Dr.WEB

«Доктор Веб»: обзор вирусной активности для мобильных устройств в IV квартале 2024 года

2024

Главное

Согласно данным статистики детектирований Dr.Web Security Space для мобильных устройств, в **IV квартале 2024 года** наиболее распространенными вредоносными программами стали рекламные трояны **Android.HiddenAds**. За ними расположились используемые в мошеннических целях вредоносные приложения **Android.FakeApp**. Тройку лидеров замыкали трояны **Android.Siggen** с различной вредоносной функциональностью.

ТРОЙКА ЛИДЕРОВ ПО РАСПРОСТРАНЕННОСТИ

- Android.HiddenAds
- Android.FakeApp
- Android.Siggen

В течение квартала вирусные аналитики компании «Доктор Веб» выявили множество угроз в каталоге Google Play. Среди них были многочисленные трояны **Android.FakeApp**, а также вредоносные программы семейств **Android.Subscription** и **Android.Joker**, которые подписывали пользователей на платные услуги. Были зафиксированы очередные рекламные трояны **Android.HiddenAds**. Кроме того, злоумышленники распространяли вредоносные приложения, защищенные сложным упаковщиком.

Главные тенденции IV квартала

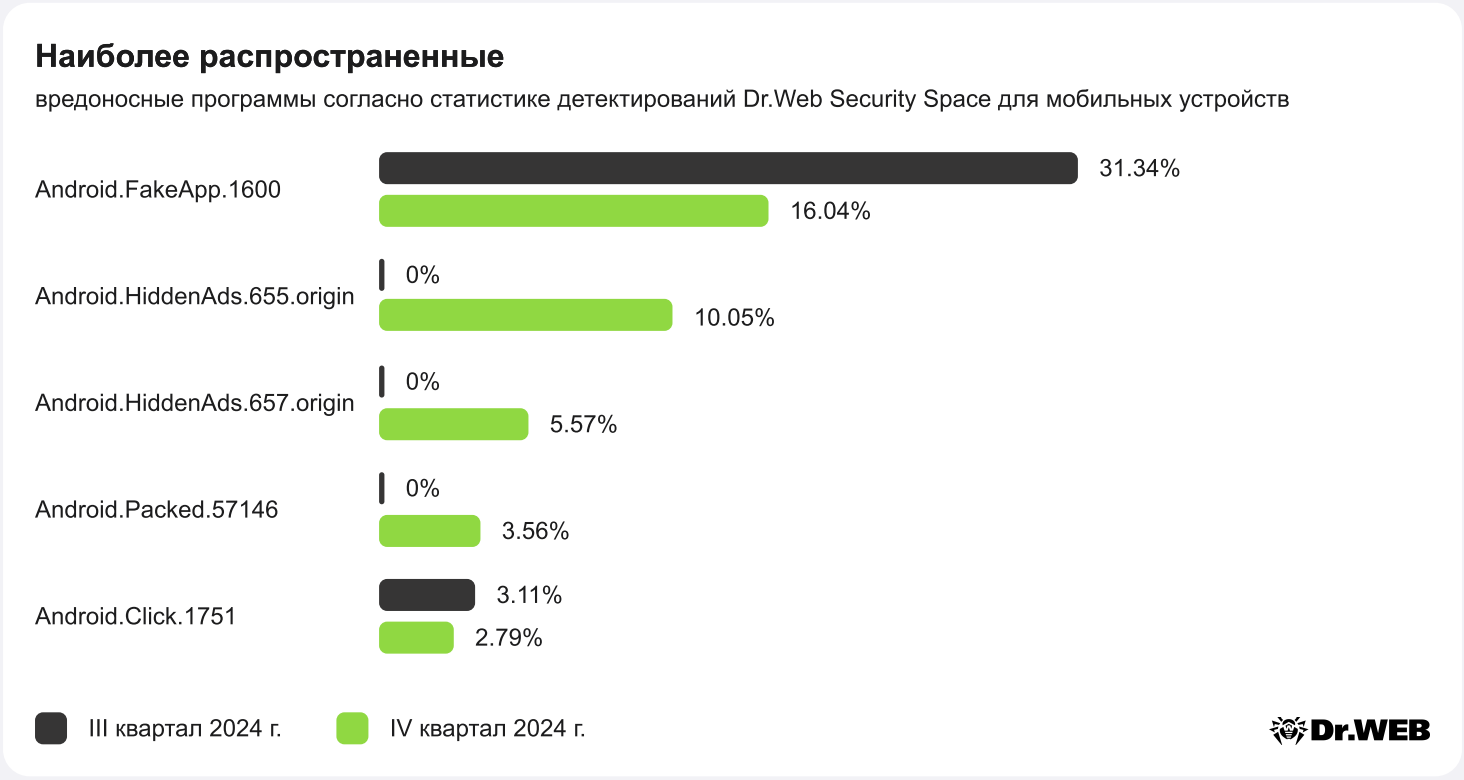
Рекламные трояны

Высокая активность рекламных троянов Android.HiddenAds и мошеннических программ Android.FakeApp

Google Play

Распространение множества вредоносных приложений через каталог Google Play

По данным Dr.Web Security Space для мобильных устройств



Android.FakeApp.1600

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

Android.Packed.57083

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

Android.HiddenAds.655.origin

Android.HiddenAds.657.origin

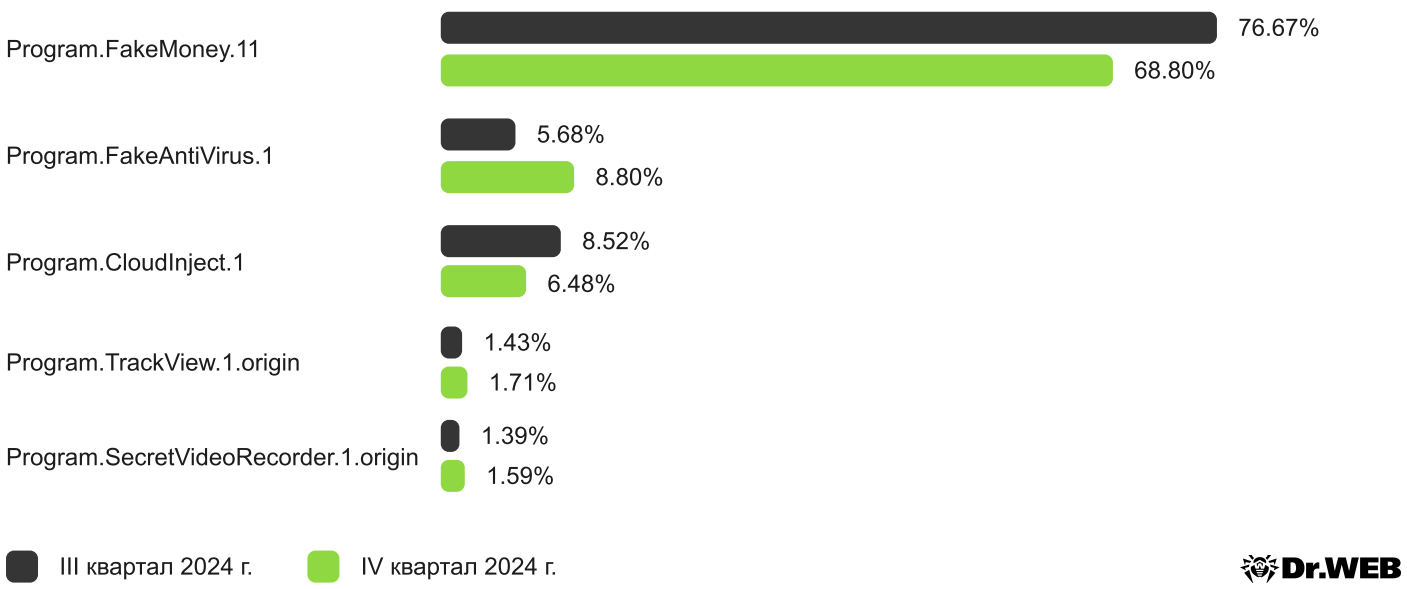
Троянские программы для показа навязчивой рекламы. Представители семейства Android.HiddenAds часто распространяются под видом безобидных приложений и в некоторых случаях устанавливаются в системный каталог другим вредоносным ПО. Попадая на Android-устройства, такие рекламные трояны обычно скрывают от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

Android.Click.1751

Троян, встраиваемый в модификации мессенджера WhatsApp и маскирующийся под классы библиотек от Google. Во время использования приложения-носителя Android.Click.1751 делает запросы к одному из управляющих серверов. В ответ троян получает две ссылки, одна из которых предназначена для русскоязычных пользователей, а другая — для всех остальных. Затем он демонстрирует диалоговое окно с полученным от сервера содержимым и после нажатия пользователем на кнопку подтверждения загружает соответствующую ссылку в браузере.

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.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.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.TrackView.1.origin

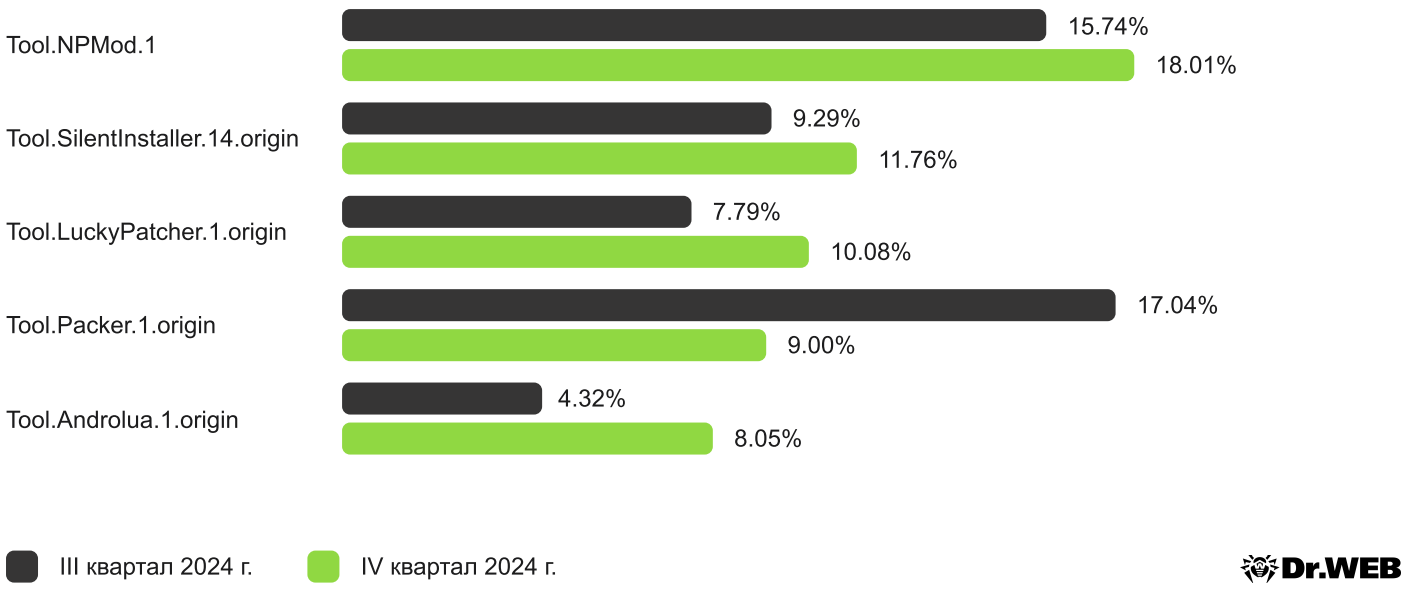
Детектирование приложения, позволяющего вести наблюдение за пользователями через Android-устройства. С помощью этой программы злоумышленники могут определять местоположение целевых устройств, использовать камеру для записи видео и создания фотографий, выполнять прослушивание через микрофон, создавать 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.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.SilentInstaller.17.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.

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 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.Packer.1.origin

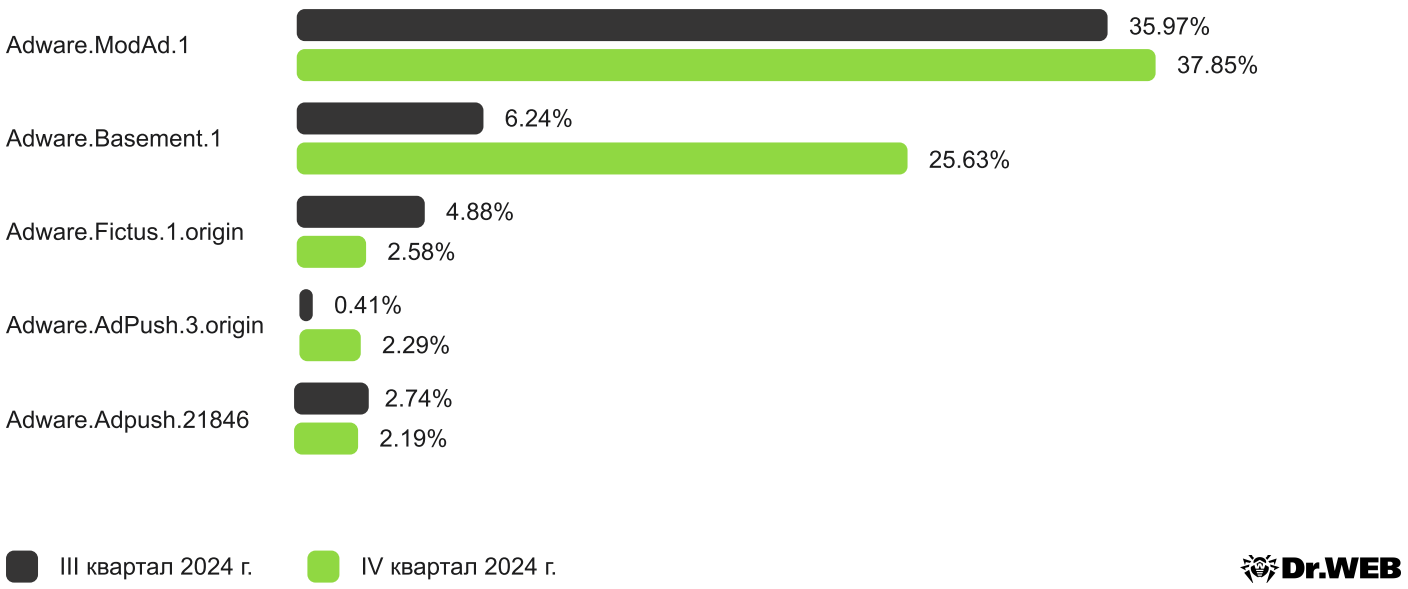
Специализированная утилита-упаковщик для защиты Android-приложений от модификации и обратного инжиниринга. Она не является вредоносной, но может использоваться для защиты как безобидных, так и троянских программ.

Tool.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.ModAd.1

Детектирование некоторых модифицированных версий (модов) мессенджера WhatsApp, в функции которого 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.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.

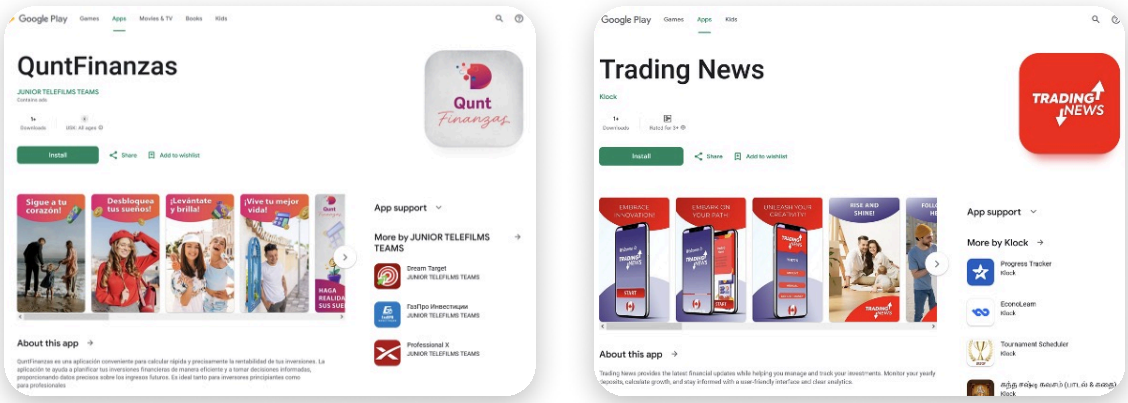
Adware.AdPush.3.origin

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.

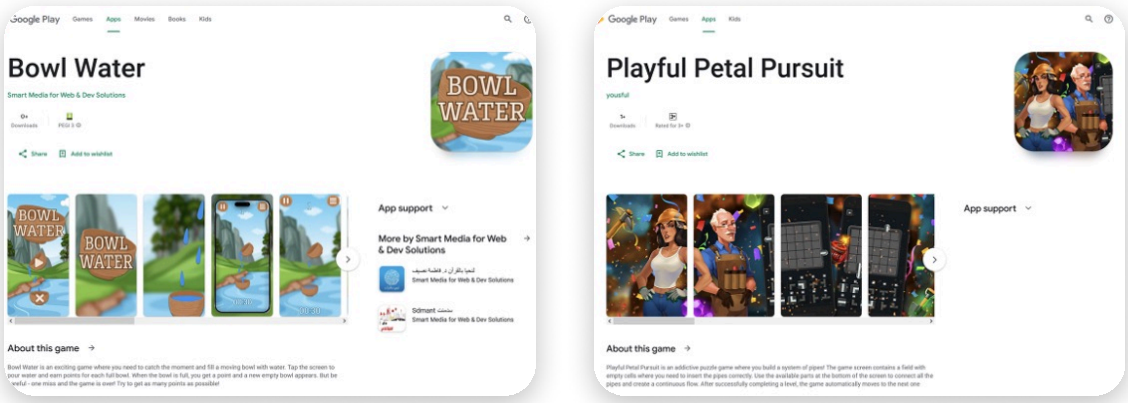
Угрозы в Google Play

В IV квартале 2024 года вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play свыше 60 различных вредоносных приложений, большинство из которых — трояны семейства Android.FakeApp. Часть из них распространялась под видом программ финансовой тематики, справочников и обучающих пособий, а также прочего ПО — дневников, записных книжек и т. п. Их основной задачей была загрузка мошеннических сайтов.



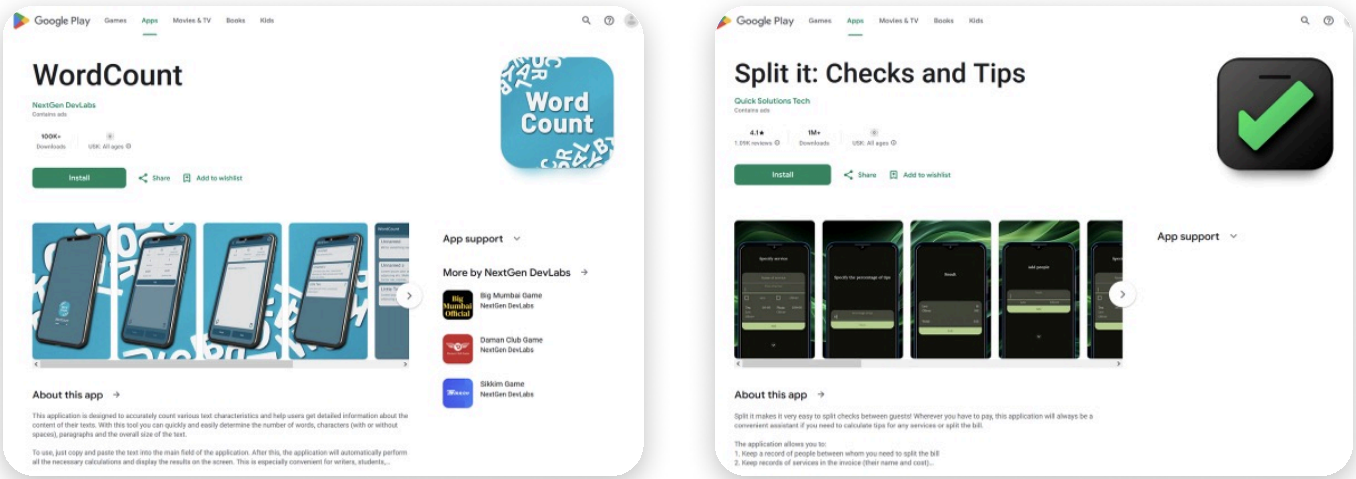
Программы QuntFinanzas и Trading News, которые в числе прочих многочисленных троянов Android.FakeApp загружали мошеннические сайты

Другие трояны Android.FakeApp злоумышленники выдавали за игры. Они могли загружать сайты онлайн-казино и букмекеров.



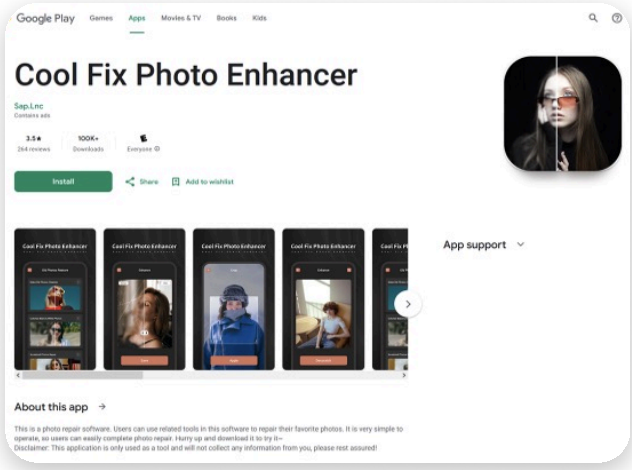
Bowl Water и Playful Petal Pursuit — примеры игр с троянской функциональностью

Вместе с тем наши специалисты обнаружили новые варианты трояна Android.FakeApp.1669, который скрывался под маской разнообразных приложений и также мог загружать сайты онлайн-казино. Android.FakeApp.1669 интересен тем, что получает адрес целевого сайта из TXT-файла вредоносного DNS-сервера. При этом он проявляет себя только при подключении к интернету через определенных провайдеров.



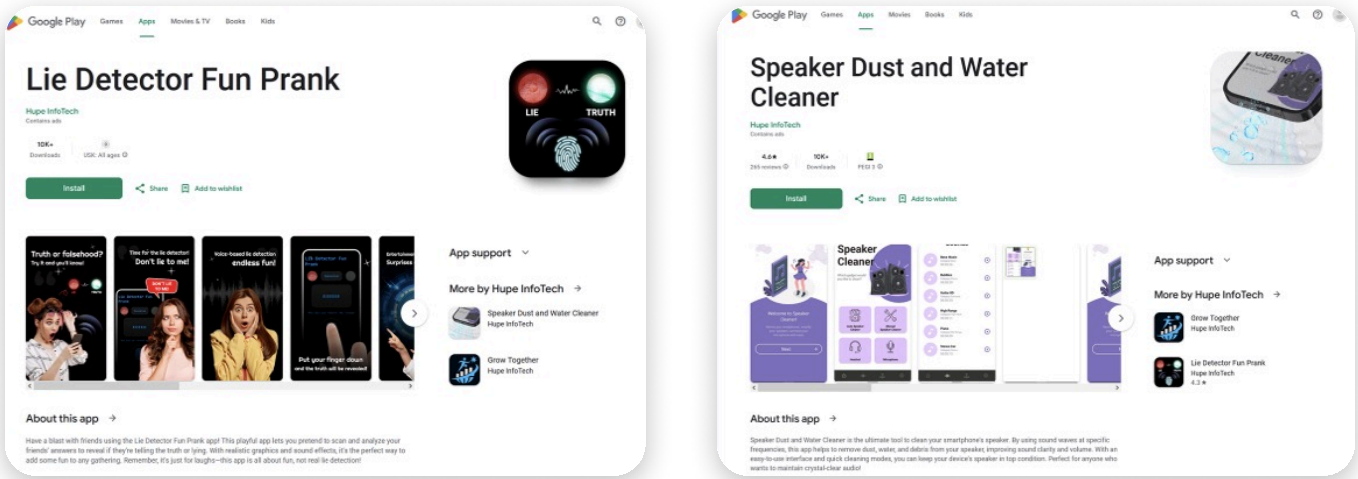
Примеры новых модификаций трояна Android.FakeApp.1669. Программу WordCount мошенники выдавали за текстовую утилиту, а программа Split it: Checks and Tips должна была помочь посетителям кафе и ресторанов с оплатой счетов и расчетом чаевых.

Среди найденных в Google Play угроз было несколько новых представителей семейства рекламных троянов Android.HiddenAds, которые скрывают свое присутствие на зараженных устройствах.



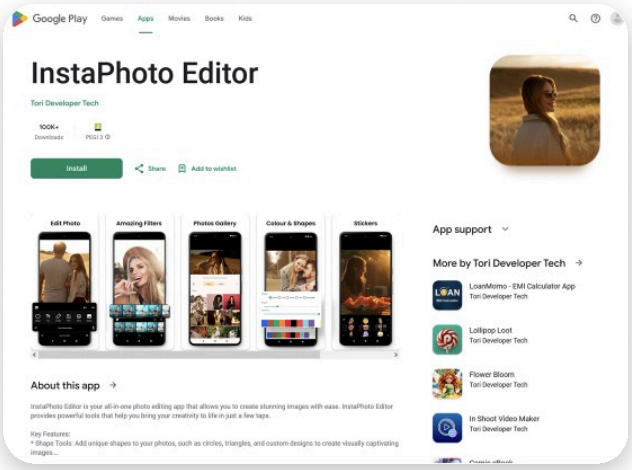
Фоторедактор Cool Fix Photo Enhancer скрывал рекламного трояна Android.HiddenAds.4013

Кроме того, были зафиксированы трояны, защищенные сложным программным упаковщиком — например, Android.Packed.57156, Android.Packed.57157 и Android.Packed.57159.



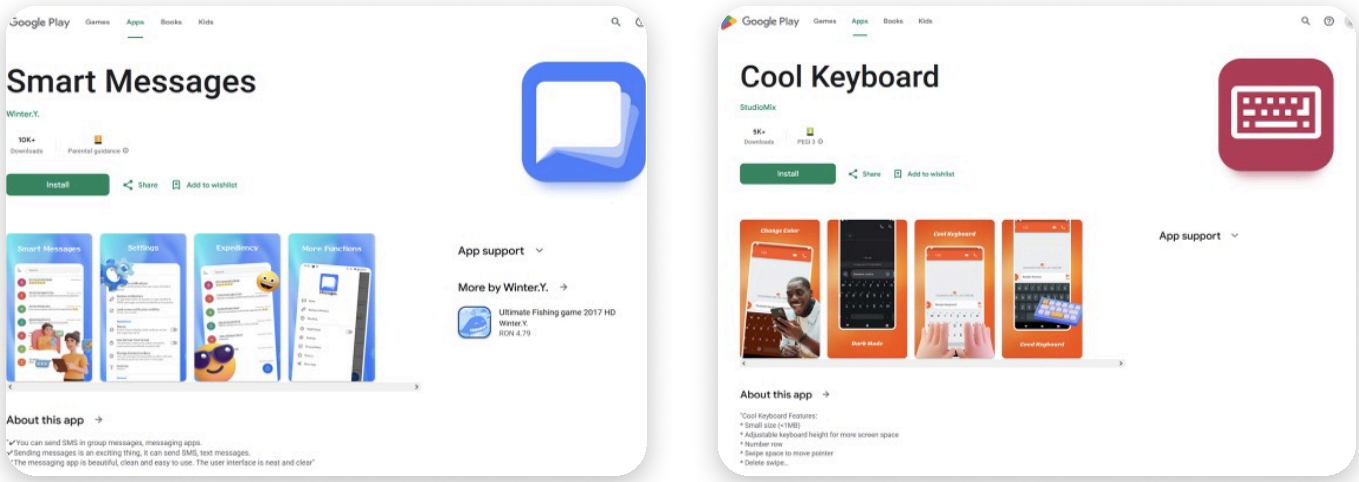
Приложения Lie Detector Fun Prank и Speaker Dust and Water Cleaner — трояны, защищенные упаковщиком

Также наши специалисты обнаружили вредоносную программу Android.Subscription.22, предназначенную для подписки пользователей на платные услуги.



Вместо редактирования фотографий приложение InstaPhoto Editor подписывало пользователей на платную услугу

При этом злоумышленники вновь распространяли троянов семейства Android.Joker, которые тоже подписывали жертв на платные сервисы.



СМС-мессенджер Smart Messages и сторонняя клавиатура Cool Keyboard пытались незаметно подписать жертв на платную услугу

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

Индикаторы компрометации

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 | www.drweb.ru
«Доктор Веб» в других странах