Веб» [сообщила](#) в апреле.

## Обзор вирусной активности для мобильных устройств в мае 2018 года

### По данным антивирусных продуктов Dr.Web для Android

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



#### [Android.HiddenAds.210.origin](#)

#### [Android.HiddenAds.222.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.Mobifun.4](#)

Троянец, предназначенный для загрузки других Android-приложений.

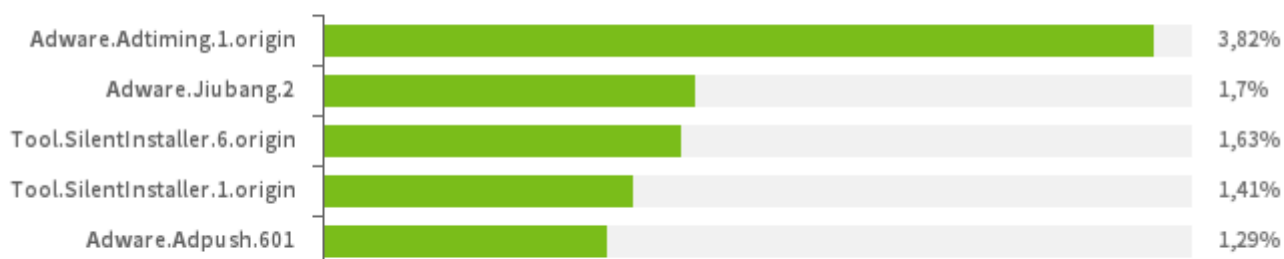
#### [Android.Xiny.1403](#)

Троянец, предназначенный для незаметной загрузки и установки других вредоносных приложений.

## Обзор вирусной активности для мобильных устройств в мае 2018 года

### По данным антивирусных продуктов Dr.Web для Android

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



**Adware.Adtiming.1.origin**

**Adware.Jiubang.2**

[Adware.Adpush.601](#)

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

[Tool.SilentInstaller.1.origin](#)

[Tool.SilentInstaller.6.origin](#)

Потенциально опасные программы, предназначенные для незаметного запуска приложений без вмешательства пользователя.

# Обзор вирусной активности для мобильных устройств в мае 2018 года

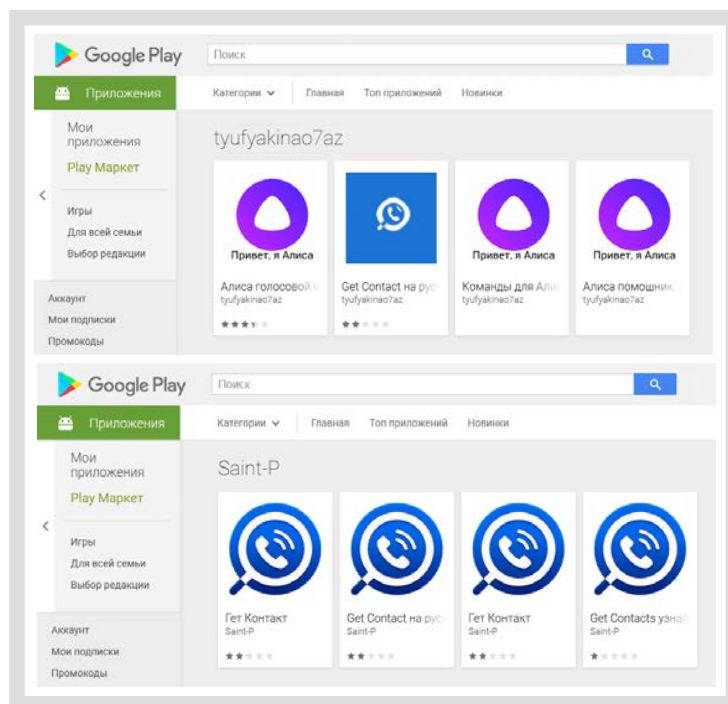
## Угрозы в Google Play

В мае в каталоге Google Play вирусные аналитики компании «Доктор Веб» обнаружили троянца [Android.FakeApp](#), распространявшегося под видом популярных приложений. По команде вирусописателей [Android.FakeApp](#) переходил по заданным ими ссылкам и загружал веб-сайты, накручивая счетчик их посещений.

### Особенности троянца:

- создан с использованием сервиса AppsGeyser, который за несколько элементарных шагов позволяет построить простые Android-программы;
- распространялся под видом известных приложений;
- не содержал никаких полезных функций;
- выявлено 7 разработчиков, от имени которых троянец распространялся в Google Play.

Пример приложений-подделок, найденных в Google Play:



Кроме того, в мае в официальном каталоге ПО для ОС Android были обнаружены очередные представители троянцев семейства [Android.HiddenAds](#), такие как [Android.HiddenAds.267.origin](#) и [Android.HiddenAds.277.origin](#). Эти вредоносные программы распространялись под видом безобидных и известных приложений. Главная функция троянцев – показ рекламы.

Узнайте больше

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

## Обзор вирусной активности для мобильных устройств в мае 2018 года

### Кибершпионаж

В уходящем месяце специалисты по информационной безопасности обнаружили несколько новых Android-троянцев, которых злоумышленники использовали для кибершпионажа. Один из них распространялся через Google Play и получил имя [Android.Spy.456.origin](#). Вредоносная программа похищала фотографии, СМС-сообщения, а также контакты из телефонной книги зараженных мобильных устройств и загружала их на удаленный сервер киберпреступников. Другой мобильный троянец-шпион, выявленный в мае, был добавлен в вирусную базу Dr.Web как [Android.Spy.457.origin](#). Он крад изображения и видеоролики, хранящиеся в памяти Android-смартфонов и планшетов, похищал СМС, отслеживал координаты мобильных устройств, а также мог прослушивать окружение и записывать телефонные разговоры.

В конце месяца специалисты компании «Доктор Веб» обнаружили новую версию коммерческой программы-шпиона Onespy, получившую имя [Program.Onespy.3.origin](#). Это приложение способно перехватывать СМС-сообщения и телефонные звонки, отслеживать местоположение зараженного устройства, прослушивать окружение, красть фотографии, видео, документы и другие файлы, следить за перепиской в популярных программах для общения, таких как Skype, Viber, WhatsApp, Line, Facebook и других, а также выполнять прочие опасные действия.

Несмотря на усилия корпорации Google, злоумышленникам по-прежнему удается распространять Android-троянцев через каталог Google Play. Кроме того, вредоносные и потенциально опасные программы для мобильных устройств подстерегают пользователей и вне официального каталога приложений. Для защиты смартфонов и планшетов их владельцам следует установить антивирусные продукты Dr.Web для Android.



# Обзор вирусной активности для мобильных устройств в мае 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](http://www.антивирус.рф) | [www.drweb.ru](http://www.drweb.ru) | [free.drweb.ru](http://free.drweb.ru) | [www.av-desk.ru](http://www.av-desk.ru)

[«Доктор Веб» в других странах](#)



© ООО «Доктор Веб»,  
2003-2018

Узнайте больше

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