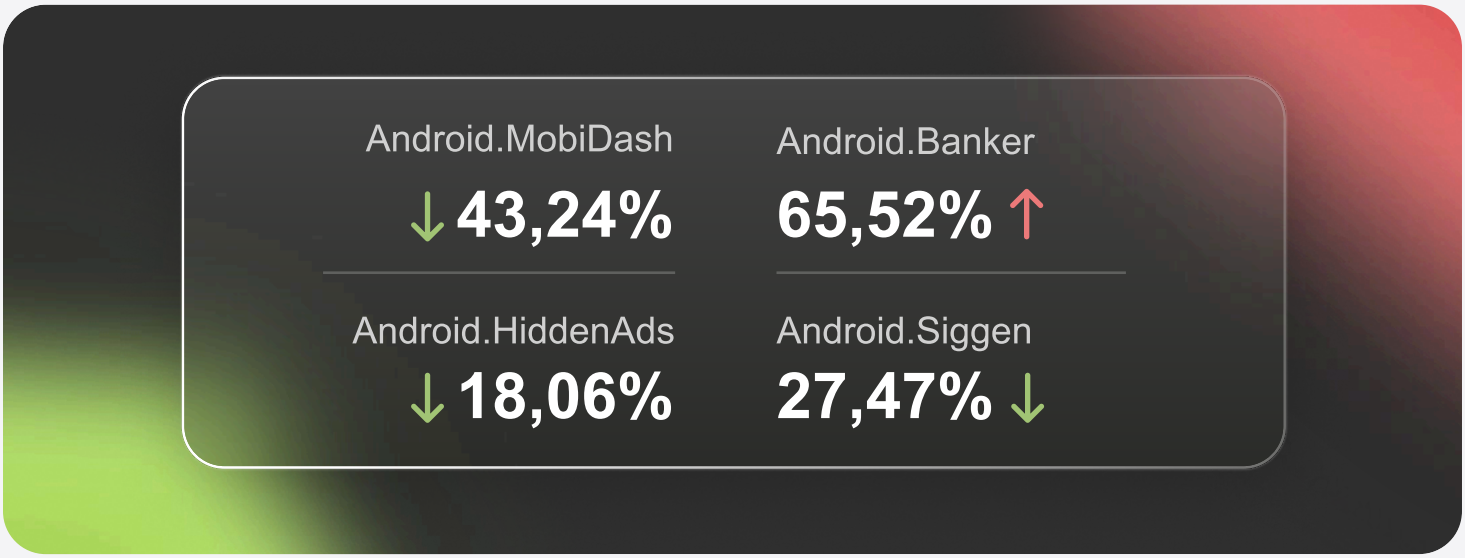
Dr.WEB

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

Главное

Согласно данным статистики детектирований Dr.Web Security Space для мобильных устройств, в IV квартале 2025 года самыми распространенными Android-угрозами вновь стали рекламные трояны **Android.MobiDash** и **Android.HiddenAds**, демонстрирующие надоедливые объявления. При этом их активность снизилась: первые обнаруживались на защищаемых устройствах на 43,24% реже, а вторые — на 18,06%. За ними расположились трояны семейства **Android.Siggen**, которые включают вредоносные приложения, обладающие различной функциональностью. Они также детектировались несколько реже — на 27,47%.

В то же время отмечался заметный рост активности банковских троянов, с которыми пользователи сталкивались чаще на 65,52%. Этот рост произошел в большей степени за счет представителей семейства **Android.Banker**. Такие вредоносные программы перехватывают СМС с одноразовыми кодами для подтверждения банковских операций, а также могут имитировать внешний вид настоящего банковского ПО и демонстрировать фишинговые окна.



Среди нежелательного ПО наибольшее распространение получили Android-программы, модифицированные через облачный сервис CloudInject (антивирус Dr.Web детектирует их как **Program.CloudInject**). С его помощью в приложения добавляются опасные системные разрешения и обфусцированный код, функциональность которого невозможно проконтролировать.

Кроме того, на устройствах часто встречались поддельные антивирусы **Program.FakeAntiVirus**, которые обнаруживают несуществующие угрозы и для их «лечения» требуют приобрести полную версию, а также **Program.FakeMoney** — приложения, якобы позволяющие зарабатывать на выполнении различных заданий.

Самым распространенным потенциально опасным ПО в IV квартале стали приложения **Tool.NPMod**, модифицированные при помощи утилиты NP Manager. Она обфусцирует код модов и добавляет в них специальный модуль, позволяющий обходить проверку цифровой подписи после модификации приложений. Среди рекламных программ лидерство сохранили представители семейства **Adware.Adpush**. Это специальные программные модули, которые разработчики встраивают в ПО для демонстрации рекламных уведомлений.

В октябре наши специалисты рассказали об опасном бэкдоре **Android.Backdoor.Baohuo.1.origin**, который злоумышленники встроили в неофициальные модификации мессенджера Telegram X и распространяли как через вредоносные сайты, так и через сторонние каталоги Android-приложений. Вредоносная программа похищает логины и пароли от учетных записей Telegram, а также другие конфиденциальные данные. Кроме того, с ее помощью киберпреступники фактически способны управлять аккаунтом жертвы и незаметно выполнять в мессенджере различные действия от ее имени. Например — присоединяться к Telegram-каналам и выходить из них, скрывать новые авторизованные устройства, скрывать определенные сообщения и т. д.

Android.Backdoor.Baohuo.1.origin управляется в том числе через базу данных Redis, что ранее не встречалось в Android-угрозах. В общей сложности бэкдор заразил порядка 58 000 устройств, среди которых около 3 000 различных моделей смартфонов, планшетов, ТВ-приставок и автомобилей с бортовыми компьютерами на базе Android.

За минувший квартал антивирусная лаборатория компании «Доктор Веб» выявила в каталоге Google Play новые вредоносные программы, среди которых были трояны **Android.Joker**, подписывающие жертв на платные услуги, и различные программы-подделки **Android.FakeApp**, применяемые в мошеннических схемах. В общей сложности их загрузили по меньшей мере 263 000 раз.

Главные тенденции IV квартала

Рекламные трояны остаются наиболее распространенными Android-угрозами

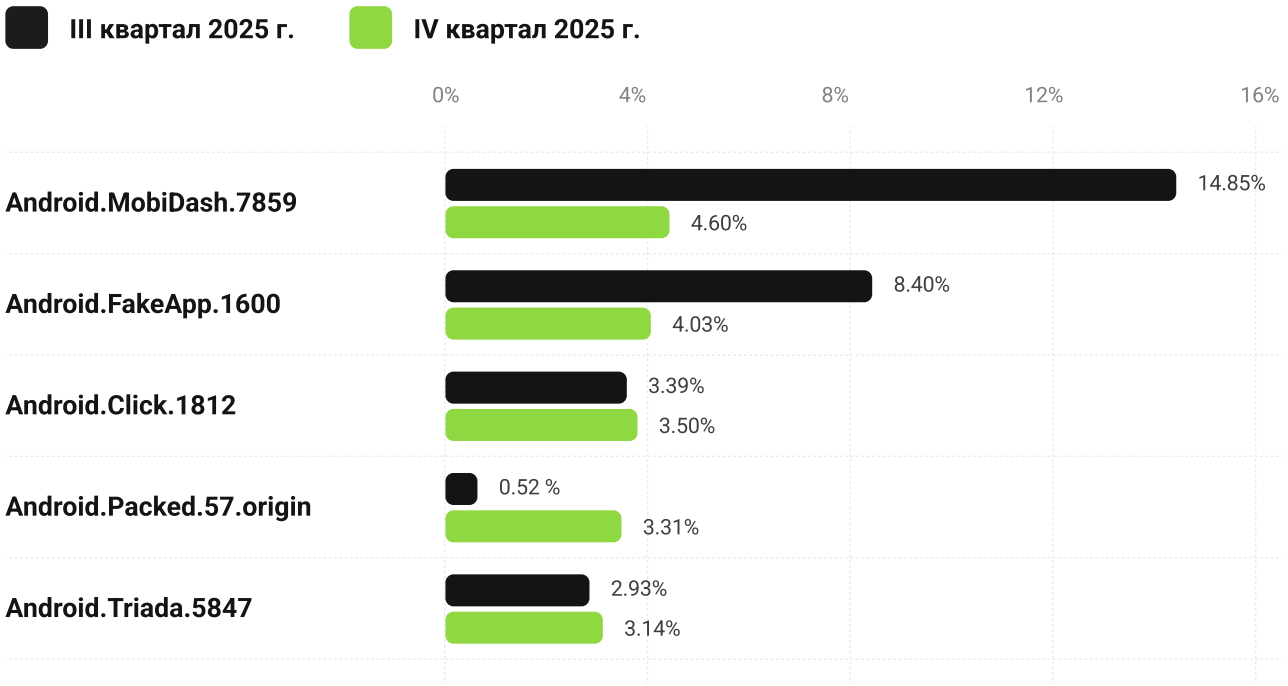
Распространение опасного бэкдора Android.Backdoor.Baohuo.1.origin, встроенного в модификации мессенджера Telegram X

Рост числа атак банковских троянов

Появление очередных вредоносных приложений в каталоге Google Play

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.Click.1812

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

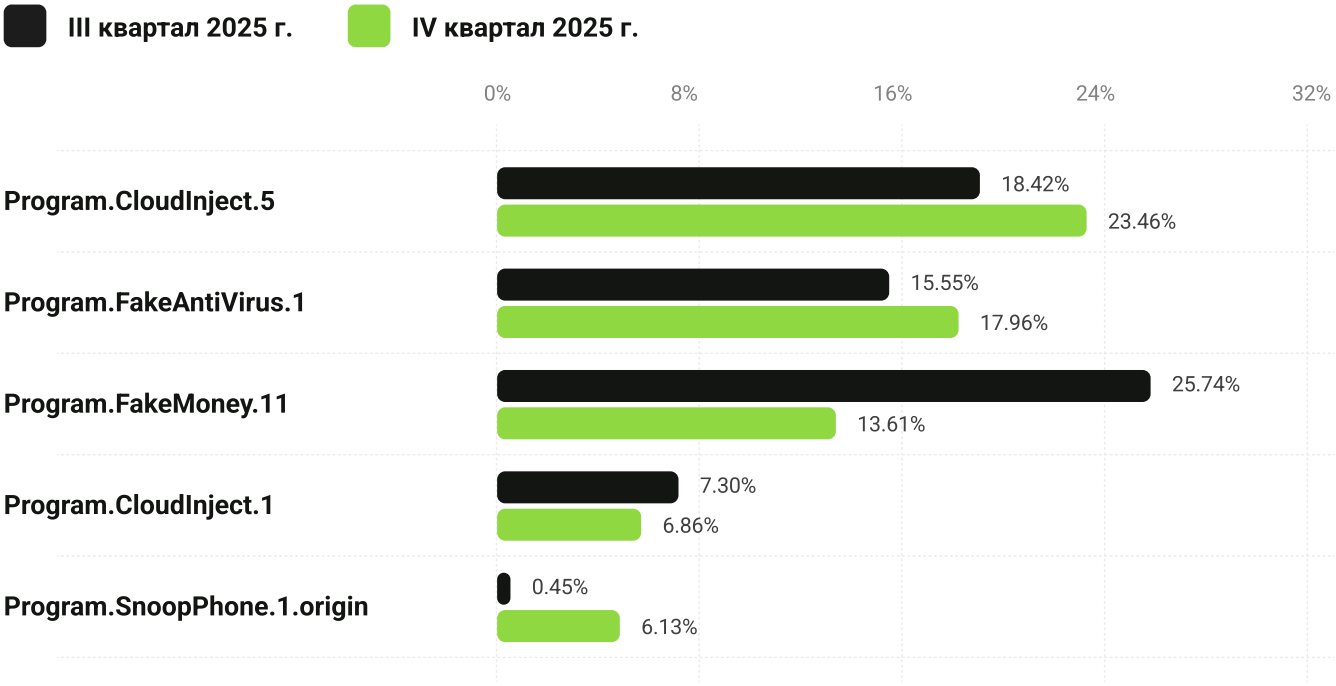
Android.Packed.57.origin

Детектирование обфускатора, который в том числе используется для защиты вредоносных приложений (например, некоторых версий банковских троянов **Android.SpyMax**).

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.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.

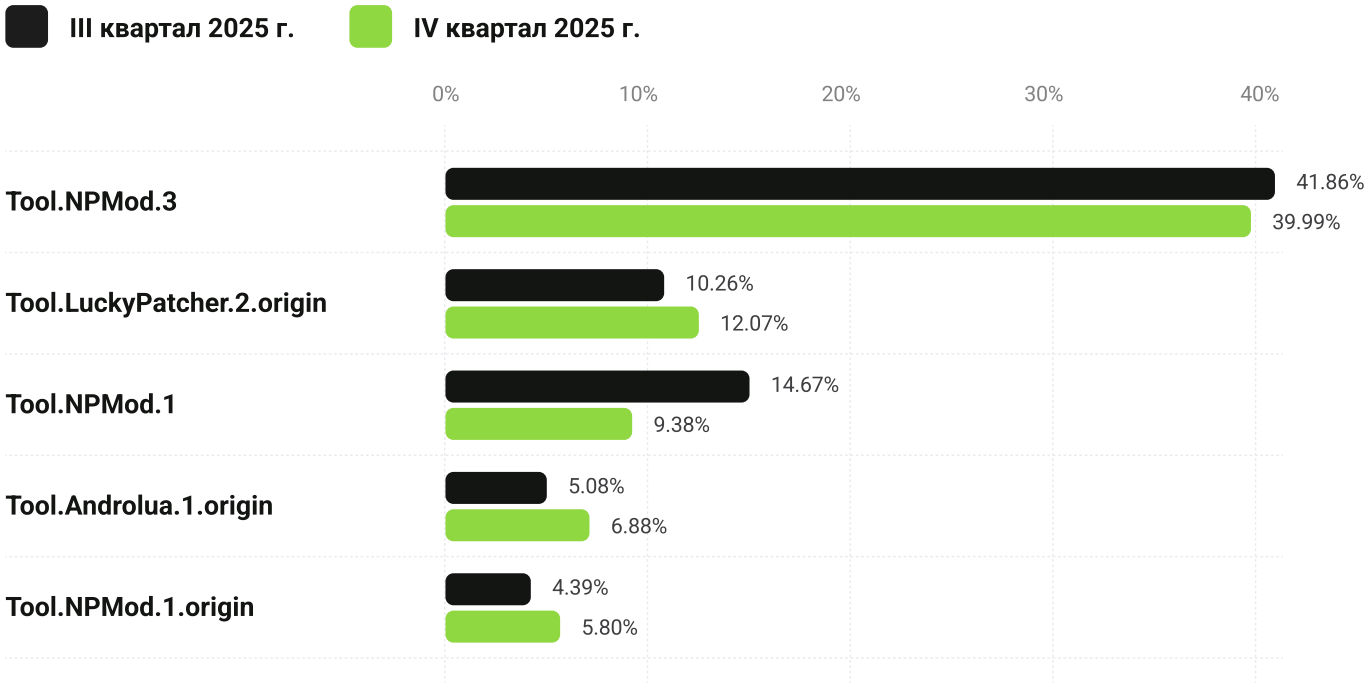
Program.FakeMoney.11

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.SnoopPhone.1.origin

Программа для наблюдения за владельцами Android-устройств. Она позволяет читать СМС, получать информацию о телефонных вызовах, отслеживать местоположение устройства и выполнять аудиозапись окружения.

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



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

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

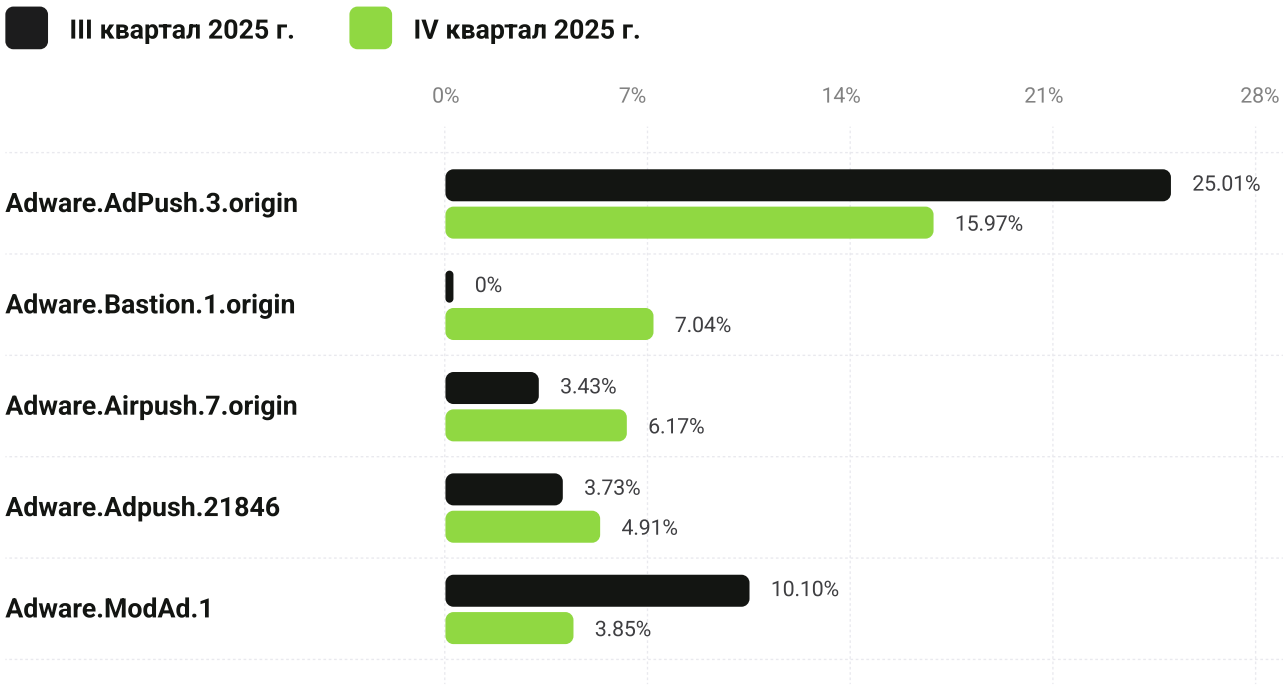
Tool.LuckyPatcher.2.origin

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.Bastion.1.origin

Детектирование программ-оптимизаторов, которые периодически создают уведомления с вводящими в заблуждение сообщениями о якобы нехватке памяти и ошибках системы с целью показывать рекламу во время «оптимизации».

Adware.Airpush.7.origin

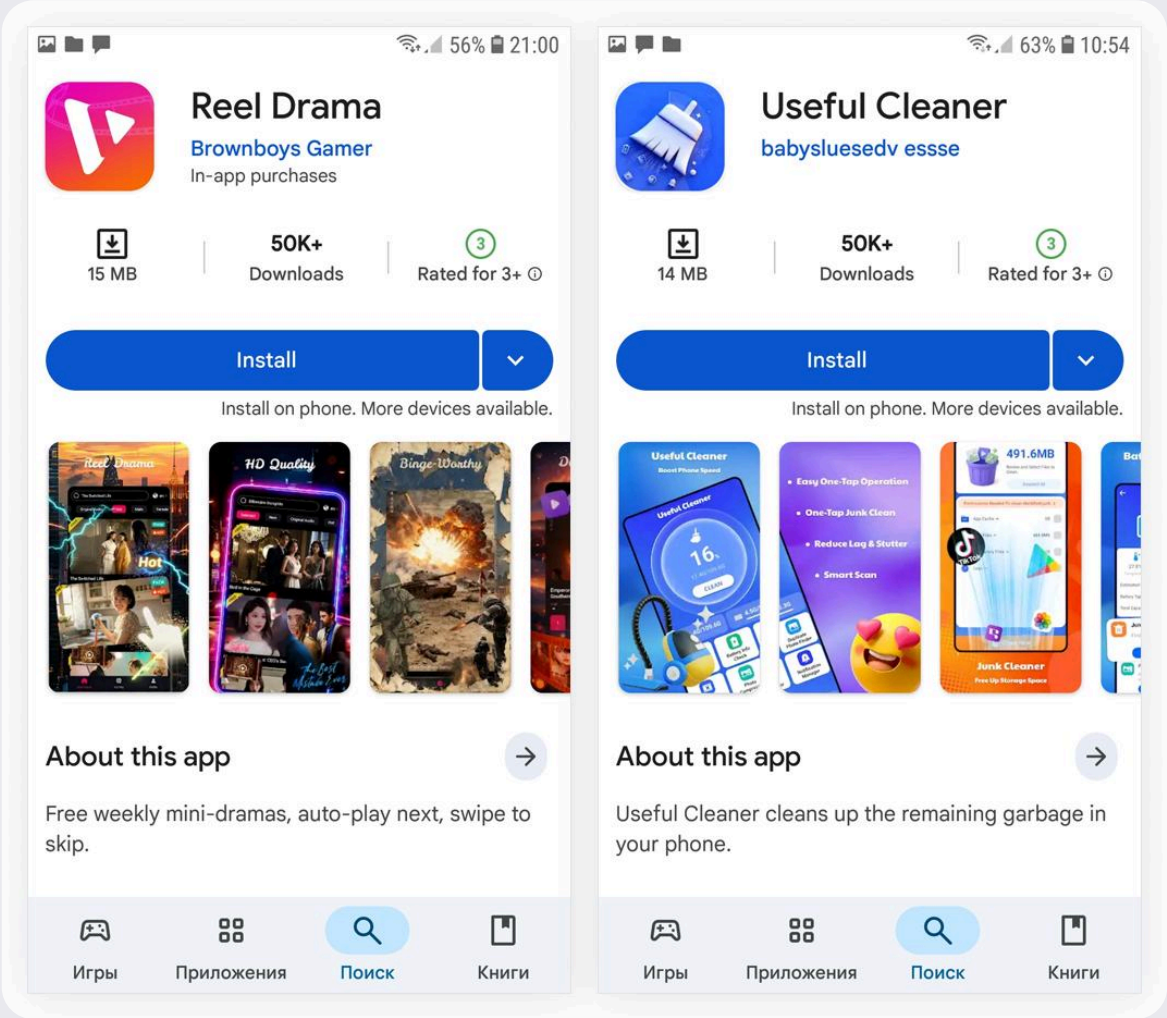
Программные модули, встраиваемые в Android-приложения и демонстрирующие разнообразную рекламу. В зависимости от версии и модификации это могут быть рекламные уведомления, всплывающие окна или баннеры. С помощью данных модулей злоумышленники часто распространяют вредоносные программы, предлагая установить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

Adware.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.

Угрозы в Google Play

В течение IV квартала 2025 года вирусные аналитики компании «Доктор Веб» зафиксировали появление в каталоге Google Play более двух десятков вредоносных приложений **Android.Joker**, предназначенных для подписки пользователей на платные услуги. Злоумышленники замаскировали их под различное ПО: мессенджеры, утилиты для оптимизации работы системы, графические редакторы и программы для просмотра фильмов.



Примеры выявленных вредоносных программ **Android.Joker. Android.Joker.2496** был замаскирован под инструмент Useful Cleaner для «очистки мусора» на телефоне, а одна из модификаций **Android.Joker.2495** — под проигрыватель фильмов Reel Drama

Также наши специалисты обнаружили несколько новых программ-подделок из семейства **Android.FakeApp**. Как и ранее, некоторые из них распространились под видом финансовых приложений и загружали мошеннические сайты. Другие такие подделки выдавались за игры. При определенных условиях (например, если IP-адрес пользователя удовлетворял требованиям злоумышленников) они могли загружать сайты букмекерских контор и онлайн-казино.

Игра Chicken Road Fun являлась программой-подделкой **Android.FakeApp.1910**, и вместо того, чтобы предоставить ожидаемую пользователем функциональность, могла загрузить сайт онлайн-казино

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