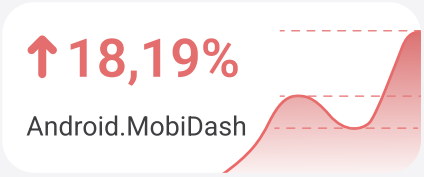
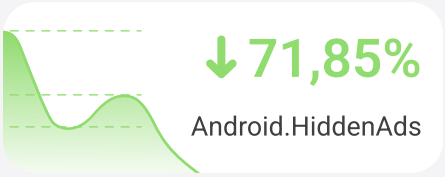
Dr.WEB

«Доктор Веб»: обзор вирусной активности для мобильных устройств в III квартале 2025 года

Главное

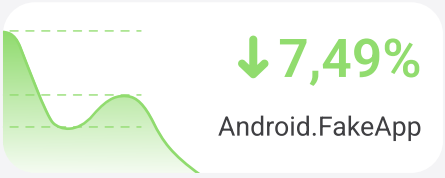
Согласно данным статистики детектирований Dr.Web Security Space для мобильных устройств, в III квартале 2025 года наибольшее распространение получили трояны **Android.MobiDash**, которые показывают навязчивую рекламу. По сравнению с прошлым периодом наблюдения они обнаруживались на защищаемых устройствах на **18,19%** чаще.

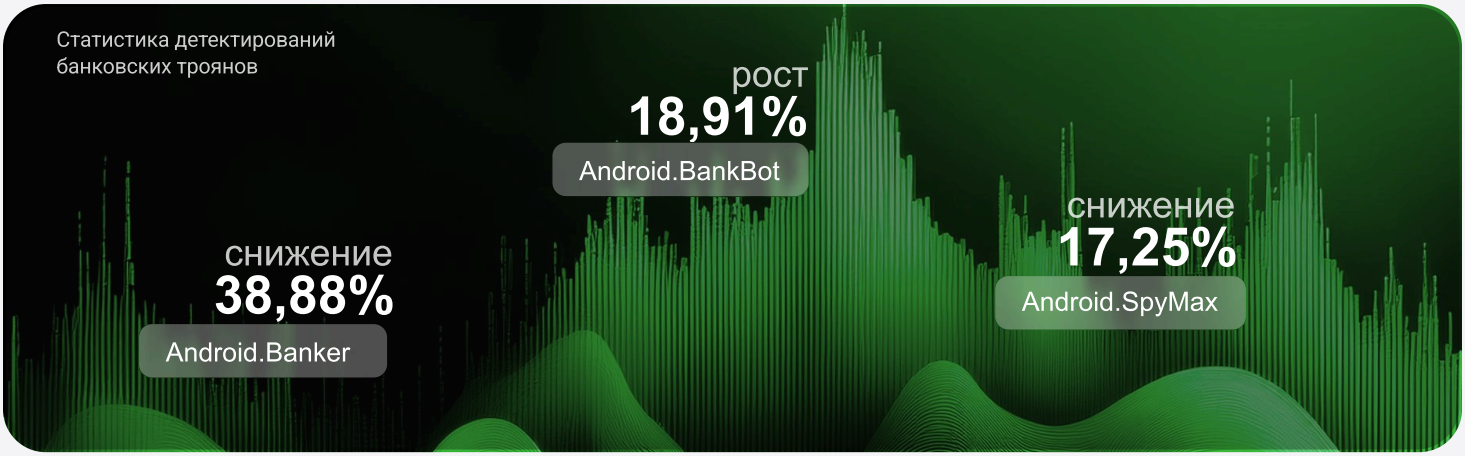




На второе место опустились рекламные трояны **Android.HiddenAds**, активность которых снижается второй квартал подряд. В течение последних трех месяцев пользователи сталкивались с ними на 71,85% реже. Эти вредоносные приложения скрывают свои значки, чтобы их было сложнее обнаружить и удалить, и демонстрируют рекламу, в том числе полноэкранные видеоролики.

На третьем месте вновь расположились вредоносные программы-подделки **Android.FakeApp**, которые злоумышленники используют в различных мошеннических схемах. Число их детектирований снизилось на 7,49%. Такие трояны вместо заявленной функциональности часто загружают различные сайты — например, мошеннические и вредоносные, а также сайты онлайн-казино и букмекерских контор.





Самыми распространенными банковскими троянами остались представители семейства **Android.Banker**, несмотря на снижение активности на 38,88%. Злоумышленники используют их для получения нелегального доступа к банковским счетам и похищения денег. Эти трояны могут демонстрировать фишинговые окна для кражи логинов и паролей, имитировать внешний вид настоящих программ «банк-клиент», перехватывать СМС для получения одноразовых кодов и т. д.

За ними расположились трояны **Android.BankBot**, которые детектировались на 18,91% чаще. Они также пытаются получить доступ к учетным записям онлайн-банка пользователей, перехватывая коды подтверждения. При этом данные банковские трояны могут выполнять различные команды киберпреступников, а некоторые из них позволяют дистанционно управлять зараженными устройствами.

Замыкают тройку лидеров представители семейства **Android.SpyMax**, основанные на исходном коде трояна-шпиона SpyNote. Они детектировались на 17,25% реже, чем во II квартале. Эти вредоносные программы обладают широким набором вредоносных функций, в том числе позволяют дистанционно управлять устройствами.

В августе мы сообщили о кампании по распространению многофункционального бэкдора **Android.Backdoor.916.origin**, которого киберпреступники используют для кражи конфиденциальных данных и слежки за пользователями Android-устройств. Злоумышленники отправляли потенциальным жертвам сообщения в различных мессенджерах, предлагая установить «антивирус» из прикрепленного APK-файла. Антивирусная лаборатория «Доктор Веб» обнаружила первые версии этой вредоносной программы еще в январе 2025 года и с тех пор продолжает отслеживать ее развитие. По оценкам наших экспертов, бэкдор применяется в таргетированных атаках и не предназначен для массового распространения. Основной целью киберпреступников являются представители российского бизнеса.

В течение III квартала в каталоге Google Play распространялось множество вредоносных и нежелательных приложений, которые суммарно были установлены свыше 1 459 000 раз. Среди них — десятки троянов **Android.Joker**, подписывающих жертв на платные услуги, а также программы-подделки **Android.FakeApp**. Кроме того, наши вирусные аналитики выявили очередную программу, которая якобы позволяла конвертировать виртуальные награды в настоящие деньги.

Главные тенденции II квартала

Рекламные трояны Android.MobiDash стали самыми распространенными угрозами

Продолжилось снижение активности рекламных троянов Android.HiddenAds

Возросло число атак банковских троянов семейства Android.BankBot

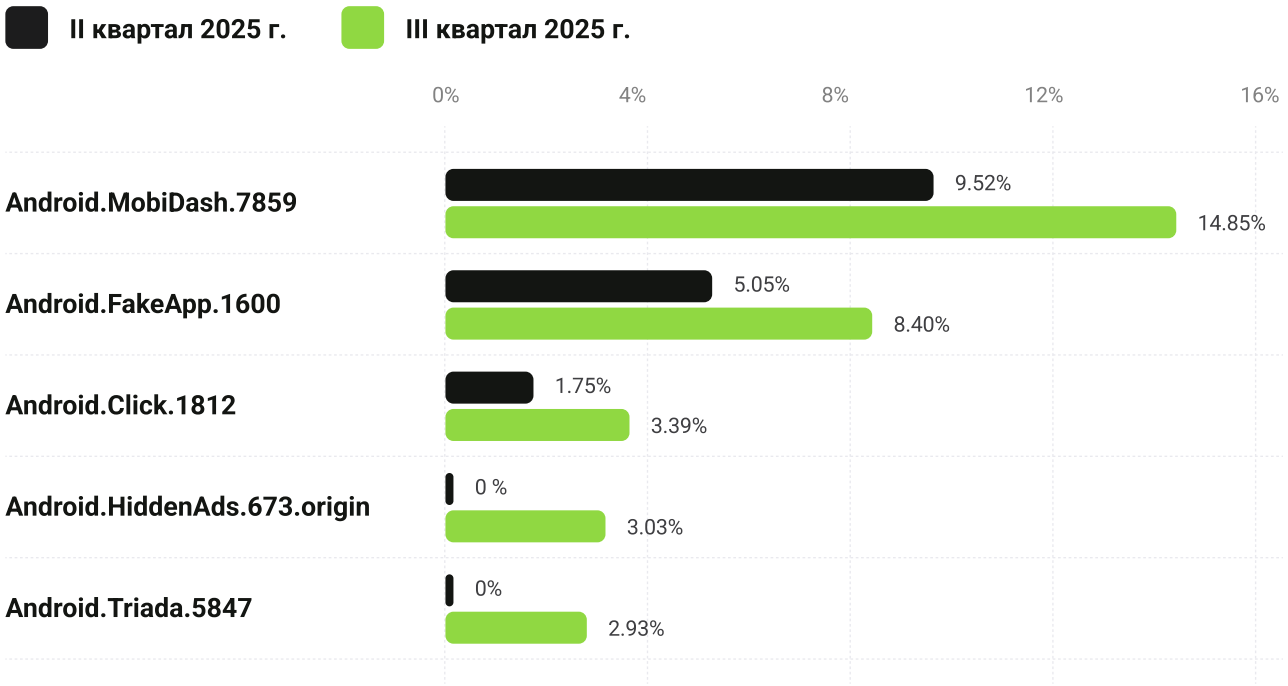
В каталоге Google Play распространялось множество вредоносных программ

Снизилась активность банковских троянов Android.Banker и Android.SpyMax

Киберпреступники использовали многофункционального бэкдора Android.Backdoor.916.origin для атак на представителей российского бизнеса

По данным Dr.Web Security Space для мобильных устройств

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



Android.MobiDash.7859

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

Android.FakeApp.1600

Троянская программа, которая загружает указанный в ее настройках веб-сайт. Известные модификации этого вредоносного приложения загружают сайт онлайн-казино.

Android.HiddenAds.673.origin

Троянская программа для показа навязчивой рекламы. Представители семейства Android.HiddenAds 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.

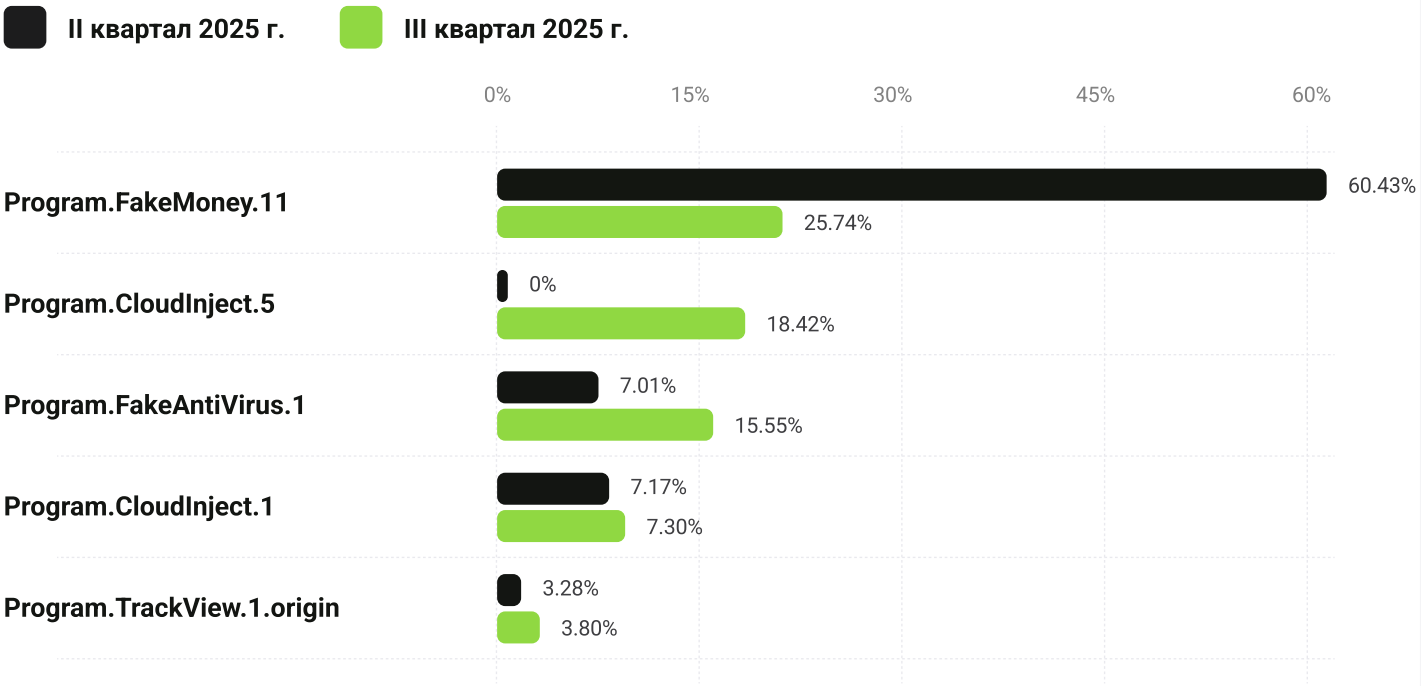
Android.Click.1812

Детектирование вредоносных модов мессенджера WhatsApp, которые незаметно для пользователя могут загружать различные сайты в фоновом режиме.

Android.Triada.5847

Детектирование упаковщика для троянов семейства Android.Triada, предназначенного для их защиты от анализа и обнаружения. Чаще всего злоумышленники используют его совместно с вредоносными модами мессенджера Telegram, в которые непосредственно встроены эти трояны.

Наиболее распространенные нежелательные программы
согласно статистике детектирований Dr.Web Security Space для мобильных устройств



Program.FakeMoney.11

Детектирование приложений, якобы позволяющих зарабатывать на выполнении тех или иных действий или заданий. Эти программы имитируют начисление вознаграждений, причем для вывода «заработанных» денег требуется накопить определенную сумму. Обычно в них имеется список популярных платежных систем и банков, через которые якобы возможно перевести награды. Но даже когда пользователям удается накопить достаточную для вывода сумму, обещанные выплаты не поступают. Этой записью также детектируется другое нежелательное ПО, основанное на коде таких программ.

Program.CloudInject.5 **Program.CloudInject.1**

Детектирование Android-приложений, модифицированных при помощи облачного сервиса CloudInject и одноименной Android-утилиты (добавлена в вирусную базу Dr.Web как Tool.CloudInject). Такие программы модифицируются на удаленном сервере, при этом заинтересованный в их изменении пользователь (моддер) не контролирует, что именно будет в них встроено. Кроме того, приложения получают набор опасных разрешений. После модификации программ у моддера появляется возможность дистанционно управлять ими — блокировать, показывать настраиваемые диалоги, отслеживать факт установки и удаления другого ПО и т. д.

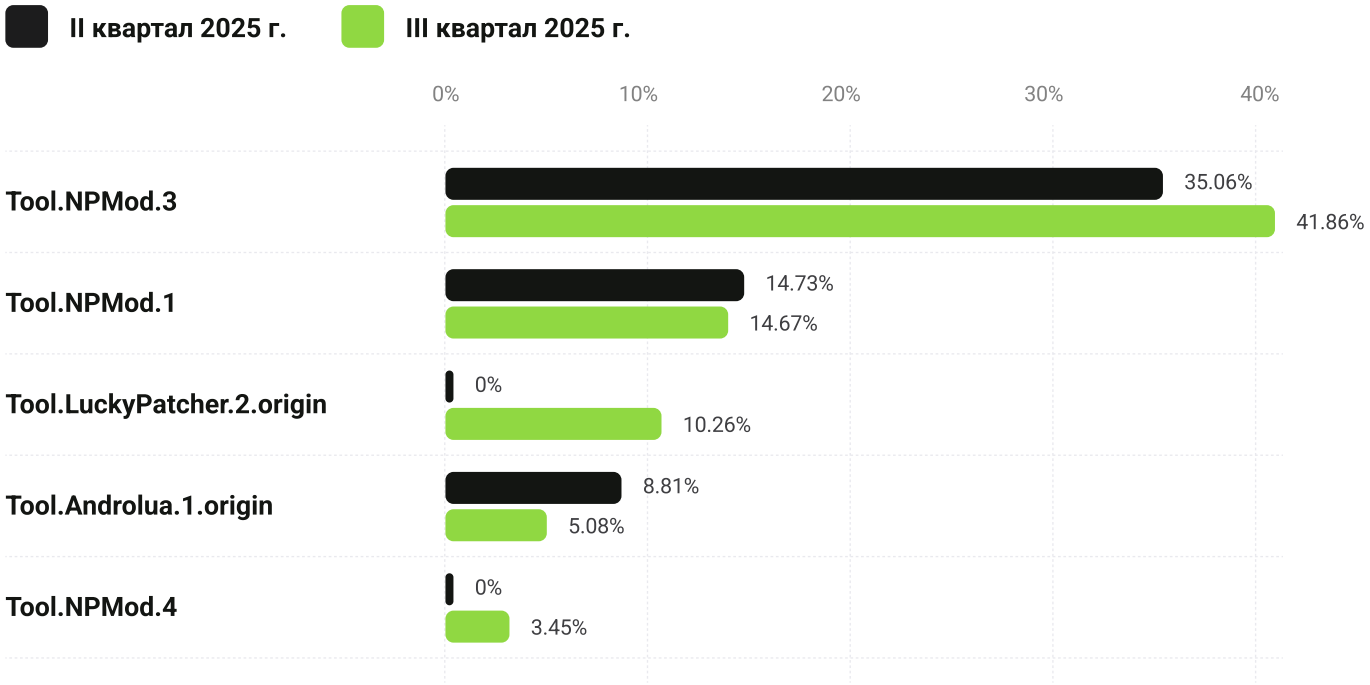
Program.FakeAntiVirus.1

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.TrackView.1.origin

Приложение, позволяющее вести наблюдение за пользователями через Android-устройства. С помощью этой программы злоумышленники могут определять местоположение целевых устройств, использовать камеру для записи видео и создания фотографий, выполнять прослушивание через микрофон, создавать аудиозаписи и т. д.

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



Tool.NPMod.3 **Tool.NPMod.1** **Tool.NPMod.4**

Детектирование Android-приложений, модифицированных при помощи утилиты NP Manager. В такие программы внедрен специальный модуль, который позволяет обойти проверку цифровой подписи после их модификации.

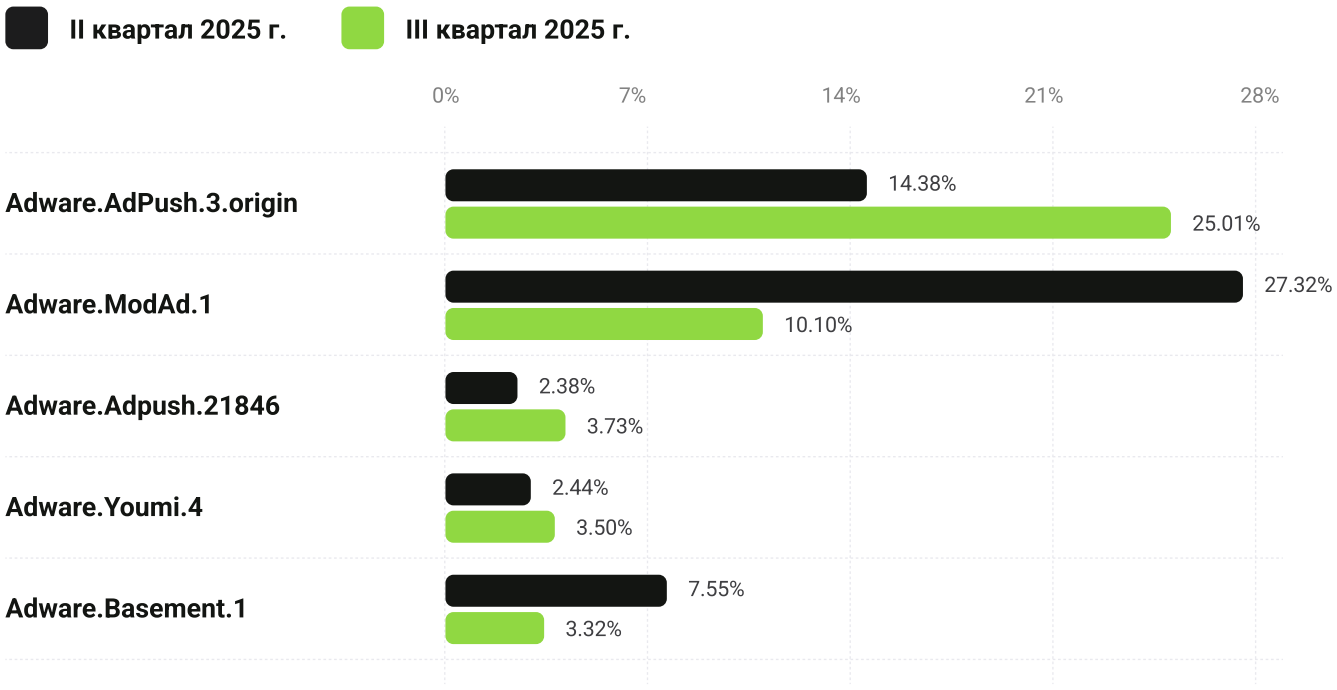
Tool.LuckyPatcher.2.origin

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 попытаться 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.

Tool.Androlua.1.origin

Детектирование ряда потенциально опасных версий специализированного фреймворка для разработки Android-программ на скриптовом языке программирования Lua. Основная логика Lua-приложений расположена в соответствующих скриптах, которые зашифрованы и расшифровываются интерпретатором перед выполнением. Часто данный фреймворк по умолчанию запрашивает доступ ко множеству системных разрешений для работы. В результате исполняемые через него Lua-скрипты способны выполнять различные вредоносные действия в соответствии с полученными разрешениями.

Наиболее распространенные рекламные программы
согласно статистике детектирований Dr.Web Security Space для мобильных устройств



Adware.AdPush.3.origin **Adware.Adpush.21846**

Рекламные модули, которые могут быть интегрированы в Android-программы. Они демонстрируют рекламные уведомления, вводящие пользователей в заблуждение. Например, такие уведомления могут напоминать сообщения от операционной системы. Кроме того, эти модули собирают ряд конфиденциальных данных, а также способны загружать другие приложения и инициировать их установку.

Adware.ModAd.1

Детектирование некоторых модифицированных версий (модов) мессенджера WhatsApp, в функции которых внедрен код для загрузки заданных ссылок через веб-отображение во время работы с мессенджером. С этих интернет-адресов выполняется перенаправление на рекламируемые сайты — например, онлайн-казино и букмекеров, сайты для взрослых.

Adware.Youmi.4

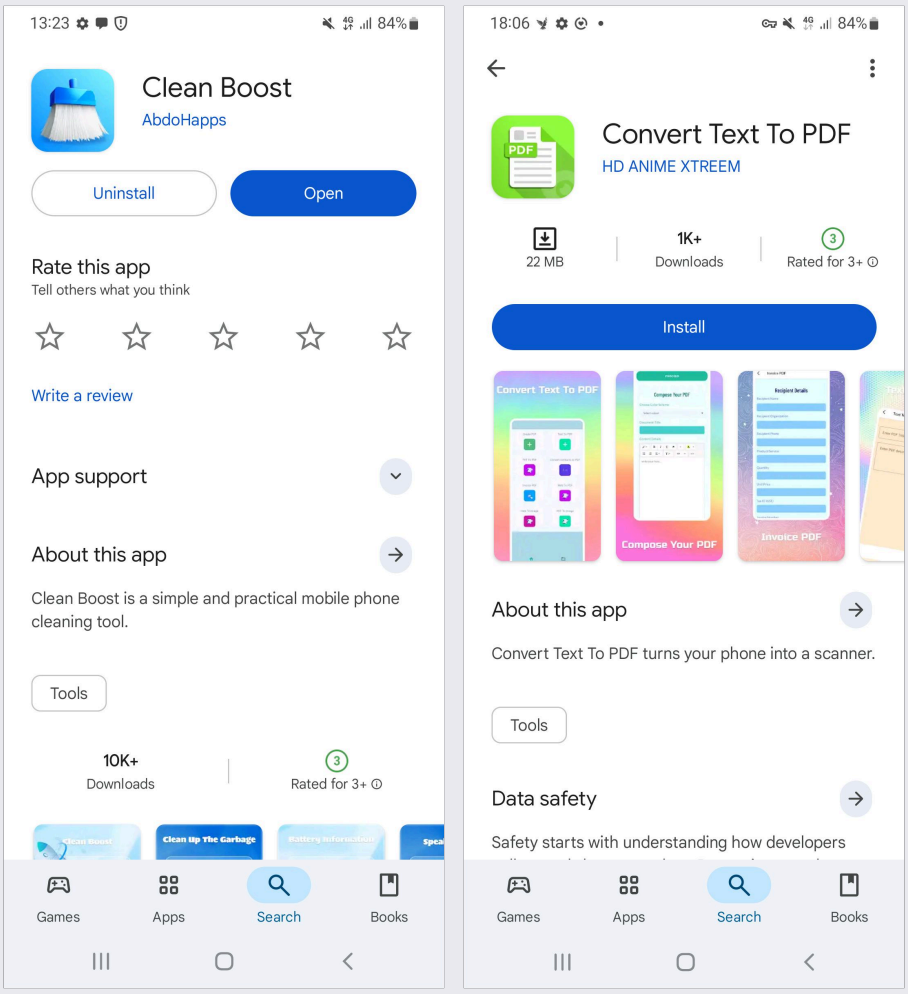
Детектирование нежелательного рекламного модуля, который размещает рекламные ярлыки на главном экране Android-устройств.

Adware.Basement.1

Приложения, демонстрирующие нежелательную рекламу, которая часто ведет на вредоносные и мошеннические сайты. Они имеют общую кодовую базу с нежелательными программами Program.FakeMoney.11.

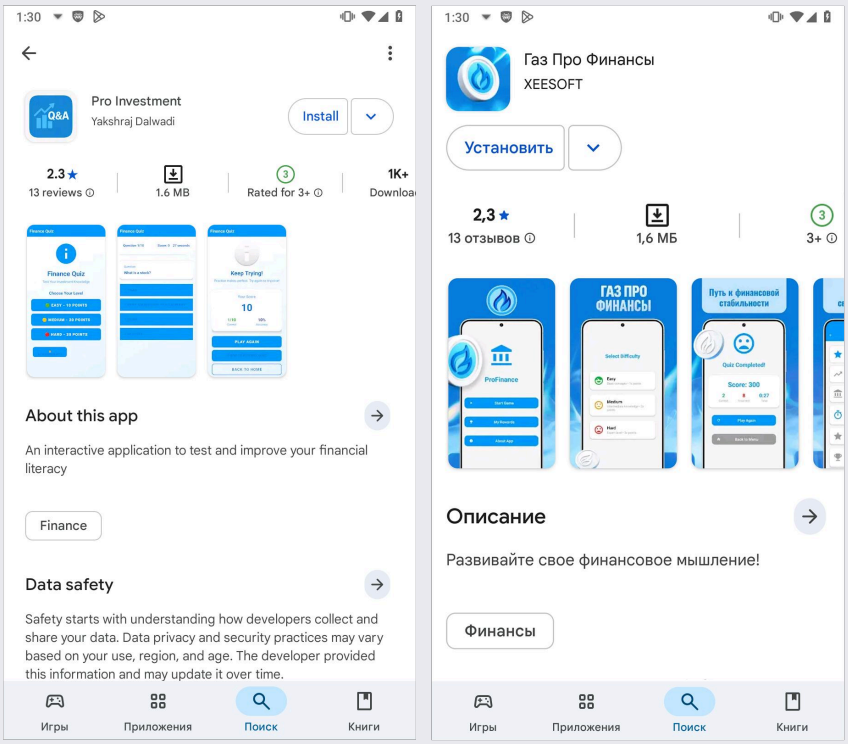
Угрозы в Google Play

В III квартале 2025 года антивирусная лаборатория «Доктор Веб» зафиксировала в каталоге Google Play свыше 50 троянов семейства Android.Joker, которые подписывают пользователей на платные услуги. Они распространялись под видом различного ПО, включая мессенджеры, всевозможные системные утилиты, редакторы изображений, программы для фотосъемки, работы с документами и т. д.



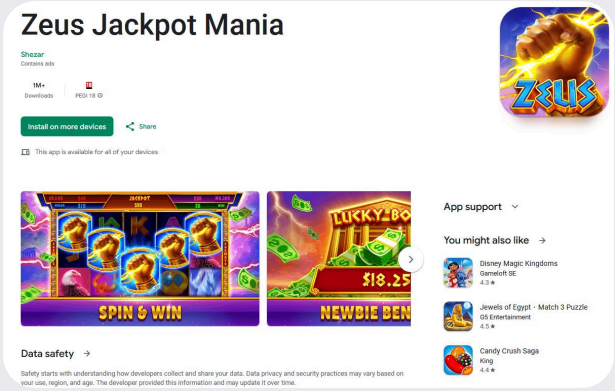
Один из троянов скрывался в программе для оптимизации работы системы Clean Boost (**Android.Joker.2412**), другой — в приложении Convert Text to PDF (**Android.Joker.2422**) для преобразования текста в PDF-документы

Кроме того, наши специалисты обнаружили очередные программы-подделки **Android.FakeApp**, используемые в мошеннических схемах. Как и прежде, некоторые из них киберпреступники выдавали за финансовые приложения — справочники, обучающие пособия, ПО для доступа к инвестиционным сервисам. Эти подделки загружали мошеннические сайты. Другие троянские программы **Android.FakeApp** распространялись под видом игр и при определенных условиях вместо обещанной функциональности загружали сайты букмекеров и онлайн-казино.



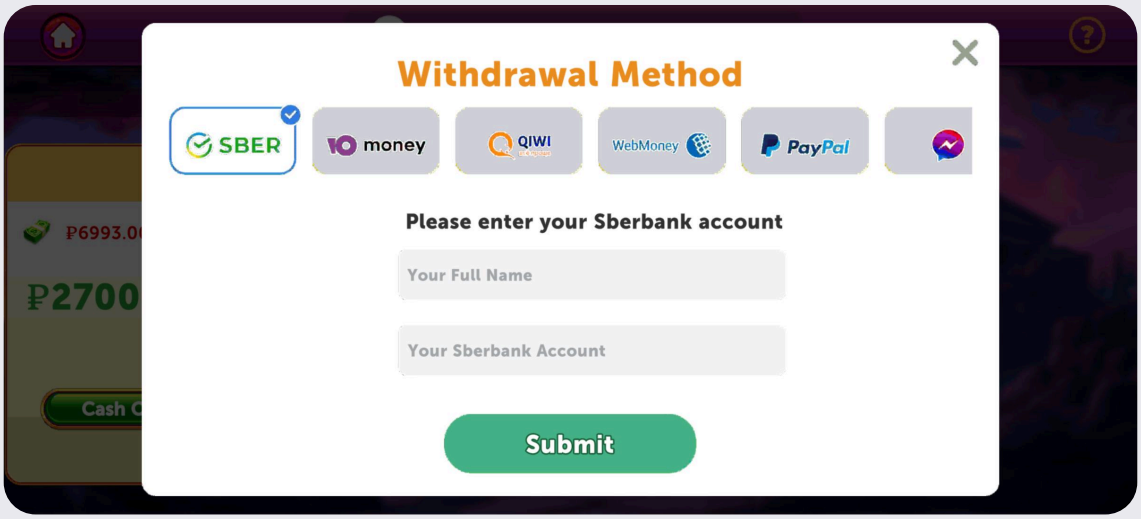
Примеры троянов **Android.FakeApp**, замаскированных под приложения финансовой тематики. **Android.FakeApp.1889** предлагал пользователям проверить финансовую грамотность, а **Android.FakeApp.1890** — развивать финансовое мышление

Также наши эксперты обнаружили нежелательную программу **Program.FakeMoney.16**, которая распространялась в виде приложения Zeus Jackpot Mania. Пользователи этого ПО получали виртуальные награды, которые затем якобы могли конвертировать в настоящие деньги и вывести из приложения.



Program.FakeMoney.16 в каталоге Google Play

Для «вывода» денег программа запрашивала ряд данных, однако никаких выплат жертвы в итоге не получали.



Program.FakeMoney.16 просит указать полное имя пользователя и сведения об учетной записи банка

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

Индикаторы компрометации

Подробнее

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

- Антивирусная правда
- Обучающие курсы
- Просветительные проекты

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
www.drweb.ru