Dr.WEB

«Доктор Веб»: обзор вирусной активности для мобильных устройств во II квартале 2025 года

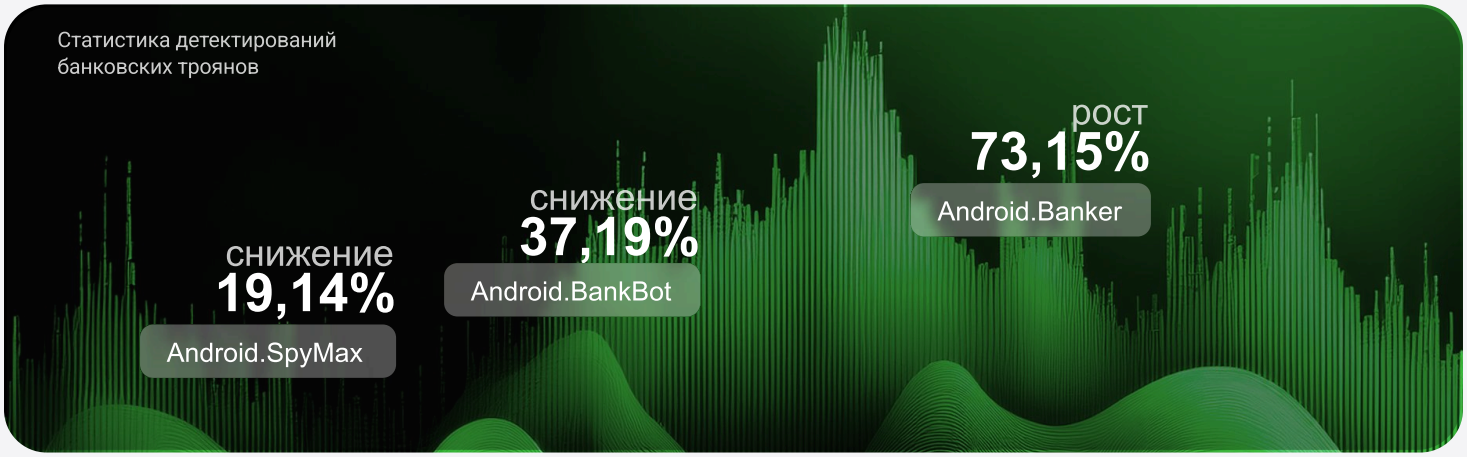
Главное

Согласно данным статистики детектирований Dr.Web Security Space для мобильных устройств, во II квартале 2025 года самыми распространенными вредоносными программами вновь стали рекламные трояны различных семейств. Наибольшая активность наблюдалась со стороны представителей группы **Android.HiddenAds** несмотря на то, что пользователи сталкивались с ними на 8,62% реже. Следом расположились рекламные трояны **Android.MobiDash**, число атак с их участием увеличилось на 11,17%. Вредоносные программы **Android.FakeApp**, которые применяются в различных мошеннических схемах, замыкают тройку лидеров — они детектировались на защищаемых устройствах на 25,17% реже.

Во II квартале 2025 года чаще всего детектировались:

1. **Android.HiddenAds** — рекламные трояны
2. **Android.MobiDash** — рекламные трояны
3. **Android.FakeApp** — вредоносные программы

Отмечался рост активности банковских троянов **Android.Banker** — на 73,15% по сравнению с предыдущим кварталом. В то же время ряд других семейств детектировался реже; например, **Android.BankBot** — на 37,19%, а **Android.SpyMax** — на 19,14%.



Android.Clipper.31

В апреле наши вирусные аналитики сообщили о выявленной масштабной кампании по краже криптовалют у владельцев Android-смартфонов. В ее рамках злоумышленники внедрили трояна Android.Clipper.31 в прошивку ряда бюджетных моделей, скрыв его в модифицированной версии приложения WhatsApp. Эта вредоносная программа перехватывает отправляемые и получаемые в мессенджере сообщения, ищет в них адреса криптокошельков Tron и Ethereum и заменяет их адресами, которые принадлежат мошенникам. При этом троян скрывает подмену, и пользователи зараженных устройств видят в таких сообщениях «правильные» кошельки. Кроме того, Android.Clipper.31 отправляет на удаленный сервер все изображения форматов *jpg*, *png* и *jpeg* с целью поиска в них мнемонических фраз для криптокошельков жертв.

Android.Spy.1292.origin

В этом же месяце мы рассказали о трояне-шпионе, нацеленном на российских военнослужащих. Вредоносная программа Android.Spy.1292.origin скрывалась в одной из модифицированных версий картографического ПО Alpine Quest. Она распространялась как через принадлежащий злоумышленникам поддельный Telegram-канал приложения, так и через один из российских каталогов Android-приложений. Android.Spy.1292.origin передавал атакующим различные конфиденциальные данные. Среди них — учетные записи пользователя, его номер мобильного телефона, контакты из телефонной книги, сведения о геолокации устройства, а также о хранящихся на нем файлах. По команде злоумышленников троян мог похищать заданные файлы. В частности, вирусописателей интересовали конфиденциальные документы, передаваемые через популярные мессенджеры, а также файл журнала локаций программы Alpine Quest.

Вместе с тем за прошедший период наблюдения вирусная лаборатория компании «Доктор Веб» выявила очередные угрозы в каталоге Google Play. Среди них были различные трояны, а также нежелательное рекламное ПО.

Главные тенденции II квартала

Снизилась активность рекламных троянов Android.HiddenAds

Увеличилась активность рекламных троянов Android.MobiDash

Снизилось число атак семейств банковских троянов Android.BankBot и Android.SpyMax

Очередные угрозы были выявлены в каталоге Google Play

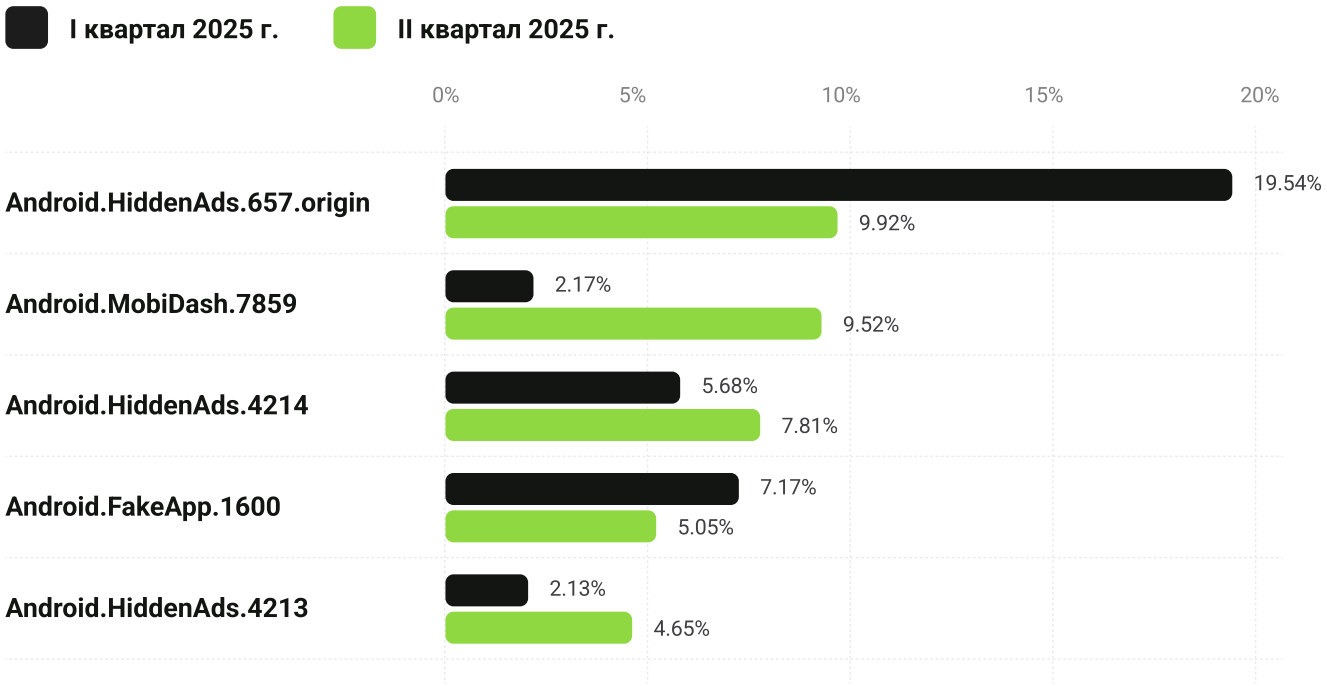
Злоумышленники распространяли трояна, который шпионил за российскими военнослужащими

Банковские трояны Android.Banker детектировались на защищаемых устройствах чаще, чем в предыдущем квартале

В прошивках ряда бюджетных моделей Android-смартфонов обнаружен троян для кражи криптовалют

По данным Dr.Web Security Space для мобильных устройств

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



Android.HiddenAds.657.origin **Android.HiddenAds.4214** **Android.HiddenAds.4213**

Троянские программы 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.

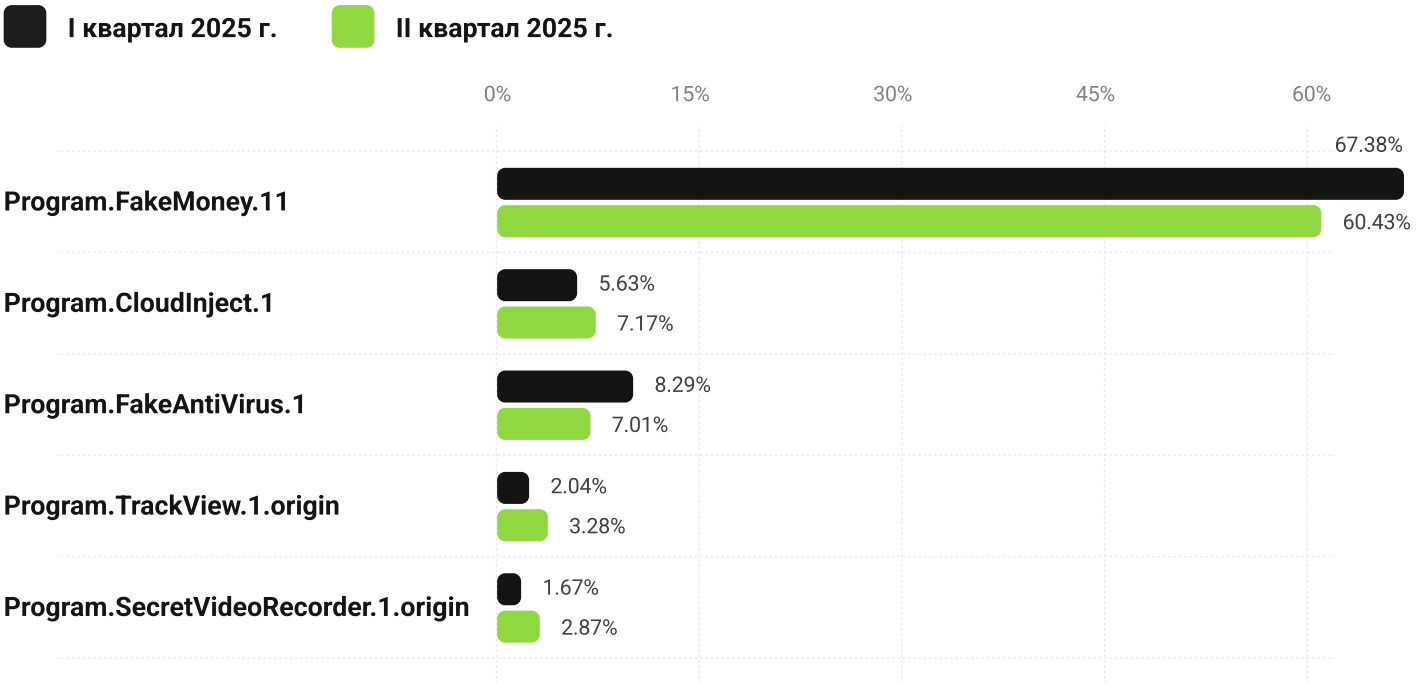
Android.MobiDash.7859

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.

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.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.

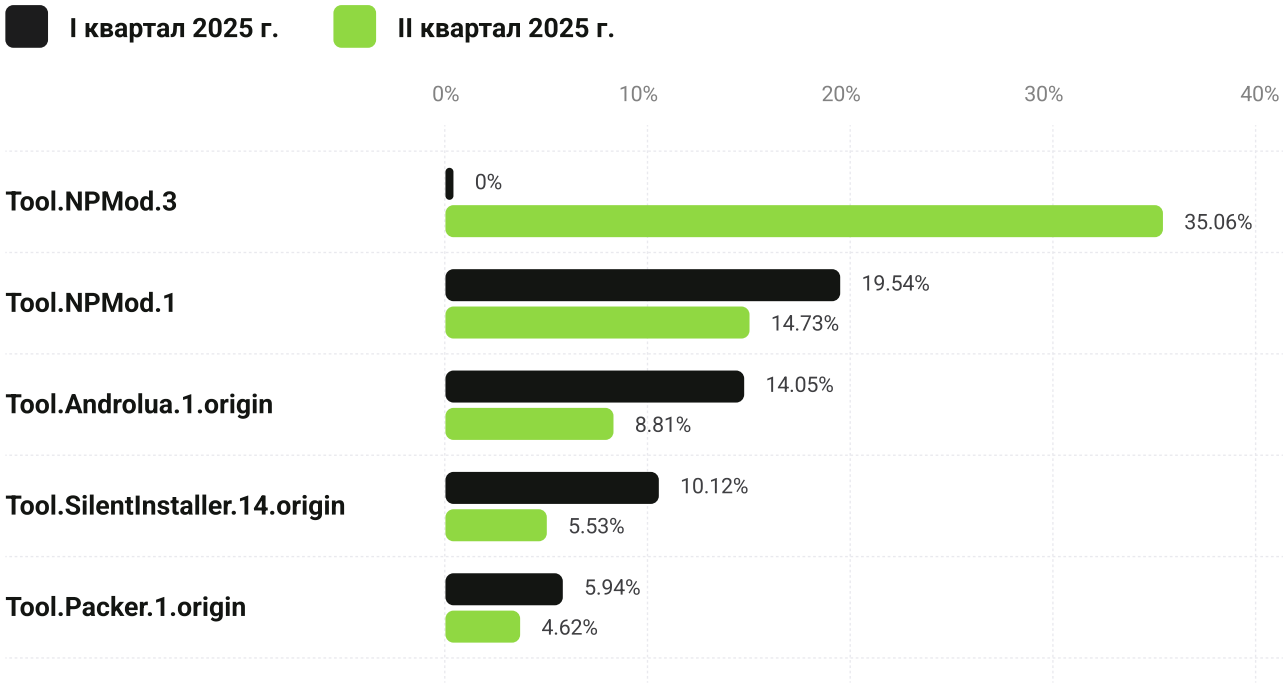
Program.TrackView.1.origin

Детектирование приложения, позволяющего 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.

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.

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



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

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.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.

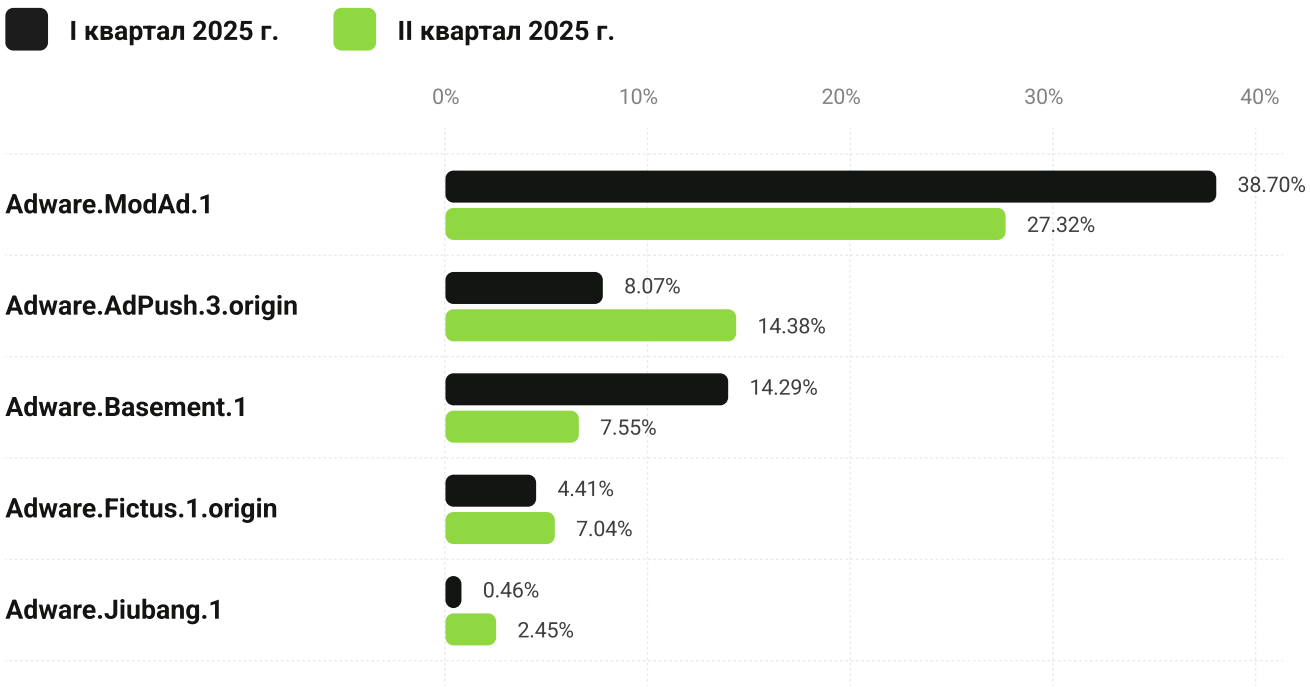
Tool.Packer.1.origin

Специализированная утилита-упаковщик для защиты Android-приложений от модификации и обратного инжиниринга. Она не является вредоносной, но может использоваться для защиты как безобидных, так и троянских программ.

Tool.SilentInstaller.14.origin

Потенциально опасная программная платформа, которая позволяет приложениям запускать APK-файлы без их установки. Эта платформа создает виртуальную среду исполнения в контексте приложений, в которые они встроены. Запускаемые с их помощью APK-файлы могут работать так, как будто являются частью таких программ, и автоматически получать те же разрешения.

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



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.AdPush.3.origin

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.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.

Adware.Fictus.1.origin

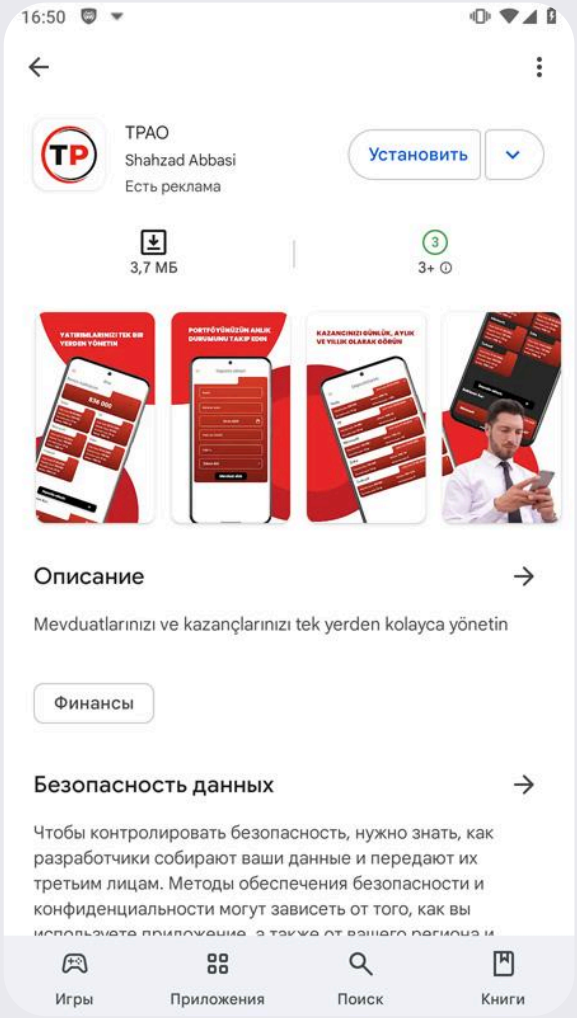
Рекламный модуль, который злоумышленники встраивают в версии-клоны популярных Android-игр и программ. Его интеграция в программы происходит при помощи специализированного упаковщика net2share. Созданные таким образом копии ПО распространяются через различные каталоги приложений и после установки демонстрируют нежелательную рекламу.

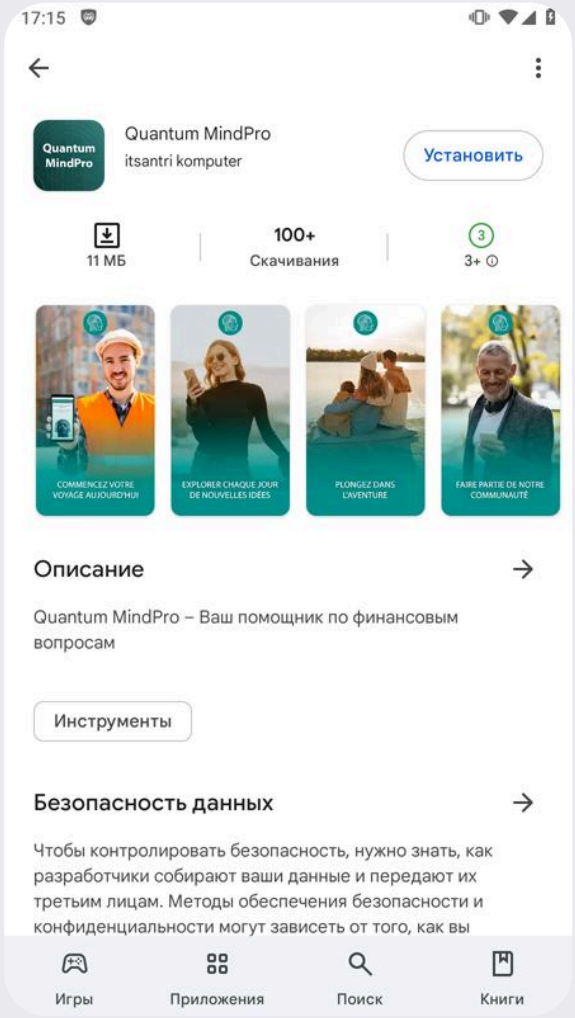
Adware.Jiubang.1

Нежелательное рекламное ПО для Android-устройств, которое при установке приложений демонстрирует баннер с рекомендуемыми к установке программами.

Угрозы в Google Play

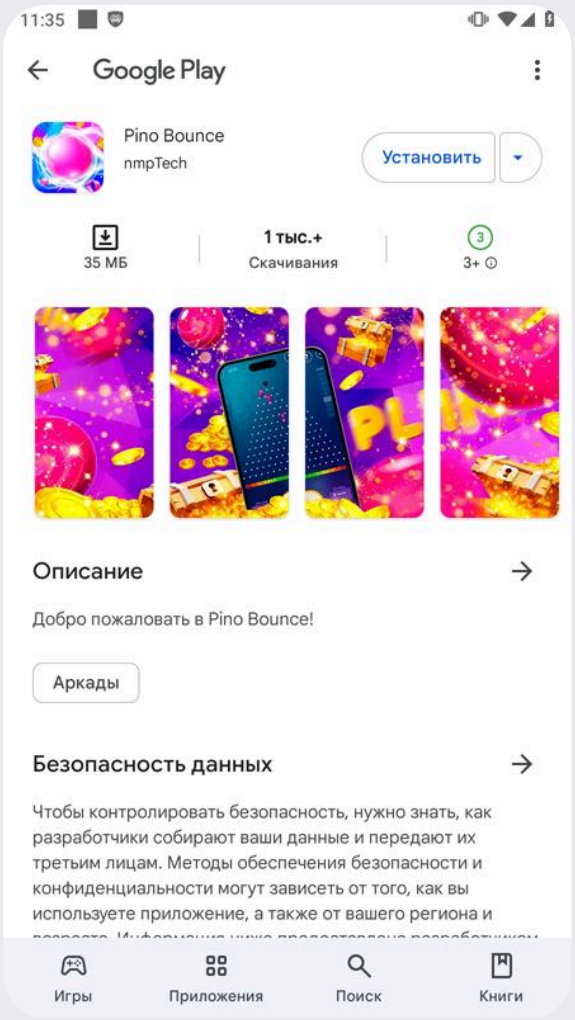
В течение II квартала 2025 года вирусные аналитики «Доктор Веб» обнаружили в каталоге Google Play несколько десятков угроз, включая разнообразные программы-подделки Android.FakeApp. Эти трояны вновь активно распространялись под видом приложений финансовой тематики и вместо обещанной функциональности могли загружать мошеннические сайты.





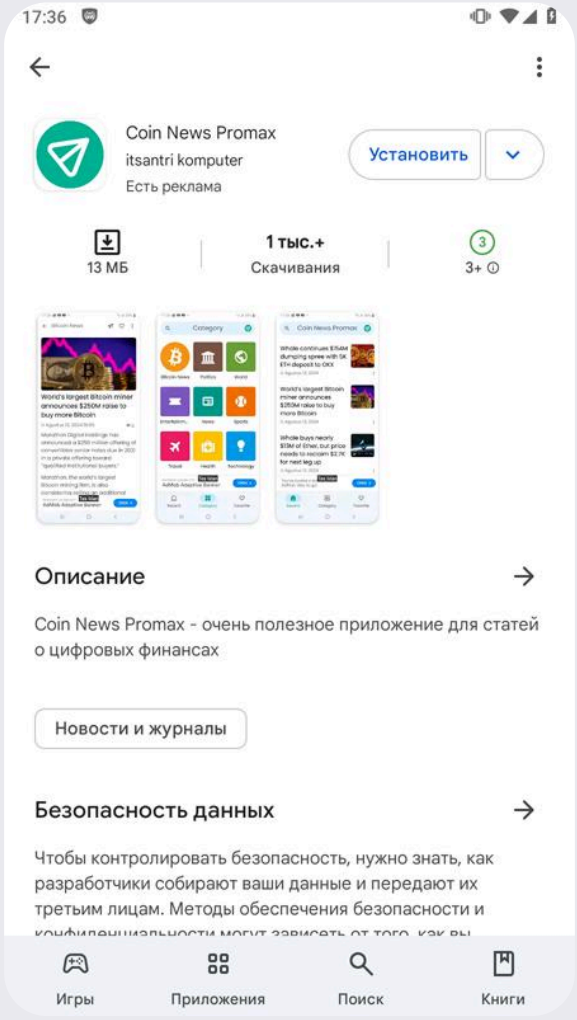
Android.FakeApp.1863 и **Android.FakeApp.1859** — примеры обнаруженных троянов. Первый скрывался в программе TPAO и был нацелен на турецких пользователей, которым предлагалось «легко управлять своими депозитами и доходами». Второго злоумышленники выдавали за «помощник по финансовым вопросам» Quantum MindPro, который был рассчитан на франкоговорящую аудиторию

Другим популярным прикрытием для таких программ-подделок остаются игры. При определенных условиях вместо игровой функциональности они загружают сайты онлайн-казино и букмекерских контор.



Android.FakeApp.1840 (Pino Bounce) — одна из поддельных игр, которая могла загружать сайт онлайн-казино

Вместе с тем наши специалисты выявили новое нежелательное рекламное ПО **Adware.Adpush.21912**. Оно скрывалось в программе с информационными материалами о криптовалютах Coin News Promax. **Adware.Adpush.21912** демонстрирует уведомления, при нажатии на которые в WebView загружается заданная управляющим сервером ссылка.



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