



**«Доктор Веб»:  
обзор вирусной активности  
для мобильных устройств  
в апреле 2023 года**

## «Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2023 года

14 июня 2023 года

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в апреле 2023 года пользователи сталкивались с рекламными троянскими программами семейства [Android.HiddenAds](#) на 16,13% реже, а с представителями семейства [Android.MobiDash](#) — на 40,42% чаще, чем в марте. При этом данный тип вредоносных приложений остается одним из наиболее распространенных для платформы Android.

На 27,89% сократилась активность шпионских троянских программ. Чаще всего на защищаемых устройствах вновь обнаруживались различные варианты трояна-шпиона (в том числе [Android.Spy.5106](#) и [Android.Spy.4498](#)), скрытого в некоторых неофициальных модификациях мессенджера WhatsApp.

По сравнению с мартом количество атак банковских троянских программ возросло на 32,38%, а вредоносных приложений-вымогателей [Android.Locker](#) — на 14,83%.

В течение апреля вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play очередные вредоносные приложения-подделки из семейства [Android.FakeApp](#), которые злоумышленники использовали в различных мошеннических схемах. Кроме того, киберпреступники распространяли через Google Play троянскую программу из семейства [Android.Joker](#) — она подписывала жертв на платные услуги.

### ГЛАВНЫЕ ТЕНДЕНЦИИ АПРЕЛЯ

- Рост активности рекламных троянских программ [Android.MobiDash](#)
- Снижение активности рекламных троянских программ [Android.HiddenAds](#)
- Рост активности банковских троянских приложений и программ-вымогателей
- Появление очередных угроз в каталоге Google Play

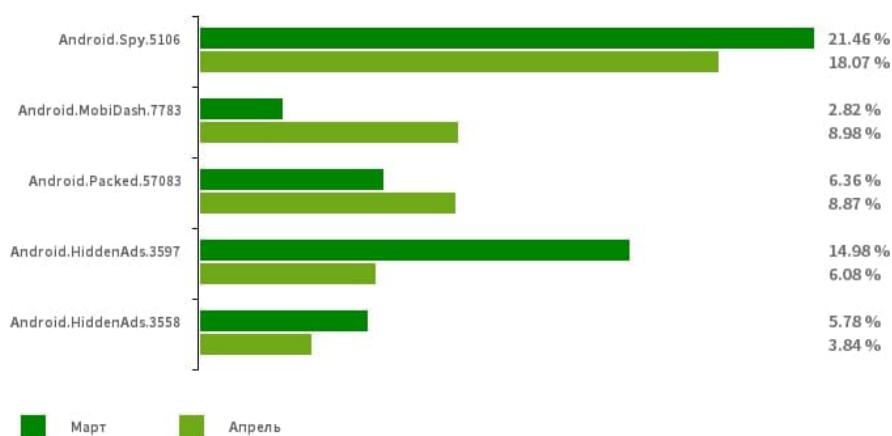
Узнайте больше

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

# «Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2023 года

## По данным антивирусных продуктов Dr.Web для Android

Наиболее распространенные вредоносные программы  
согласно статистике детектирований Dr.Web для мобильных устройств Android



### [Android.Spy.5106](#)

Троянская программа, представляющая собой видоизмененные версии неофициальных модификаций приложения WhatsApp. Она может похищать содержимое уведомлений, предлагать установку программ из неизвестных источников, а во время использования мессенджера — демонстрировать диалоговые окна с дистанционно настраиваемым содержимым.

### [Android.MobiDash.7783](#)

Троянская программа, показывающая надоедливую рекламу. Она представляет собой программный модуль, который разработчики ПО встраивают в приложения.

### [Android.Packed.57083](#)

Детектирование вредоносных приложений, защищенных программным упаковщиком ArkProtector. Среди них встречаются банковские трояны, шпионское и другое вредоносное ПО.

### [Android.HiddenAds.3597](#)

### [Android.HiddenAds.3558](#)

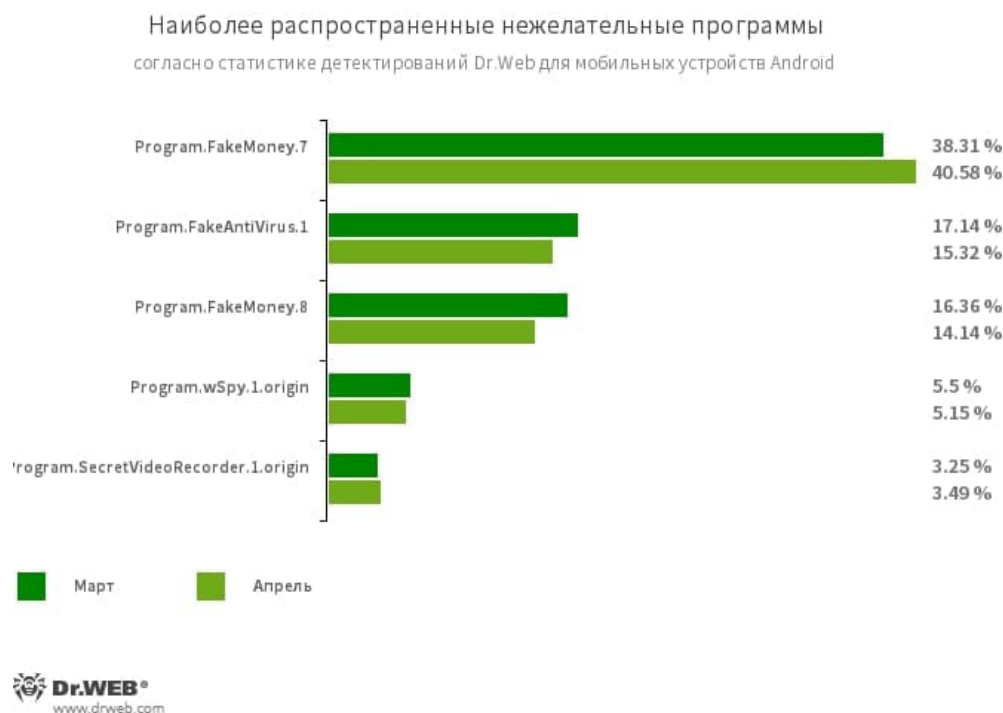
Троянские программы для показа навязчивой рекламы. Представители этого семейства часто распространяются под видом безобидных приложений и в некоторых случаях устанавливаются в системный каталог другим вредоносным ПО. Попадая на Android-устройства, такие рекламные трояны обычно скрывают от пользователя свое присутствие в системе — например, «прячут» значок приложения из меню главного экрана.

Узнайте больше

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

## «Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2023 года

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



#### Program.FakeMoney.7

#### Program.FakeMoney.8

Детектирование приложений, якобы позволяющих зарабатывать на выполнении тех или иных действий или заданий. Они имитируют начисление вознаграждений, причем для вывода «заработанных» денег требуется накопить определенную сумму. Даже когда пользователям это удается, получить выплаты они не могут.

#### Program.FakeAntiVirus.1

Детектирование рекламных программ, которые имитируют работу антивирусного ПО. Такие программы могут сообщать о несуществующих угрозах и вводить пользователей в заблуждение, требуя оплатить покупку полной версии.

#### Program.wSpy.1.origin

Коммерческая программа-шпион для скрытого наблюдения за владельцами Android-устройств. Она позволяет злоумышленникам читать переписку (сообщения в популярных мессенджерах и СМС), прослушивать окружение, отслеживать местоположение устройства, следить за историей веб-браузера, получать доступ к телефонной книге и контактам, фотографиям и видео, делать скриншоты экрана и фотографии через камеру устройства, а также имеет функцию кейлоггера.

Узнайте больше

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

## «Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2023 года

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

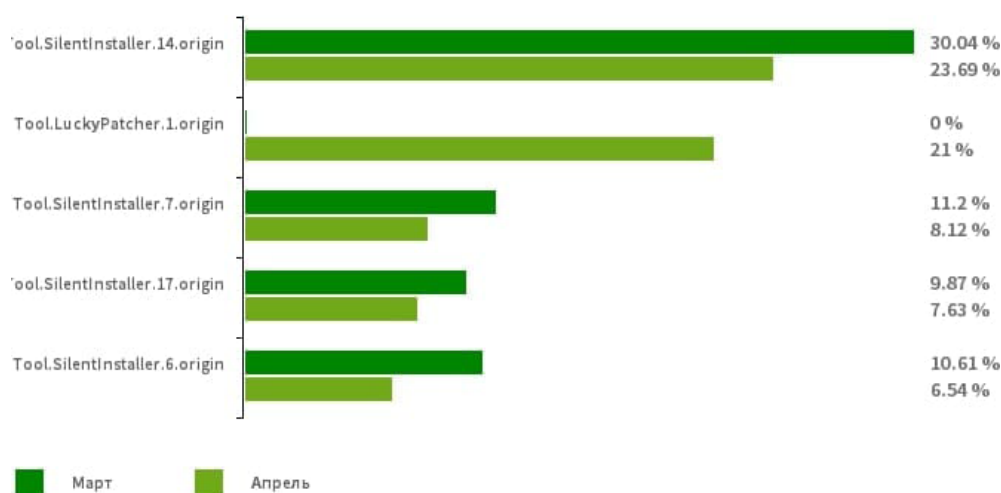
`Program.SecretVideoRecorder.1.origin`

Детектирование различных версий приложения для фоновой фото- и видеосъемки через встроенные камеры Android-устройств. Эта программа может работать незаметно, позволяя отключить уведомления о записи, а также изменять значок и описание приложения на фальшивые. Такая функциональность делает ее потенциально опасной.

## «Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2023 года

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

Наиболее распространенные потенциально опасные программы  
согласно статистике детектирований Dr.Web для мобильных устройств Android



[Tool.SilentInstaller.14.origin](#)

[Tool.SilentInstaller.7.origin](#)

[Tool.SilentInstaller.17.origin](#)

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

Потенциально опасные программные платформы, которые позволяют приложениям запускать APK-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

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

Утилита, позволяющая модифицировать установленные Android-приложения (создавать для них патчи) с целью изменения логики их работы или обхода тех или иных ограничений. Например, с ее помощью пользователи могут пытаться отключить проверку root-доступа в банковских программах или получить неограниченные ресурсы в играх. Для создания патчей утилита загружает из интернета специально подготовленные скрипты, которые могут создавать и добавлять в общую базу все желающие. Функциональность таких скриптов может оказаться в том числе и вредоносной, поэтому создаваемые патчи могут представлять потенциальную опасность.

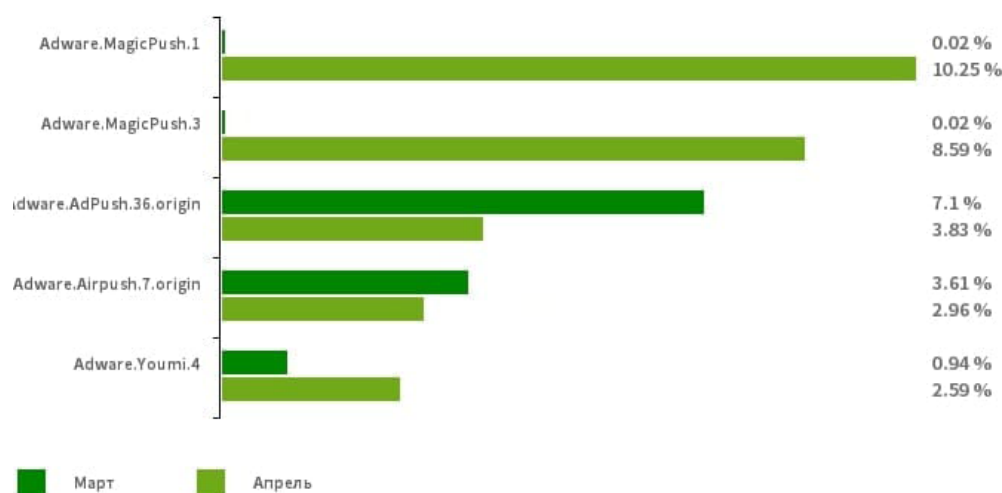
Узнайте больше

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

## «Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2023 года

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

Наиболее распространенные рекламные программы  
согласно статистике детектирования Dr.Web для мобильных устройств Android



#### [Adware.MagicPush.1](#)

#### [Adware.MagicPush.3](#)

Рекламные модули, встраиваемые в Android-приложения. Они демонстрируют всплывающие баннеры поверх интерфейса операционной системы, когда эти программы не используются. Такие баннеры содержат вводную в заблуждение информацию. Чаще всего в них сообщается о якобы обнаруженных подозрительных файлах, либо говорится о необходимости заблокировать спам или оптимизировать энергопотребление устройства. Для этого пользователю предлагается зайти в соответствующее приложение, в которое встроены один из этих модулей. При открытии программы пользователь видит рекламу.

#### [Adware.AdPush.36.origin](#)

Рекламный модуль, который может быть интегрирован в Android-программы. Он демонстрирует рекламные уведомления, вводящие пользователей в заблуждение. Например, такие уведомления могут быть похожи на сообщения от операционной системы. Кроме того, этот модуль собирает ряд конфиденциальных данных, а также способен загружать другие приложения и инициировать их установку.

Узнайте больше

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

## «Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2023 года

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

#### [Adware.Airpush.7.origin](#)

Представитель семейства рекламных модулей, встраиваемых в Android-приложения и демонстрирующих разнообразную рекламу. В зависимости от версии и модификации это могут быть рекламные уведомления, всплывающие окна или баннеры. С помощью данных модулей злоумышленники часто распространяют вредоносные программы, предлагая установить то или иное ПО. Кроме того, такие модули передают на удаленный сервер различную конфиденциальную информацию.

#### [Adware.Youmi.4](#)

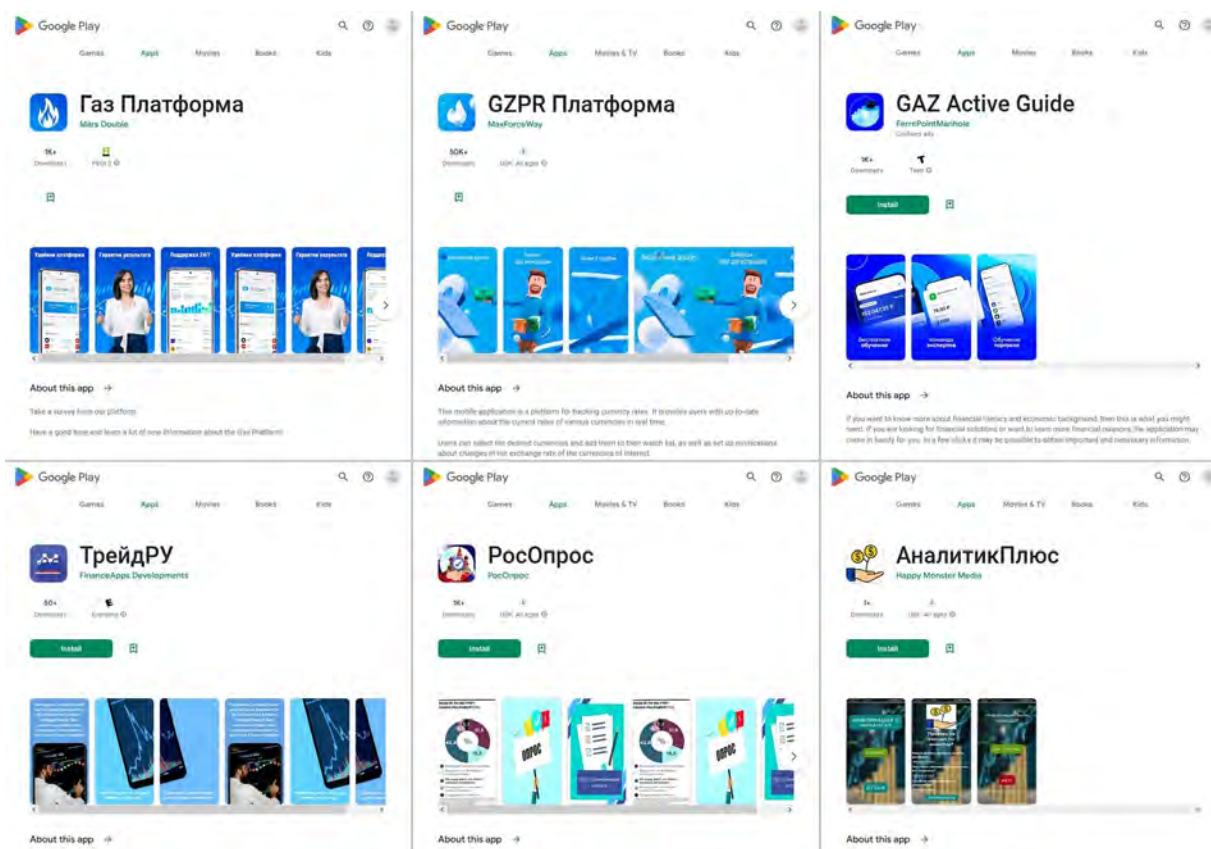
Детектирование нежелательного рекламного модуля, который размещает рекламные ярлыки на главном экране Android-устройств.



# «Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2023 года

## Угрозы в Google Play

В апреле 2023 года вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play более 30 вредоносных программ семейства [Android.FakeApp](#). Часть из них ([Android.FakeApp.1320](#), [Android.FakeApp.1329](#), [Android.FakeApp.1331](#), [Android.FakeApp.1336](#), [Android.FakeApp.1340](#), [Android.FakeApp.1347](#) и прочие) распространялась под видом приложений финансовой тематики. Например, различных справочников и пособий по инвестированию, инструментов для торговли, программ для участия в опросах и т. д. Однако их настоящей функцией была загрузка мошеннических сайтов, через которые злоумышленники пытались получить от потенциальных жертв персональные данные и похитить их деньги.



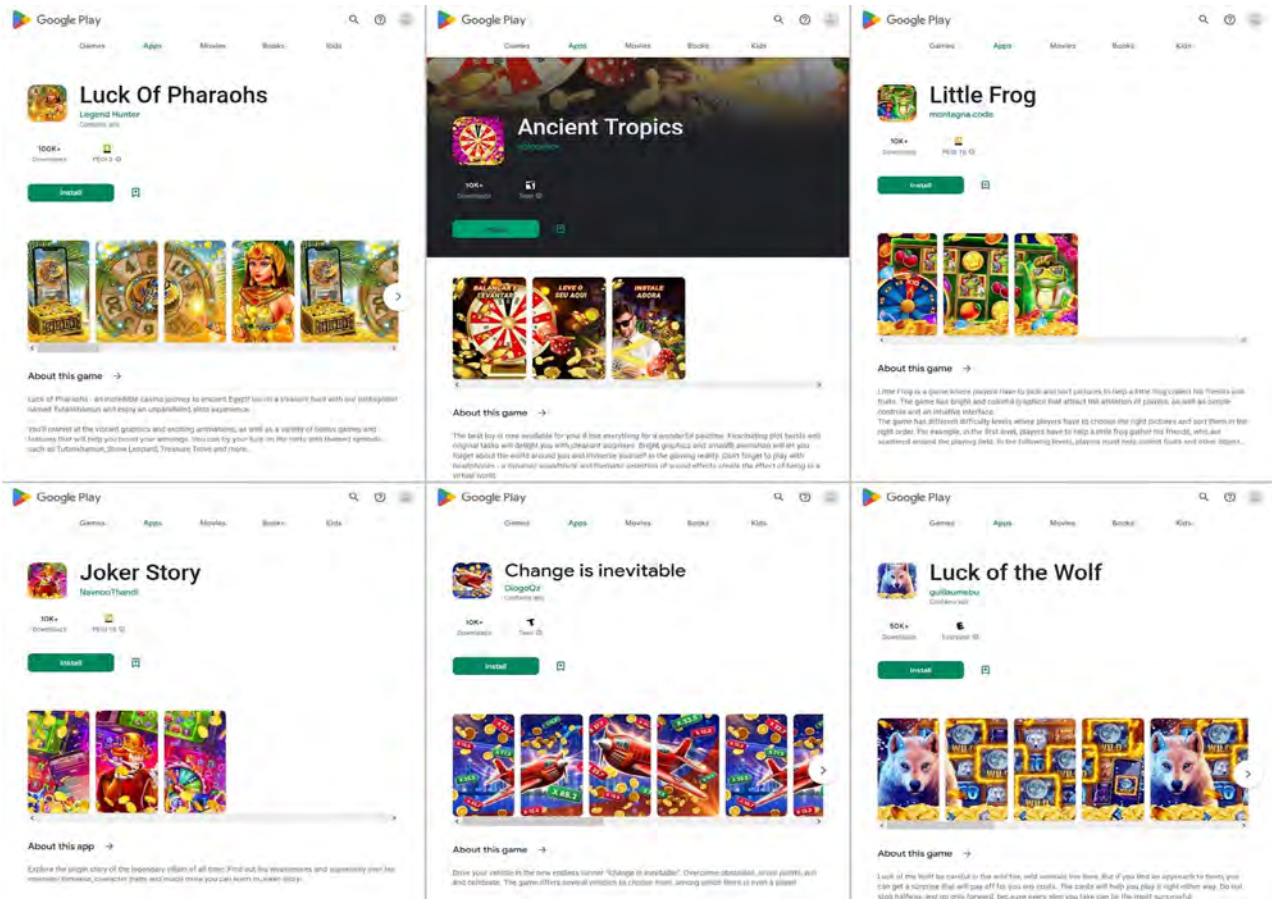
Другие программы этого типа распространялись под видом игр, например — [Android.FakeApp.1322](#), [Android.FakeApp.1326](#), [Android.FakeApp.1330](#), [Android.FakeApp.1334](#), [Android.FakeApp.1337](#) и [Android.FakeApp.26.origin](#). Вместо ожидаемой функциональности они могли загружать сайты онлайн-казино.

Узнайте больше

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

# «Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2023 года

## Угрозы в Google Play



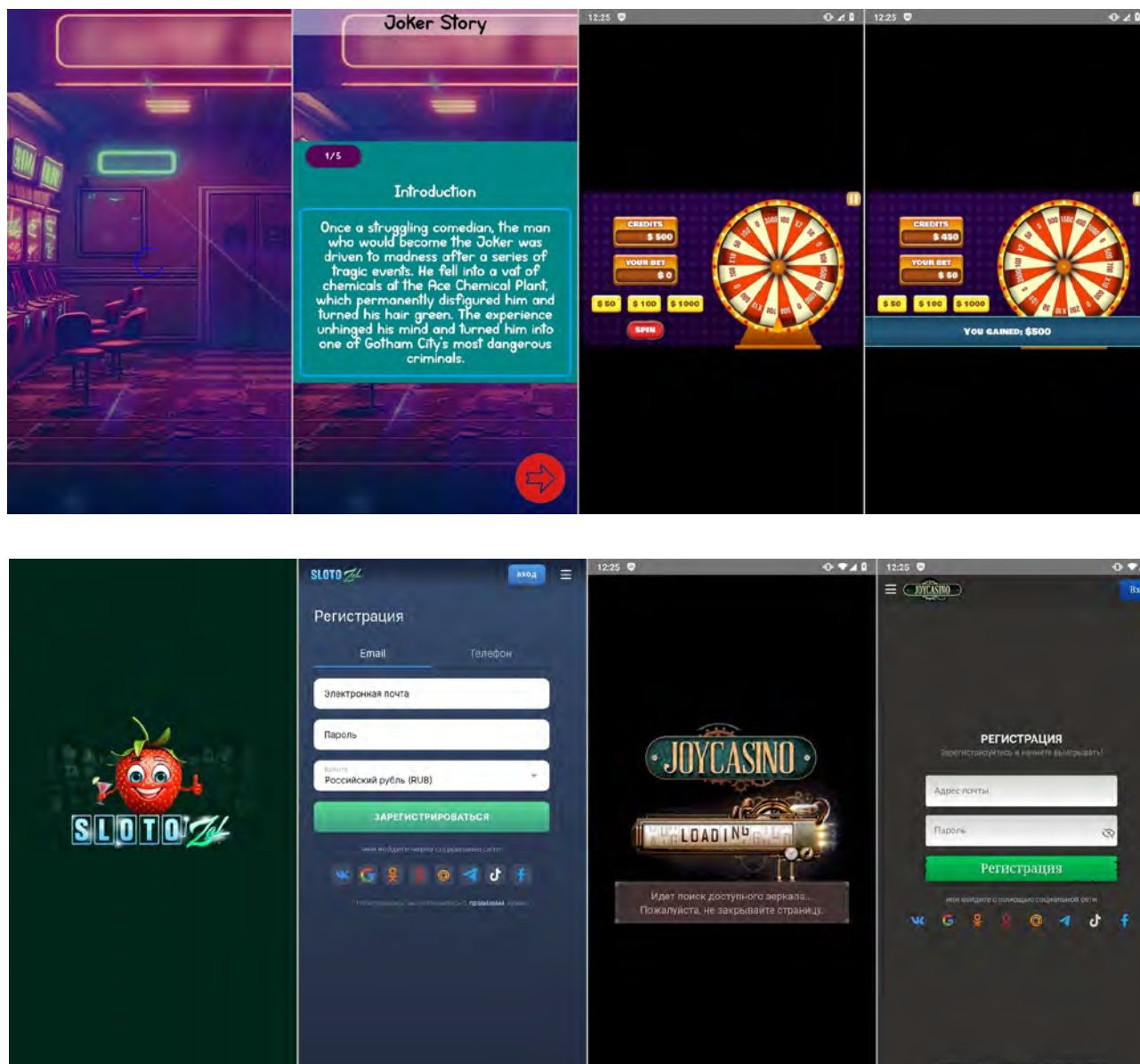
Примеры их двойственного поведения представлены ниже. В первом случае в них доступна игровая функциональность, во втором — происходит загрузка целевых сайтов.

Узнайте больше

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

# «Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2023 года

## Угрозы в Google Play



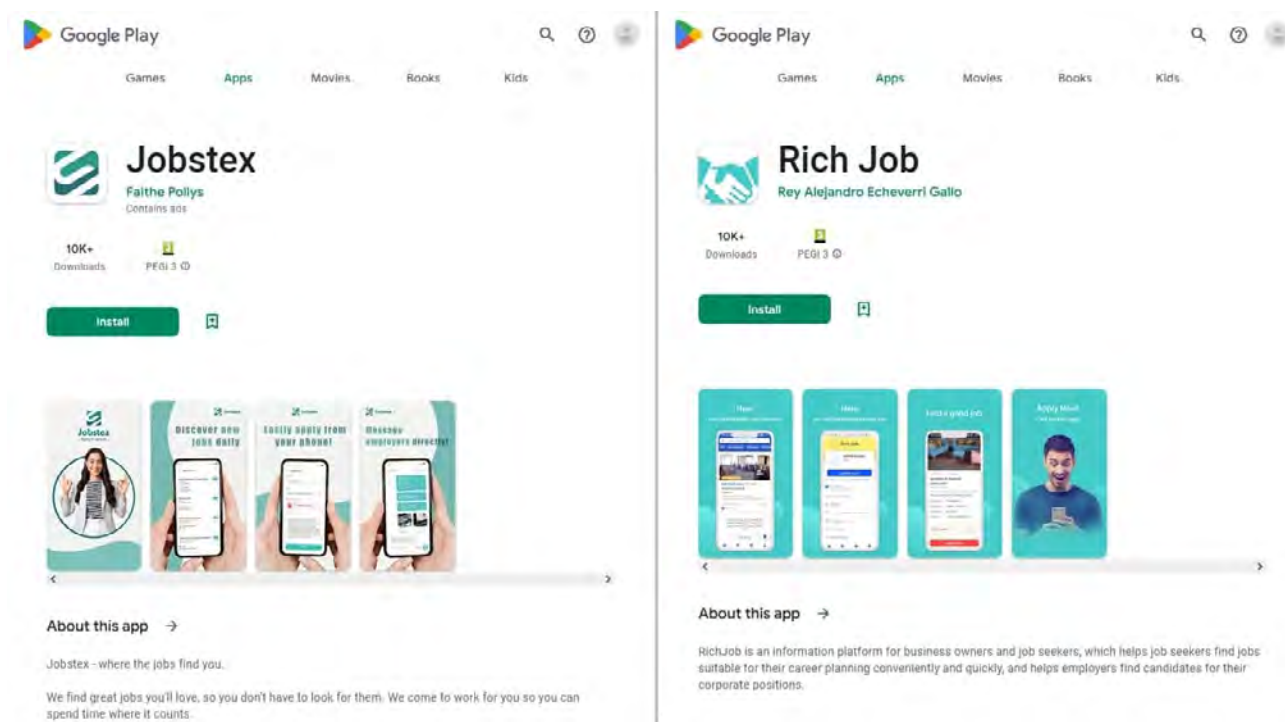
Кроме того, наши специалисты выявили очередные мошеннические программы, которые злоумышленники выдавали за инструменты для поиска вакансий. Эти представители семейства [Android.FakeApp](#), добавленные в вирусную базу Dr.Web как [Android.FakeApp.1324](#) и [Android.FakeApp.1307](#), предлагали пользователям указать персональные данные в специальной форме или связаться с «работодателями» через мессенджеры.

Узнайте больше

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

# «Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2023 года

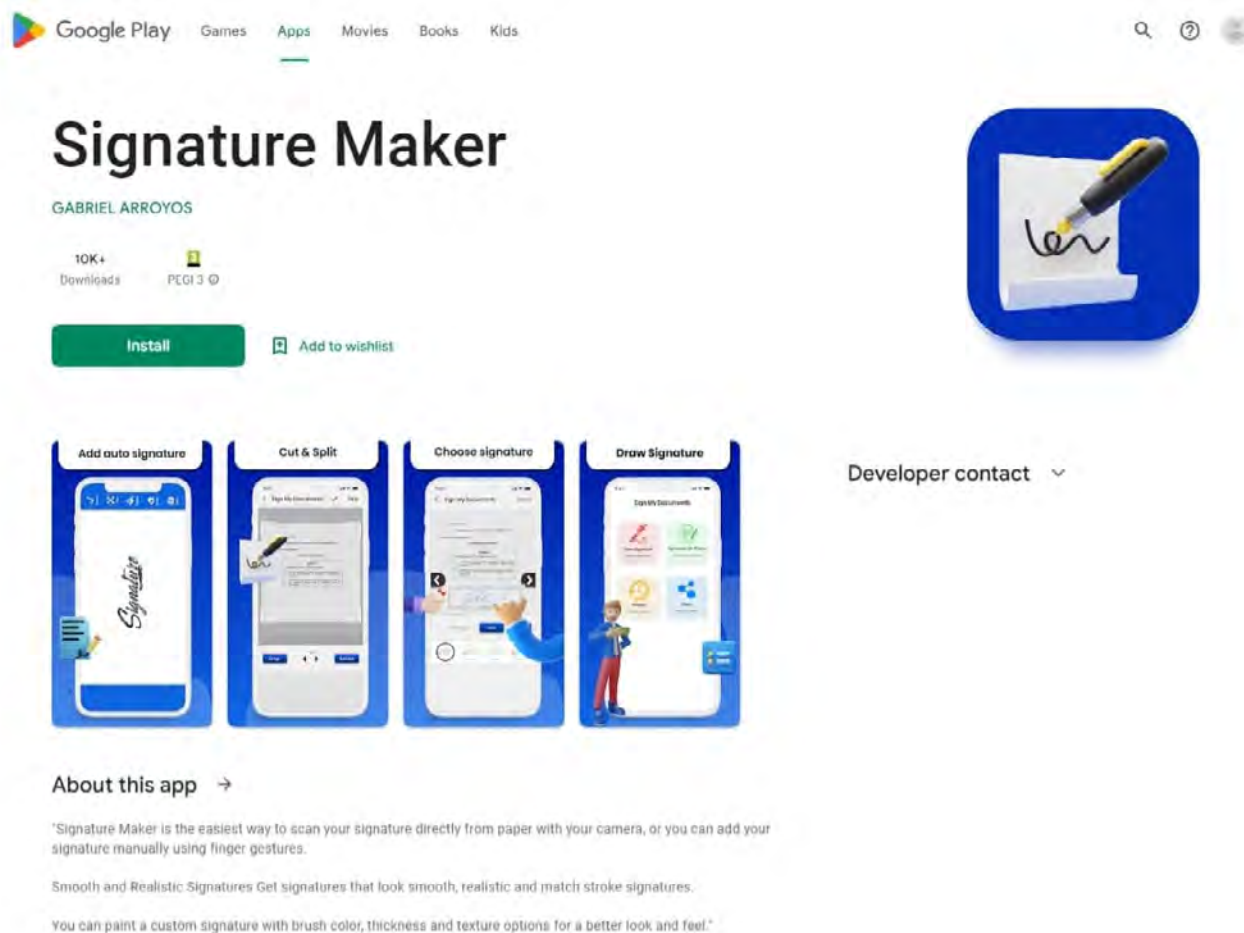
## Угрозы в Google Play



Вместе с тем злоумышленники распространяли через Google Play троянскую программу [Android.Joker.2106](#), которая подписывала жертв на платные услуги. Она скрывалась в приложении для создания подписей и работы с ними.

# «Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2023 года

## Угрозы в Google Play



Google Play Games Apps Movies Books Kids

# Signature Maker

GABRIEL ARROYOS

10K+ Downloads PEGI 3

Install Add to wishlist

Add auto signature Cut & Split Choose signature Draw Signature

Developer contact

**About this app** →

\*Signature Maker is the easiest way to scan your signature directly from paper with your camera, or you can add your signature manually using finger gestures.

Smooth and Realistic Signatures Get signatures that look smooth, realistic and match stroke signatures.

You can paint a custom signature with brush color, thickness and texture options for a better look and feel.\*

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

## «Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 2023 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

[Центр противодействия кибер-мошенничеству](#)

### Пресс-центр

[Официальная информация](#) | [Контакты для прессы](#) | [Брошюры](#) | [Галерея](#)

### Контакты

Центральный офис

125124, Россия, Москва, 3-я улица Ямского Поля, д.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»,  
2003-2023

Узнайте больше

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