Dr.WEB

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2024 год

Главное

В 2024 году самыми распространенными Android-угрозами вновь стали рекламные трояны. При этом по сравнению с годом ранее возросла активность мошеннического ПО, троянов-вымогателей, кликеров и банковских троянов. Среди последних большее распространение по сравнению с 2023 годом получили более простые банковские трояны, которые похищают только учетные данные для входа в онлайн-банк и коды подтверждений из СМС.

Среди нежелательных программ наибольшую активность проявили приложения, предлагающие пользователям выполнять различные задания за виртуальные вознаграждения, которые затем якобы можно перевести в реальные деньги. Самыми детектируемыми потенциально опасными программами стали утилиты, позволяющие запускать Android-приложения без их установки. А наиболее активным рекламным ПО оказались специальным образом модифицированные версии мессенджера WhatsApp, в функции которых внедрен код для загрузки рекламных ссылок.

В течение года вирусные аналитики компании «Доктор Веб» обнаружили сотни новых угроз в каталоге Google Play, которые суммарно были загружены свыше 26 700 000 раз. Среди них были вредоносные программы, в том числе троян-шпион, а также нежелательные и рекламные приложения.

Наши специалисты также выявили новую атаку на ТВ-приставки на базе Android — около 1 300 000 устройств пострадали от бэкдора, который заражал системную область и по команде злоумышленников мог скачивать и устанавливать стороннее ПО.

Кроме того, вирусные аналитики «Доктор Веб» отмечали рост популярности ряда техник, направленных на усложнение анализа вредоносных Android-программ и обхода их детектирования антивирусами. Они включали различные манипуляции с форматом ZIP-архивов (формат ZIP является основой для APK-файлов Android-приложений), манипуляции с файлом конфигурации программ `AndroidManifest.xml` и другие. Чаще всего эти приемы встречались в банковских троянах.

Тенденции прошедшего года

Реклама

Демонстрирующие рекламу вредоносные программы остались наиболее распространенными угрозами

Банковские трояны

Рост активности банковских троянов

Киберпреступники

Киберпреступники стали чаще использовать простые банковские трояны Android.Banker, которые похищают только данные для входа в учетные записи онлайн-банка, а также проверочные коды из СМС

APK-приложения

Злоумышленники стали чаще прибегать к манипуляции форматом APK-приложений и их структурных компонентов для обхода детектирования и усложнения анализа вредоносных программ

Трояны-вымогатели

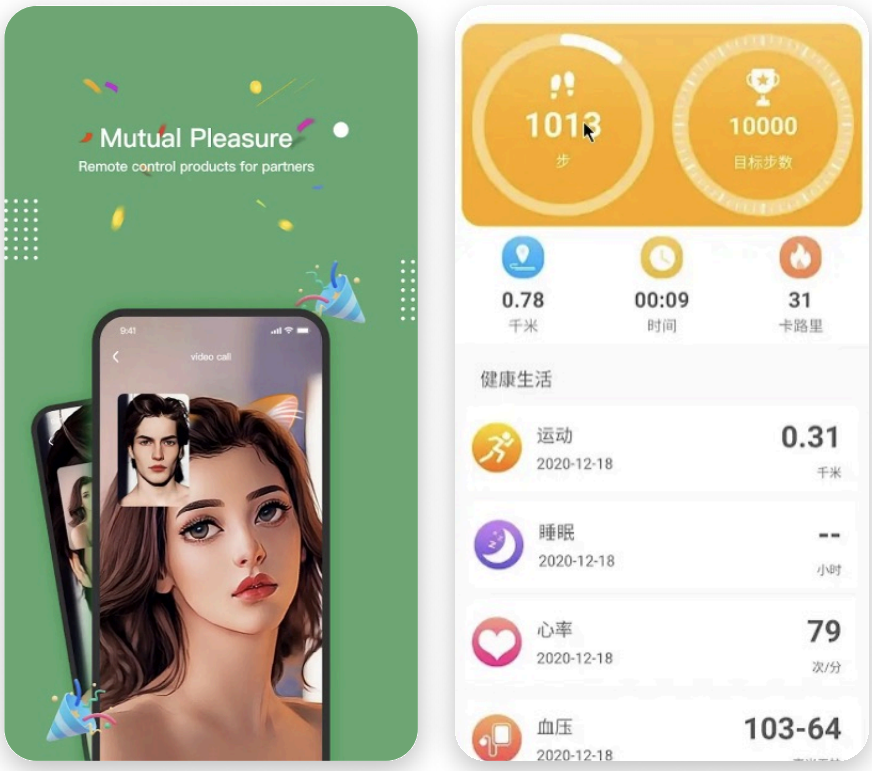
Рост числа детектирований троянов-вымогателей Android.Locker и троянов-кликеров Android.Click

Google Play

Появление множества новых угроз в каталоге Google Play

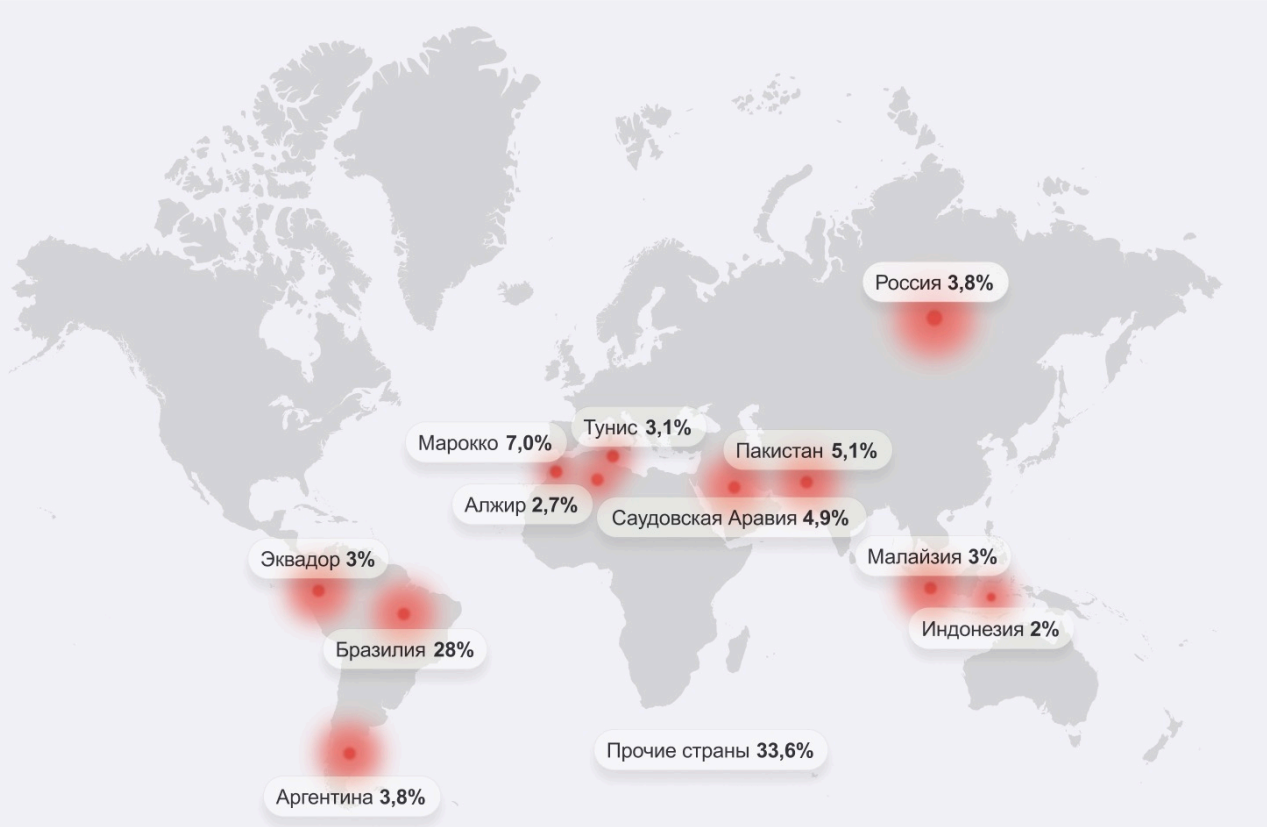
Наиболее интересные события 2024 года

В мае прошлого года эксперты компании «Доктор Веб» рассказали о трояне-кликере Android.Click.414.origin, найденном в приложении для управления секс-игрушками и в ПО для отслеживания физической активности. Обе программы распространялись через каталог Google Play и суммарно были установлены более 1 500 000 раз. Android.Click.414.origin имел модульную архитектуру и с помощью своих компонентов выполнял определенные задачи. Так, троян незаметно открывал рекламные сайты и совершал на них различные действия. Например, он мог прокручивать содержимое страниц, вводить текст в формы, отключать звук на веб-страницах и создавать их скриншоты для анализа содержимого и последующего выполнения кликов на нужных областях. Кроме того, Android.Click.414.origin передавал на управляющий сервер подробную информацию о зараженном устройстве. При этом кликер целенаправленно не атаковал определенных пользователей — он не запускался на устройствах, где был установлен китайский язык интерфейса.



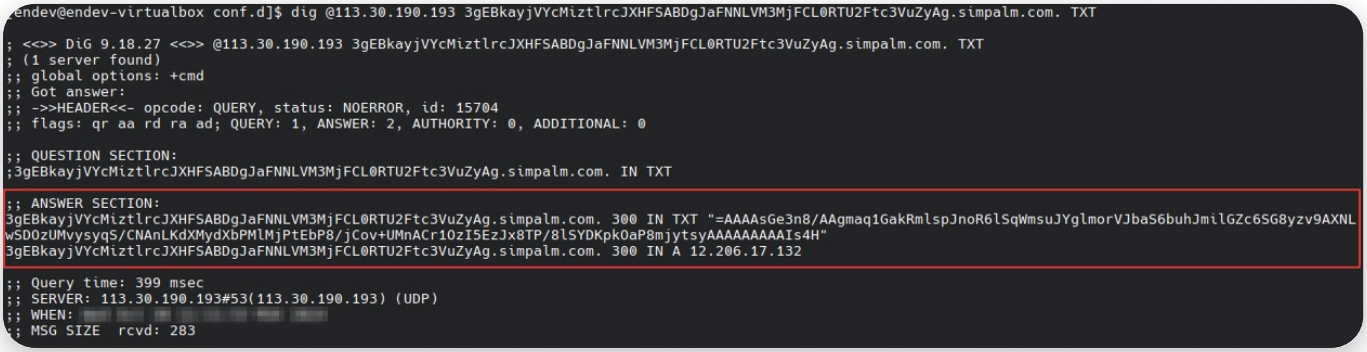
Некоторые версии программ Love Spouse и QRunning скрывали трояна Android.Click.414.origin

В сентябре наши специалисты раскрыли детали анализа случаев заражения ТВ-приставок на базе Android бэкдором Android.Vo1d. Эта модульная вредоносная программа проникла почти на 1 300 000 устройств пользователей из 197 стран. Она помещала свои компоненты в системную область и по команде злоумышленников могла скрытно загружать и устанавливать стороннее ПО.



Страны с наибольшим числом выявленных ТВ-приставок, зараженных бэкдором Android.Vo1d

Уже в ноябре наши вирусные аналитики на примере трояна Android.FakeApp.1669 рассказали о том, как злоумышленники используют DNS-протокол для скрытой связи вредоносных программ с управляющими серверами. Android.FakeApp.1669 является довольно примитивным трояном, задача которого сводится к загрузке заданных сайтов. От большинства похожих угроз он отличается тем, что адрес целевых сайтов он получает из TXT-записи вредоносного DNS-сервера, для чего использует модифицированный код открытой библиотеки dnsjava. При этом Android.FakeApp.1669 проявляет себя только при подключении к интернету через определенных провайдеров — в остальных случаях он работает как безобидное ПО.



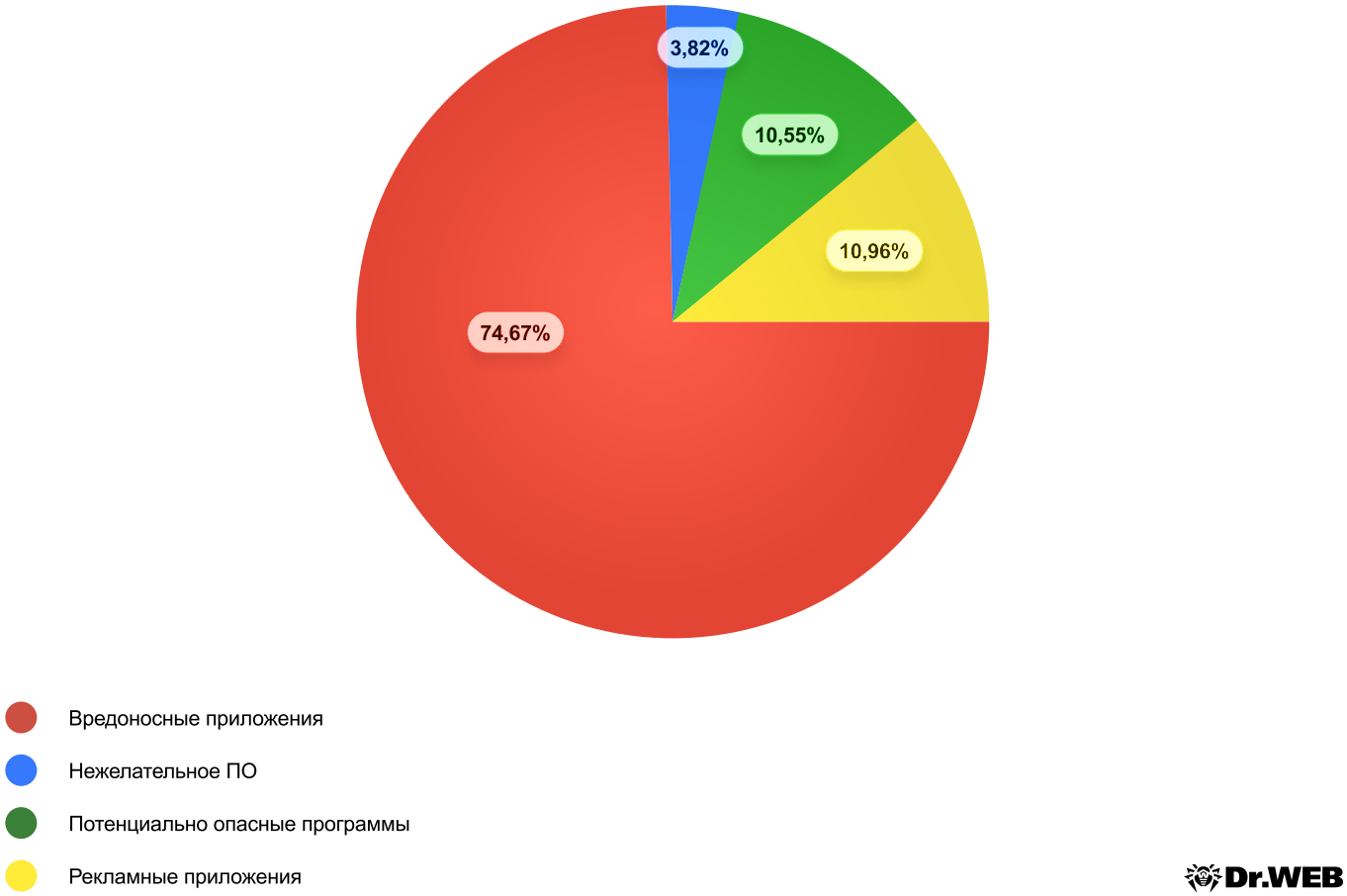
Пример TXT-записи целевого домена, которую DNS-сервер отдал при запросе через Linux-утилиту dig при анализе одной из модификаций Android.FakeApp.1669

Статистика

По данным статистики детектирований Dr.Web Security Space для мобильных устройств, в 2024 году наиболее распространенными угрозами стали вредоносные программы, на долю которых пришлось 74,67% всех случаев обнаружения. За ними расположились рекламные приложения с долей 10,96%. Третье место с показателем 10,55% заняли потенциально опасные программы. Четвертыми по распространенности стали нежелательные программы — пользователи сталкивались с ними в 3,82% случаев.

Распределение Android-угроз

по типу на основе данных статистики детектирований Dr.Web для мобильных устройств в 2024 году

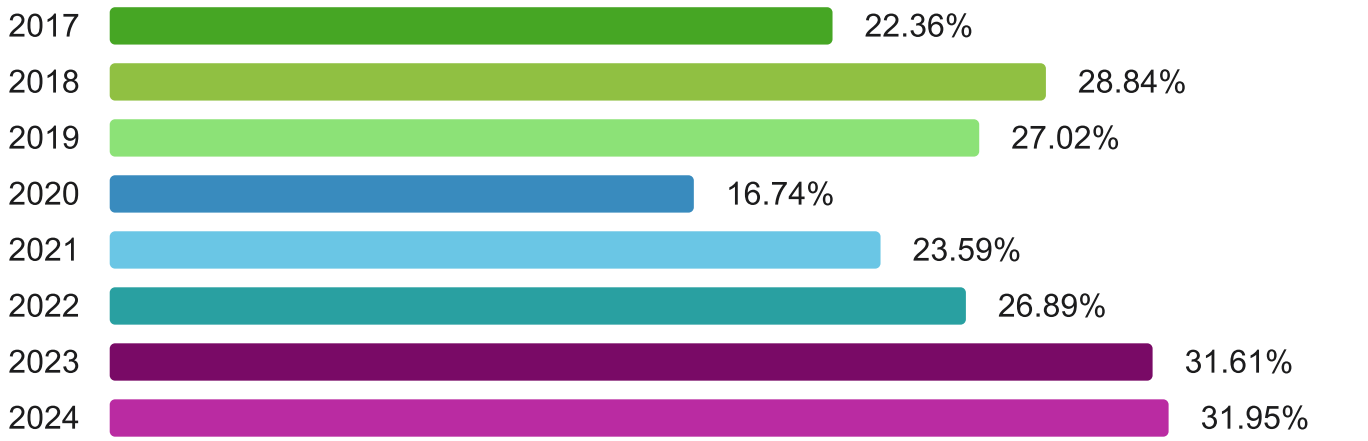


Вредоносные приложения

Самыми распространенными вредоносными программами для Android вновь стали рекламные трояны семейства Android.HiddenAds. За прошедший год их доля в общем объеме выявленных антивирусом Dr.Web вредоносных приложений увеличилась на 0,34 п. п. и составила 31,95% детектирований.

Доля рекламных троянов Android.HiddenAds

от общего числа вредоносных приложений, выявленных из защищаемых устройствах, r/r.



Среди представителей этого семейства наибольшую активность проявил Android.HiddenAds.3956 (15,10% детектирований семейства и 4,84% от общего числа детектирований вредоносного ПО). Это один из множества вариантов вредоносной программы Android.HiddenAds.1994, с которой пользователи сталкиваются на протяжении уже нескольких лет. Версия Android.HiddenAds.3956 наряду с другими модификациями появилась в 2023 году и по нашим прогнозам могла занять лидирующие позиции в семействе, что в итоге и произошло. В 2024 также получили распространение его новые варианты Android.HiddenAds.3980, Android.HiddenAds.3989, Android.HiddenAds.3994, Android.HiddenAds.655.origin, Android.HiddenAds.657.origin и ряд других.

При этом заметным также стало подсемейство троянов Android.HiddenAds.Aegis. В отличие от большинства других вредоносных программ Android.HiddenAds, представители этой группы обладают способностью автозапуска и некоторыми другими особенностями. Чаще всего на защищаемых антивирусом Dr.Web устройствах обнаруживались модификации Android.HiddenAds.Aegis.1, Android.HiddenAds.Aegis.4.origin, Android.HiddenAds.Aegis.7.origin и Android.HiddenAds.Aegis.1.origin.

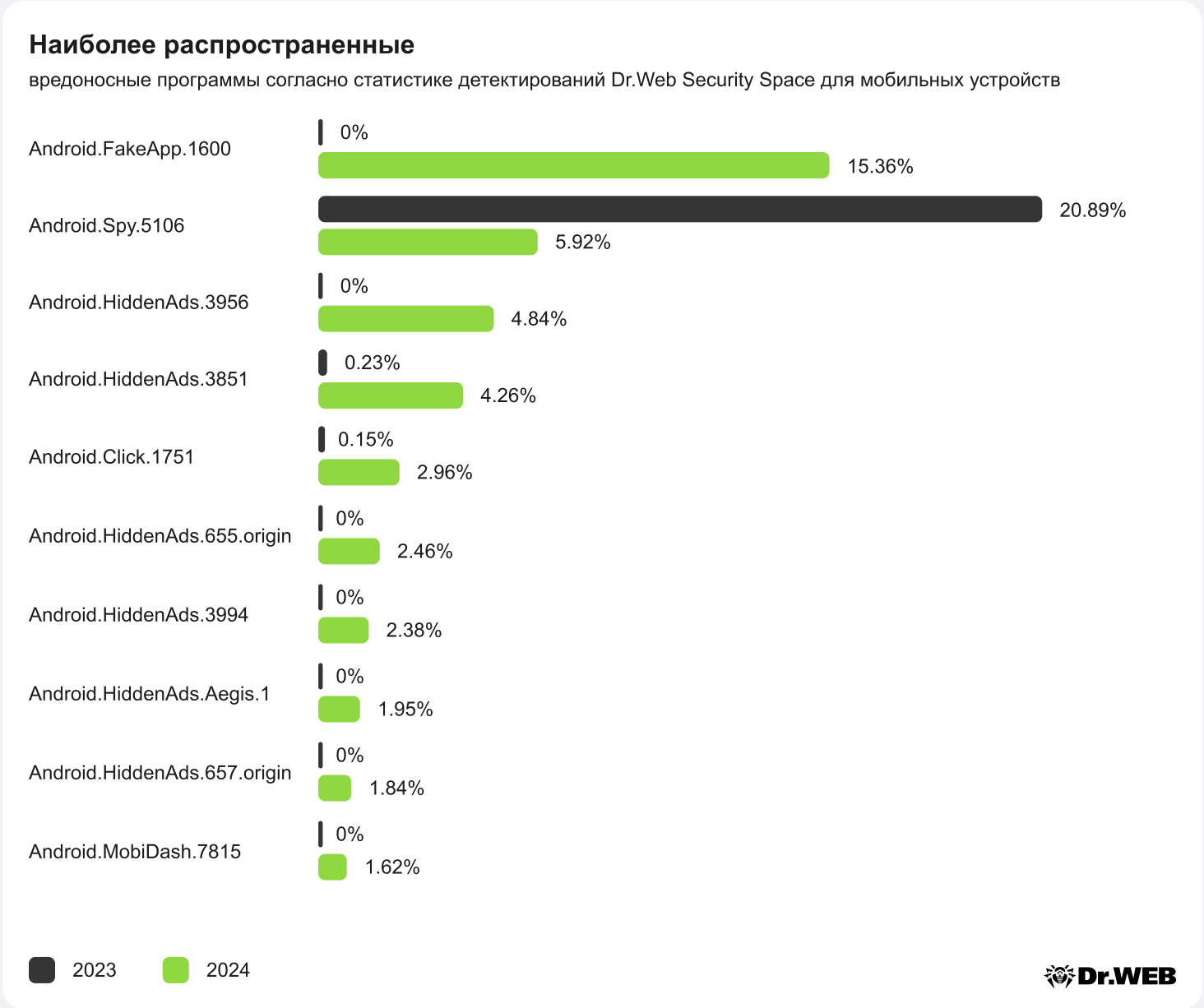
Вторыми наиболее распространенными вредоносными программами стали трояны семейства Android.FakeApp, которые злоумышленники применяют при реализации различных мошеннических схем. В минувшем году на них пришлось 18,28% всех детектирований вредоносного ПО, что на 16,45 п. п. больше, чем годом ранее. Чаще всего такие трояны загружают нежелательные сайты, предназначенные для фишинг-атак и онлайн-мошенничества.

На третьем месте с долей 11,52% (снижение на 16,7 п. п. по сравнению с 2023 годом) расположились трояны Android.Spy, которые обладают шпионской функциональностью. Как и годом ранее, самым распространенным представителем семейства стал Android.Spy.5106 — на него пришлось 5,95% детектирований вредоносных программ.

В 2024 году наблюдалась разнонаправленная тенденция в распространении вредоносного ПО, которое предназначено для загрузки и установки других программ и способно выполнять произвольный код. Так, по сравнению с годом ранее доля загрузчиков Android.DownLoader сократилась на 0,49 п. п. до 1,69%, доля троянов Android.Mobifun снизилась на 0,15 п. п. до 0,10%, а троянов Android.Xiny — на 0,14 п. п. до 0,13%.
При этом чаще детектировались трояны Android.Triada (2,74% случаев, рост на 0,6 п. п.) и Android.RemoteCode (3,78% случаев, рост на 0,95 п. п.).

Доля защищенных программными упаковщиками вредоносных приложений Android.Packed снизилась с 7,98% до 5,49%, практически вернувшись к показателю 2022 года. Также с 10,06% до 5,38% снизилось количество атак с участием рекламных троянов Android.MobiDash. В то же время несколько увеличилось число детектирований троянов-вымогателей Android.Locker (с 1,15% до 1,60%) и троянов Android.Proxy (с 0,57% до 0,81%). Последние позволяют использовать зараженные Android-устройства для перенаправления через них сетевого трафика злоумышленников. Кроме того, заметно возросла активность вредоносных программ Android.Click, способных открывать рекламные сайты и выполнять клики на веб-страницах (рост с 0,82% до 3,56%).

Десять наиболее часто детектируемых вредоносных приложений в 2024 году:



Android.FakeApp.1600

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

Android.Spy.5106

Детектирование одного из вариантов троянской программы, представляющей 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.HiddenAds.3956

Android.HiddenAds.3851

Android.HiddenAds.655.origin

Android.HiddenAds.3994

Android.HiddenAds.657.origin

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.

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.

Android.HiddenAds.Aegis.1

Троянская программа, которая скрывает свое присутствие на Android-устройствах и показывает надоедливую рекламу. Она относится к подсемейству, которое отличается от других представителей семейства Android.HiddenAds рядом признаков. Например, такие трояны способны самостоятельно запускаться после установки. Кроме того, в них реализован механизм, позволяющий их сервисам оставаться постоянно запущенными. В ряде случаев в них также могут быть задействованы скрытые функции ОС Android.

Android.MobiDash.7815

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

Нежелательное ПО

Самой часто детектируемой нежелательной программой в 2024 году стала Program.FakeMoney.11. На нее пришлось более половины — 52,10% — от общего числа выявленного на защищаемых устройствах нежелательного ПО. Она принадлежит к классу приложений, которые предлагают пользователям заработать на выполнении различных заданий, но в итоге не выплачивают никаких реальных вознаграждений.

Программы, которые антивирус Dr.Web детектирует как Program.CloudInject.1, расположились на втором месте с долей 19,21% (рост на 9,75 п. п. по сравнению с годом ранее). Такие приложения проходят модификацию через облачный сервис CloudInject — к ним добавляются опасные разрешения и обфусцированный код, назначение которого нельзя проконтролировать.

Приложения Program.FakeAntiVirus.1 второй год подряд снижают активность — они стали третьими по распространенности с показателем 10,07%, что на 9,35 п. п. меньше, чем в 2023. Эти программы имитируют работу антивирусов, обнаруживают несуществующие угрозы и предлагают владельцам Android-устройств купить полную версию для «исправления» якобы выявленных проблем.

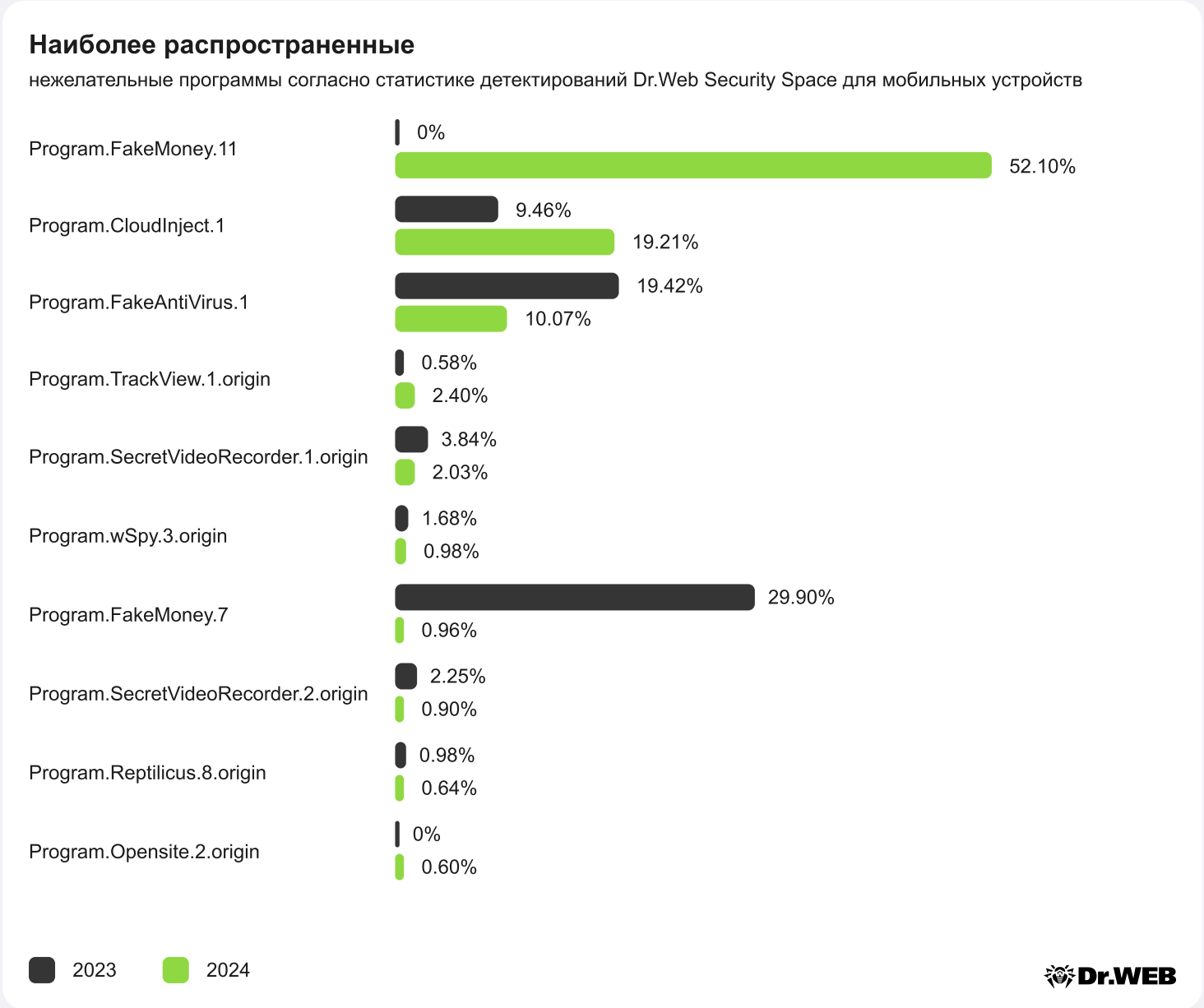
Первое место	Второе место	Третье место
Program.FakeMoney.11	Program.CloudInject.1	Program.FakeAntiVirus.1

В течение года пользователи сталкивались с различными программами для наблюдения и контроля активности. Такое ПО может использоваться для сбора данных как с согласия владельцев устройств, так и без их ведома — во втором случае они фактически превращаются в шпионские инструменты. Наиболее часто на защищаемых Dr.Web устройствах обнаруживались программы для мониторинга Program.TrackView.1.origin (2,40% случаев), Program.SecretVideoRecorder.1.origin (2,03% случаев), Program.wSpy.3.origin (0,98% случаев), Program.SecretVideoRecorder.2.origin (0,90% случаев), Program.Reptilicus.8.origin (0,64% случаев), Program.wSpy.1.origin (0,39% случаев) и Program.MonitorMinor.11 (0,38% случаев).

Кроме того, распространение получили Android-программы Program.Opensite.2.origin, задачей которых является загрузка заданных сайтов и демонстрация рекламы. Их доля составила 0,60% детектирований нежелательного ПО.

Доля защищенных программными упаковщиками вредоносных приложений Android.Packed снизилась с 7,98% до 5,49%, практически вернувшись к показателю 2022 года. Также с 10,06% до 5,38% снизилось количество атак с участием рекламных троянов Android.MobiDash. В то же время несколько увеличилось число детектирований троянов-вымогателей Android.Locker (с 1,15% до 1,60%) и троянов Android.Proxy (с 0,57% до 0,81%). Последние позволяют использовать зараженные Android-устройства для перенаправления через них сетевого трафика злоумышленников. Кроме того, заметно возросла активность вредоносных программ Android.Click, способных открывать рекламные сайты и выполнять клики на веб-страницах (рост с 0,82% до 3,56%).

Десять наиболее часто детектируемых нежелательных приложений в 2024 году:



Program.FakeMoney.11

Program.FakeMoney.7

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 им 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

Program.SecretVideoRecorder.2.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.

Program.wSpy.3.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.

Program.Reptilicus.8.origin

Приложение, позволяющее следить за владельцами Android-устройств. Оно способно контролировать местоположение устройства, собирать данные об СМС-переписке и беседах в социальных сетях, прослушивать телефонные звонки и окружение, создавать снимки экрана, отслеживать вводимую на клавиатуре информацию, копировать файлы с устройства и выполнять другие действия.

Program.Opensite.2.origin

Детектирование однотипных Android-программ, задачей которых является загрузка заданных сайтов и демонстрация рекламы. Такие приложения часто маскируются под другое ПО. Например, существуют модификации, которые распространяются под видом видеоплеера YouTube. Они загружают настоящий сайт сервиса и отображают рекламные баннеры с помощью подключенных рекламных SDK.

Потенциально опасные программы

Утилиты Tool.SilentInstaller, которые позволяют запускать Android-приложения без их установки, в минувшем году сохранили лидирующие позиции по числу детектирований потенциально опасного ПО. Суммарно на них пришлось более трети всех выявленных программ этого типа.

Чаще всего на устройствах встречались модификации:

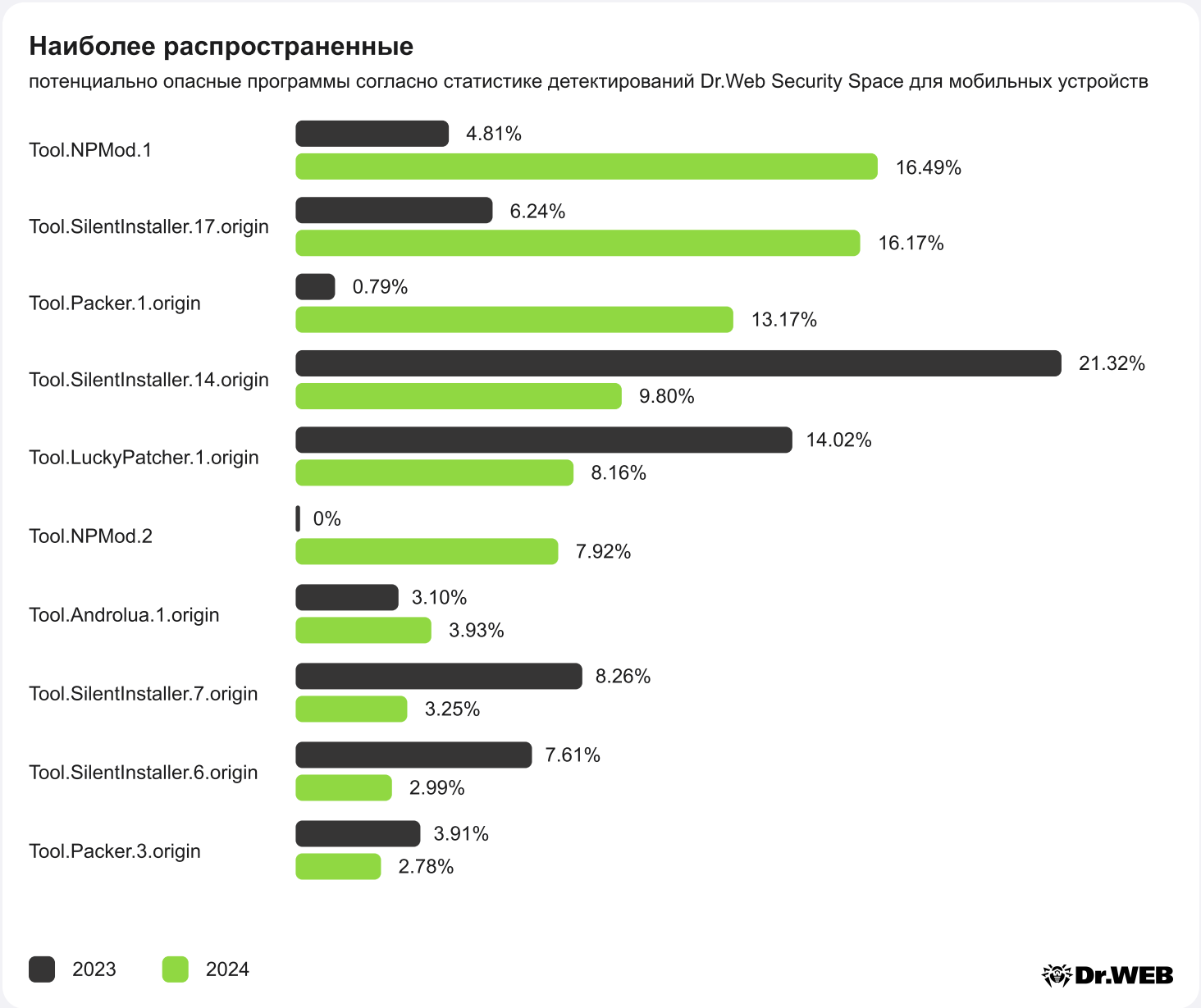
Tool.SilentInstaller.17.origin	16,17%
Tool.SilentInstaller.14.origin	9,80%
Tool.SilentInstaller.7.origin	3,25%
Tool.SilentInstaller.6.origin	2,99%

Другими распространенными потенциально опасными программами стали приложения, модифицированные при помощи утилиты NP Manager. Эта утилита встраивает в целевое ПО специальный модуль, который позволяет обходить проверку цифровой подписи после выполненной модификации. Антивирус Dr.Web детектирует такие программы как различные варианты семейства Tool.NPMod. Среди них наиболее часто выявлялись вариации Tool.NPMod.1. За год они значительно укрепили свои позиции: на их долю пришлось 16,49% детектирований потенциально опасных приложений, что на 11,68 п. п. большое, чем в 2023. При этом доля модифицированного утилитой NP Manager ПО, которое детектируется другой вирусной записью — Tool.NPMod.2, — составила 7,92%. В результате суммарно представители этого семейства были ответственны почти за четверть всех детектирований потенциально опасных программ.

Среди лидеров также оказались приложения, защищенные упаковщиком Tool.Packer.1.origin — они обнаруживались в 13,17% случаев, что на 12,38 п. п. больше по сравнению с годом ранее. Кроме того, с 3,10% до 3,93% возросло количество детектирований Tool.Androlua.1.origin. Это фреймворк, позволяющий модифицировать установленные Android-программы и исполнять Lua-скрипты, которые потенциально могут быть вредоносными.

Вместе с тем активность одного из лидеров 2023 года, семейства утилит Tool.LuckyPatcher, наоборот, несколько снизилась — с 14,02% до 8,16%. Эти утилиты позволяют модифицировать Android-программы с добавлением в них загружаемых из интернета скриптов. Реже встречались и программы, защищенные утилитой-обфускатором Tool.Obfuscapk (снижение с 3,22% до 1,05%), а также упаковщиком Tool.ApkProtector (снижение с 10,14% до 3,39%).

Десять наиболее распространенных потенциально опасных приложений, обнаруженных на Android-устройствах в 2024 году:



Tool.NPMod.1

Tool.NPMod.2

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

Tool.SilentInstaller.14.origin

Tool.SilentInstaller.7.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.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.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.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.3.origin

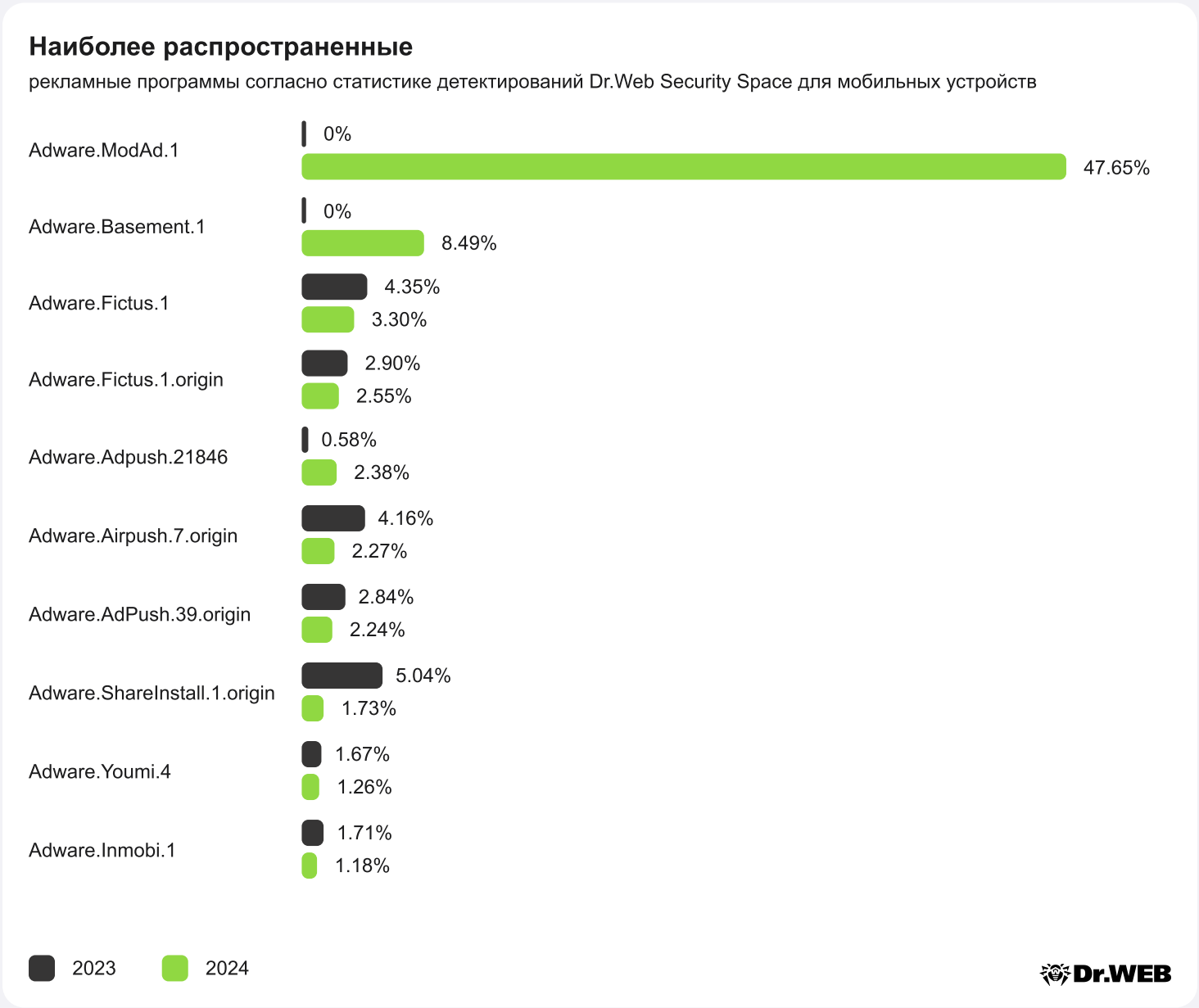
Детектирование Android-программ, код которых зашифрован и обфусцирован утилитой NP Manager.

Рекламные приложения

Наиболее распространенным рекламным ПО в 2024 году стало новое семейство программ Adware.ModAd — на него пришлось 47,45% детектирований. Лидеры предыдущего года, представители семейства Adware.Adpush, оказались на втором месте с долей 14,76% (снижение числа детектирований на 21,06 п. п.). На третьем месте с показателем 8,68% расположилось еще одного новое семейство рекламных приложений Adware.Basement.

Распространение также получили семейства Adware.Airpush (доля снизилась с 8,59% до 4,35%), Adware.Fictus (снижение с 4,41% до 3,29%), Adware.Leadbolt (снижение с 4,37% до 2,26%), Adware.ShareInstall (снижение с 5,04% до 1,71%). Занимавшие в 2023 году второе место рекламные программы Adware.MagicPush значительно снизили активность и не попали в первую десятку, переместившись сразу на одиннадцатую позицию с показателем 1,19% (снижение на 8,39 п. п.).

Десять наиболее распространенных рекламных приложений, обнаруженных на Android-устройствах в 2024 году:



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.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

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.21846

Adware.AdPush.39.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.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.ShareInstall.1.origin

Рекламный модуль, который может быть интегрирован в Android-программы. Он демонстрирует рекламные уведомления на экране блокировки ОС Android.

Adware.Youmi.4

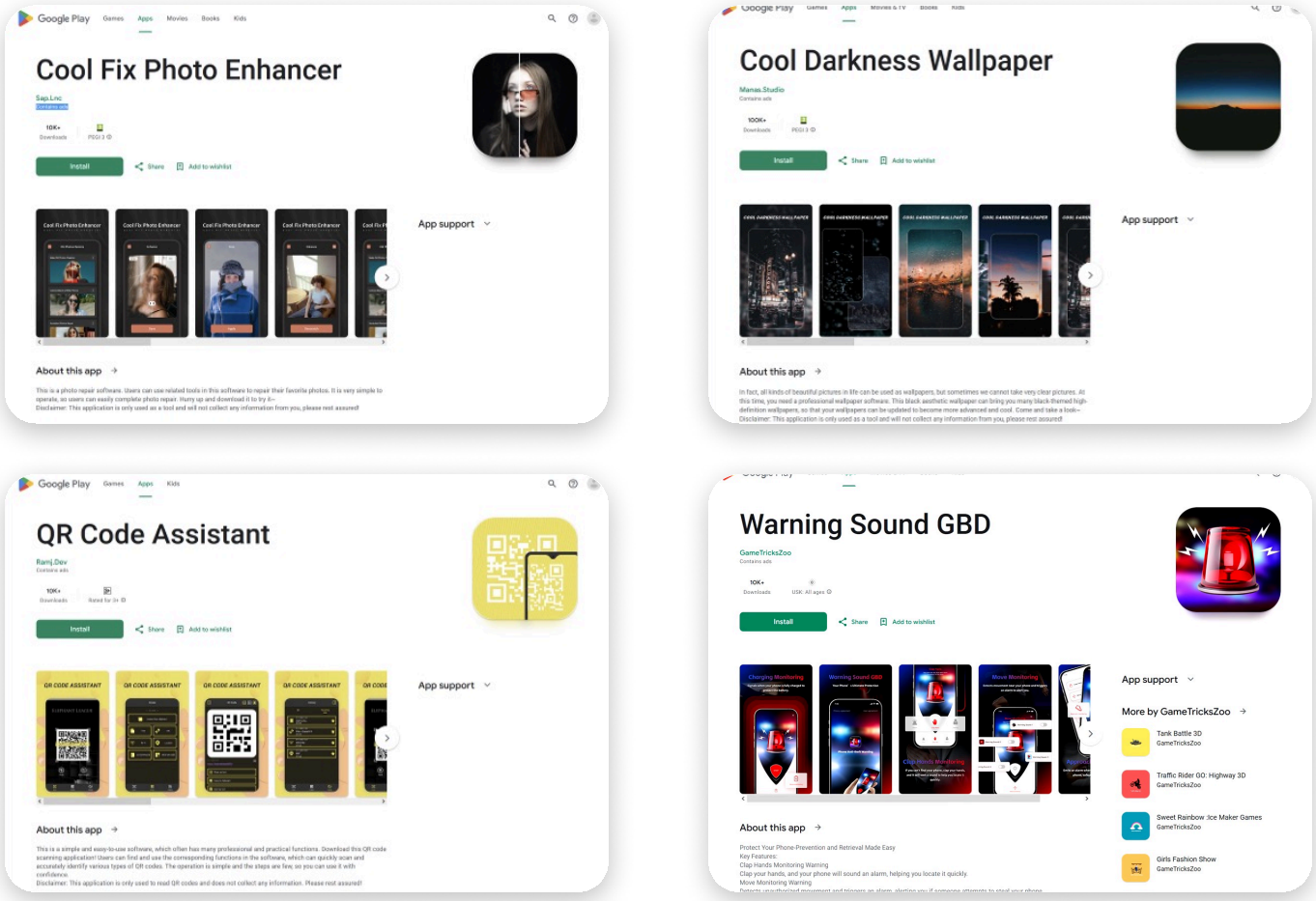
Детектирование нежелательного рекламного модуля, который размещает рекламные ярлыки на главном экране Android-устройств.

Adware.Inmobi.1

Детектирование некоторых версий рекламного SDK Inmobi, способных совершать телефонные звонки и добавлять события в календарь Android-устройств.

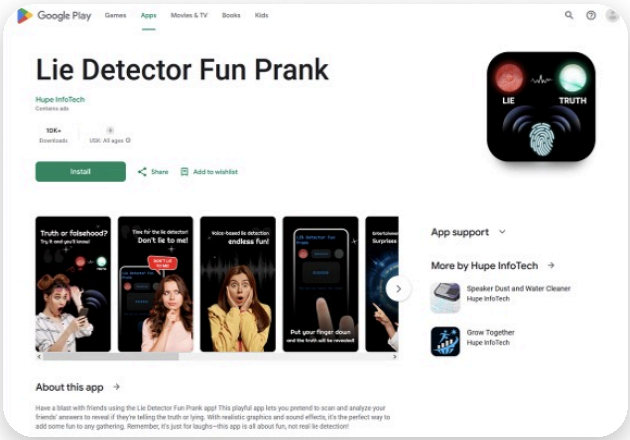
Угрозы в Google Play

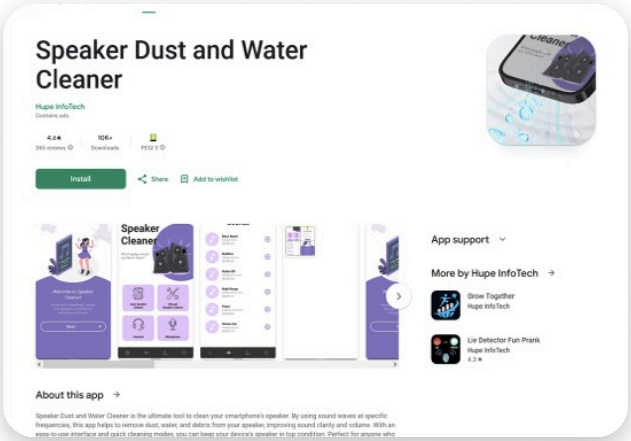
В 2024 году вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play свыше 200 угроз с более чем 26 700 000 суммарных загрузок. Помимо трояна Android.Click.414.origin среди них было множество других — например, рекламные трояны Android.HiddenAds. Они распространялись под видом самого разнообразного ПО: фоторедакторов, сканеров штрих-кодов, сборников картинок и даже «противоугонной» сигнализации для защиты смартфона от чужих рук. Такие трояны скрывают свои значки после установки и начинают показывать агрессивную рекламу, которая перекрывает интерфейс системы и других программ и мешает нормально пользоваться устройством.



Примеры рекламных троянов, обнаруженных в Google Play в 2024 году.
Android.HiddenAds.4013 скрывался в фоторедакторе Cool Fix Photo Enhancer,
Android.HiddenAds.4034 — в сборнике изображений Cool Darkness Wallpaper,
Android.HiddenAds.4025 — в программе для распознавания штрих-кодов QR Code Assistant,
Android.HiddenAds.656.origin — в программе-сигнализации Warning Sound GBD

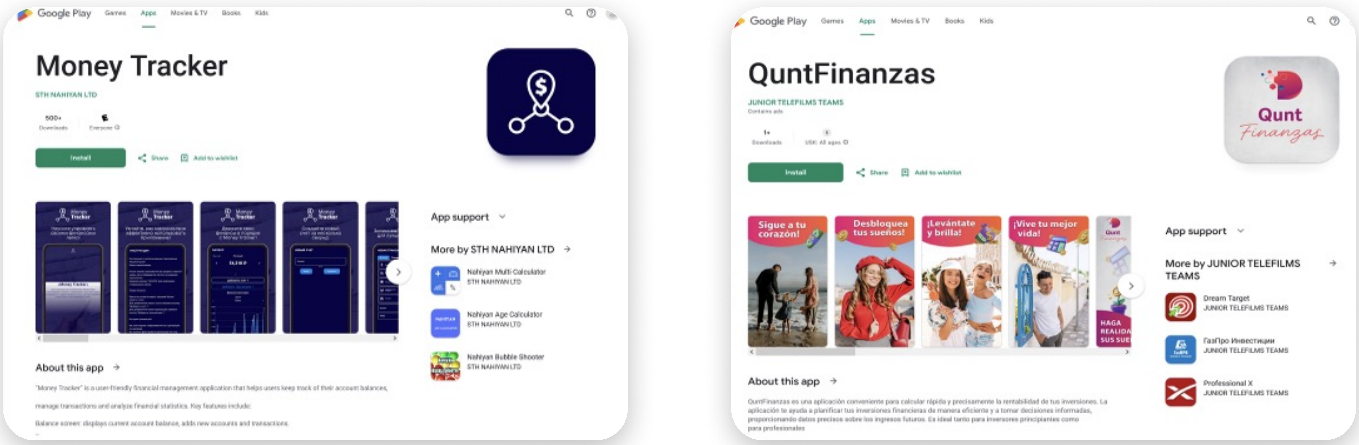
Наши специалисты также выявили различные троянские программы, которые злоумышленники защитили сложным программным упаковщиком.





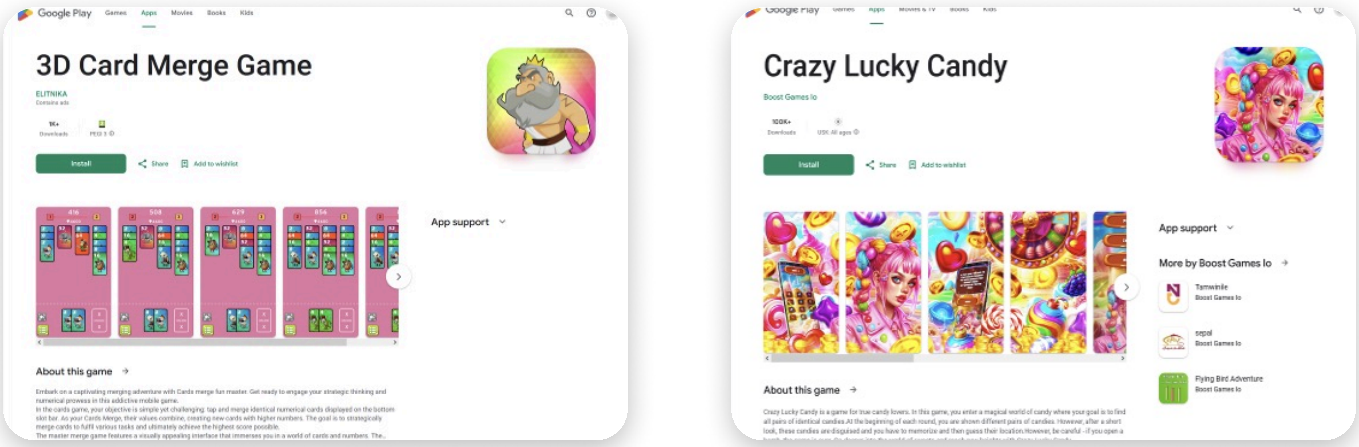
В приложении Lie Detector Fun Prank скрывался троян Android.Packed.57156, а в программе Speaker Dust and Water Cleaner — троян Android.Packed.57159, защищенные упаковщиком

Другими найденными вредоносными программами стали представители семейства Android.FakeApp, которые используются в различных мошеннических схемах. Основная задача большинства таких троянов — открыть заданную ссылку, при этом при определенных условиях они также могут работать и как заявленное ПО. Многие из них распространялись под видом различных финансовых программ (например, справочников и обучающих пособий, калькуляторов доходности, приложений для доступа к биржевой торговле, инструментов для ведения домашней бухгалтерии), записных книжек, дневников, программ для участия в викторинах и опросах и прочих. Они загружали мошеннические сайты инвестиционной тематики.



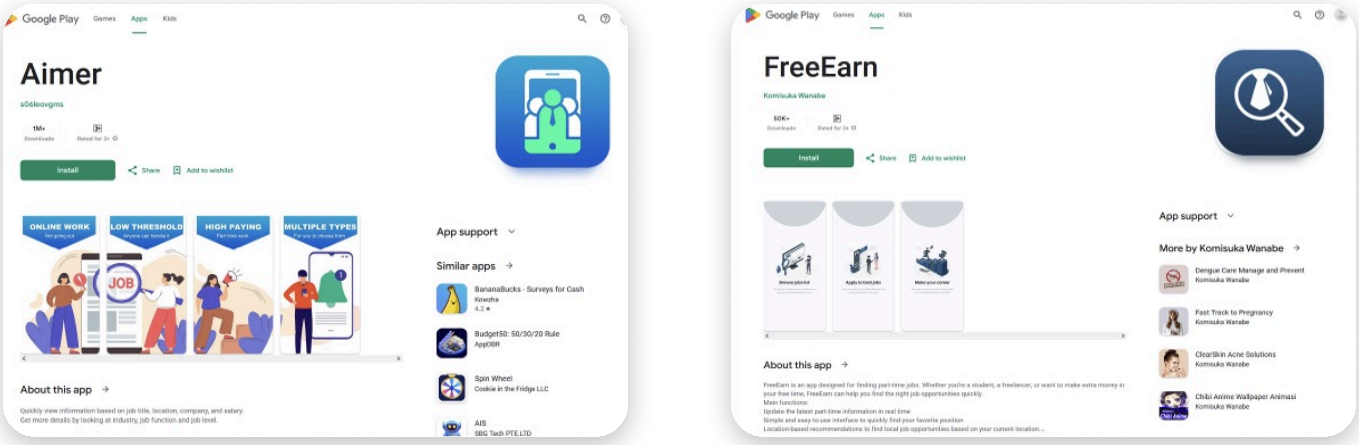
Примеры троянов Android.FakeApp, которые загружали ссылки на мошеннические сайты: Android.FakeApp.1681 (SenseStrategy), Android.FakeApp.1708 (QuntFinanzas)

Часть программ-подделок Android.FakeApp распространялись под видом всевозможных игр. Многие из них также могли предоставлять заявленную функциональность, но их главной задачей была загрузка сайтов онлайн-казино и букмекеров.



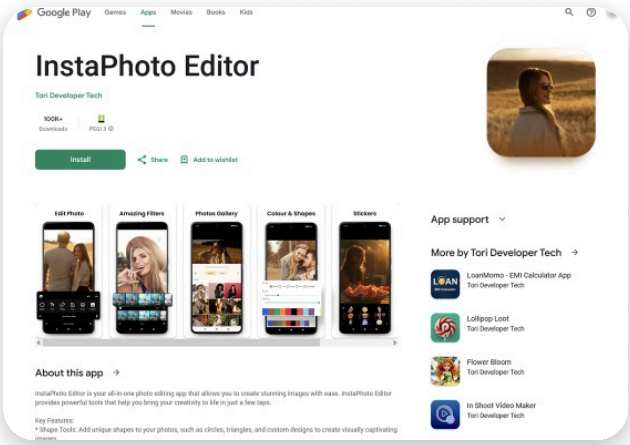
Примеры выдаваемых за игры троянов Android.FakeApp, которые загружали ссылки на сайты букмекеров и онлайн-казино: Android.FakeApp.1622 (3D Card Merge Game), Android.FakeApp.1630 (Crazy Lucky Candy)

Некоторые трояны этого семейства были вновь замаскированы под приложения для поиска работы. Такие программы-подделки загружают поддельные списки вакансий и предлагают пользователям составить «резюме», предоставив персональные данные. В других случаях трояны могут предложить потенциальным жертвам связаться с «работодателем» через мессенджер. На самом деле потенциальные жертвы напишут преступникам, которые попытаются заманить их в ту или иную мошенническую схему.



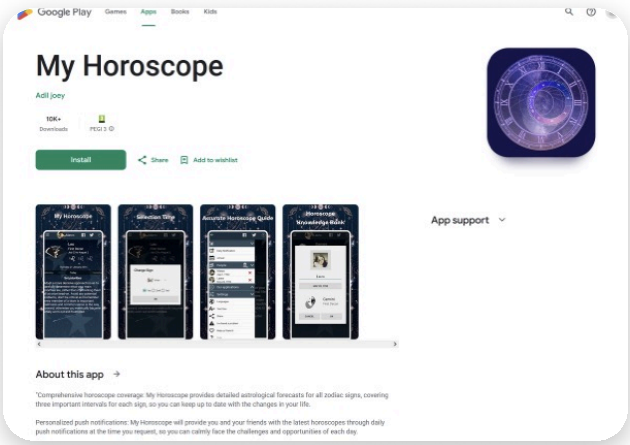
Примеры троянов Android.FakeApp, которые мошенники выдавали за программы для поиска работы: Android.FakeApp.1627 (Aimer), Android.FakeApp.1703 (FreeEarn)

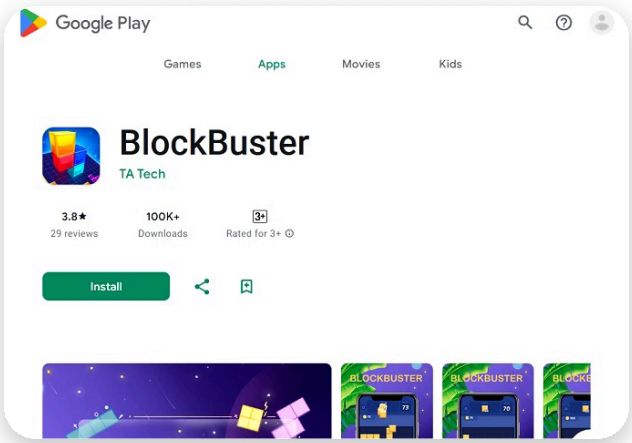
Кроме того, в Google Play были обнаружены очередные троянские приложения, подписывающие пользователей на платные услуги. Одним из них был Android.Subscription.22 — он распространялся под видом фоторедактора InstaPhoto Editor.



Троян Android.Subscription.22, предназначенный для подписки пользователей на платные услуги

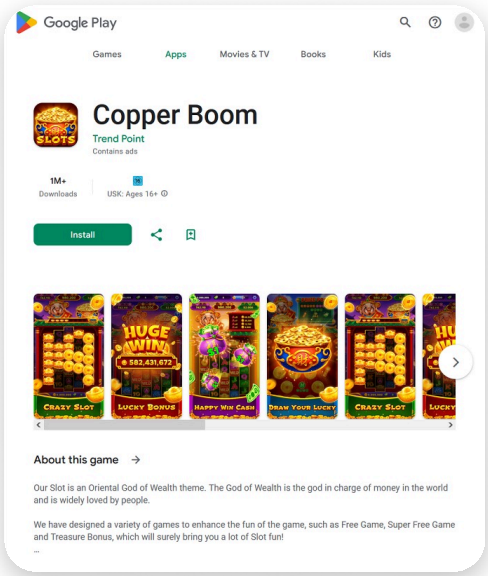
Другими такими троянами были представители родственных семейств Android.Joker и Android.Harly, имеющих модульную архитектуру. Первые способны скачивать вспомогательные компоненты из интернета, а вторые отличаются тем, что обычно хранят необходимые модули в зашифрованном виде среде своих ресурсов.

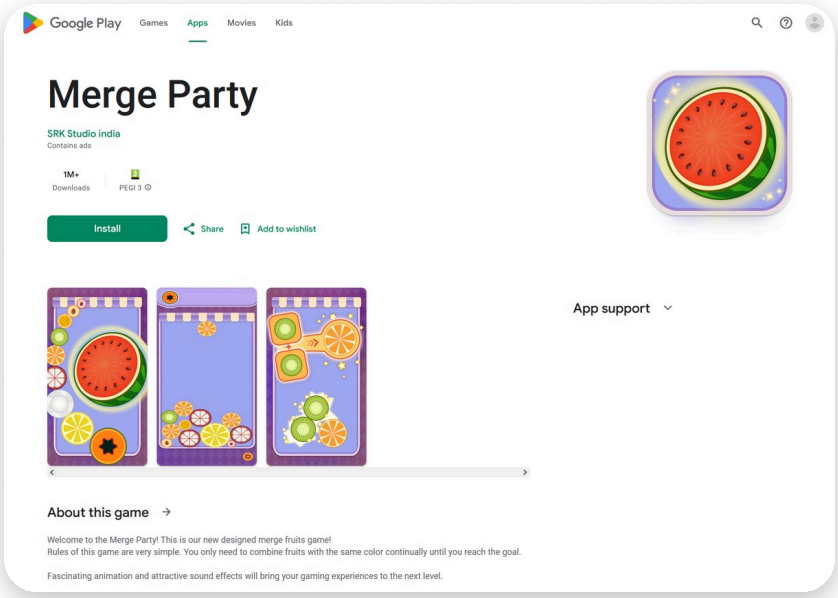




Примеры программ, которые подписывали жертв на платные услуги. Android.Joker.2280 скрывался в приложении с гороскопами My Horoscope, а Android.Harly.87 — в игре BlockBuster

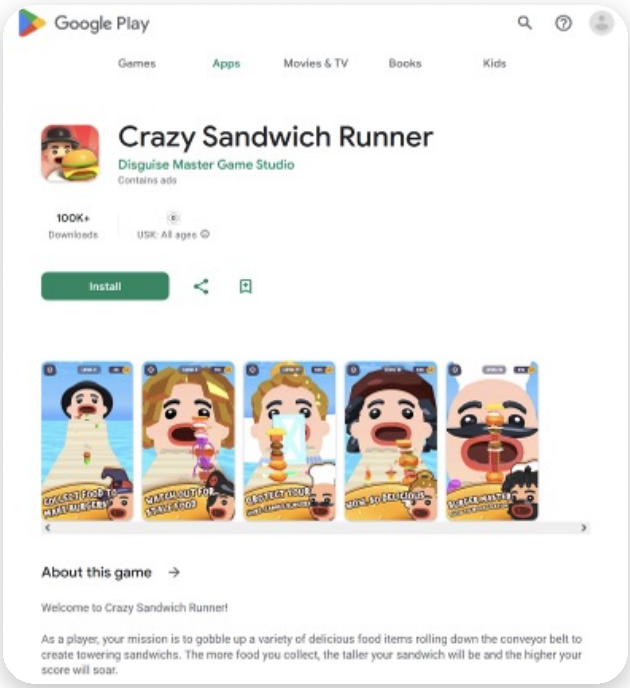
Помимо вредоносных программ специалисты «Доктор Веб» обнаружили в Google Play новое нежелательное ПО, среди которого были различные модификации Program.FakeMoney.11 и Program.FakeMoney.14. Эти программы относятся к семейству приложений, которые предлагают пользователям за виртуальные вознаграждения выполнять различные задания (зачастую просматривать рекламу). Вознаграждения в дальнейшем якобы можно конвертировать в настоящие деньги или призы, но для вывода «заработанного» от пользователя требуется накопить определенную сумму. Однако даже в случае успеха реальных выплат он в итоге не получает.

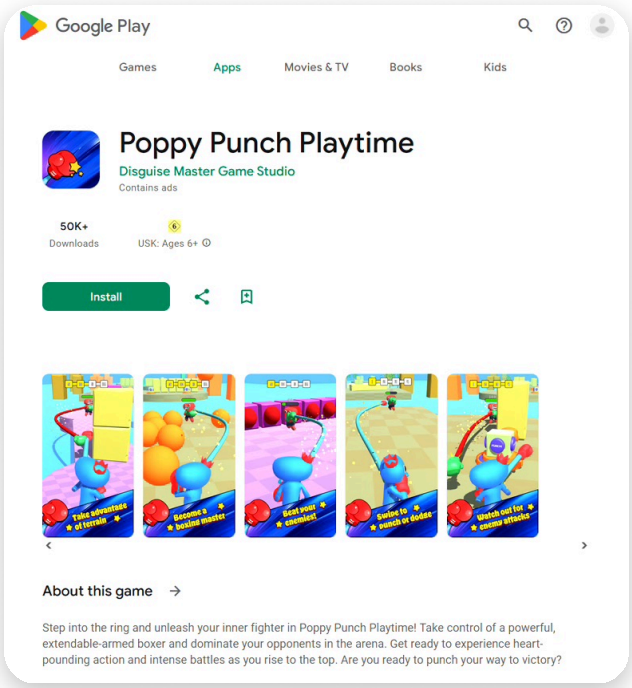


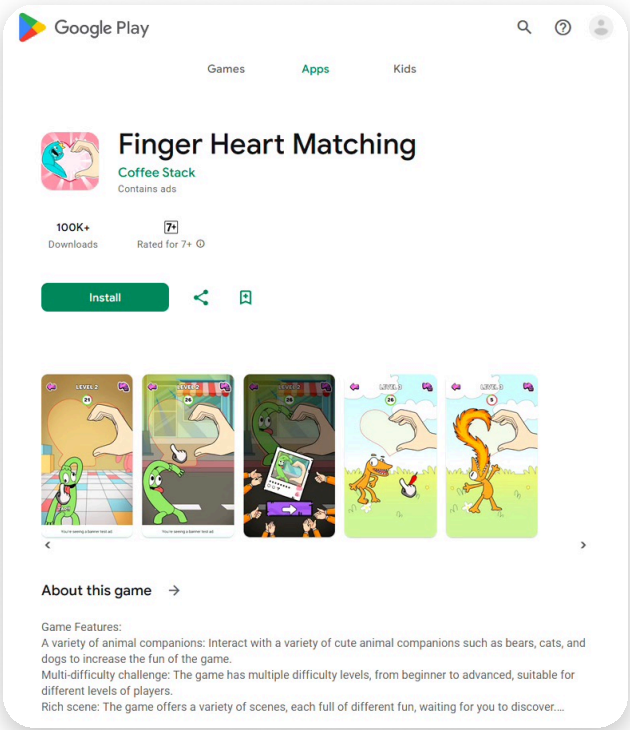


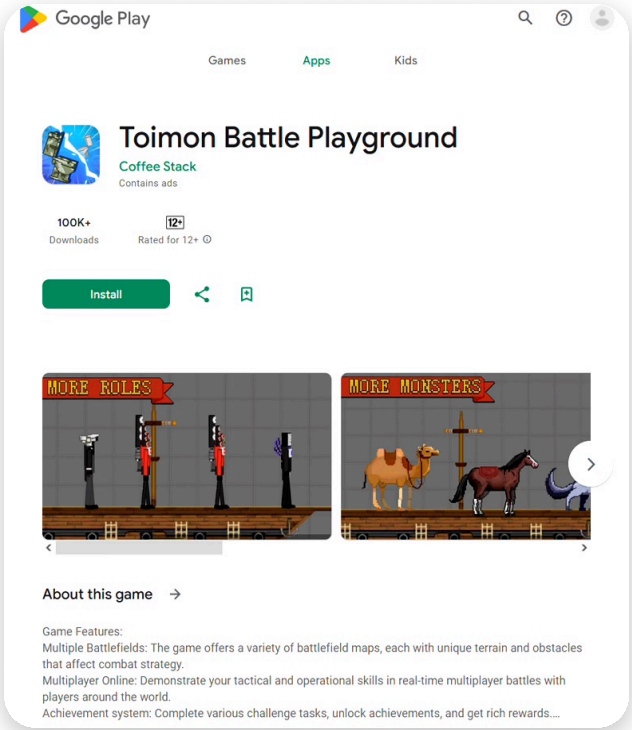
Один из вариантов Program.FakeMoney.11 распространялся в виде игры Copper Boom, а Program.FakeMoney.14 был представлен игрой Merge Party

Кроме того, в течение года в Google Play наши вирусные аналитики выявляли новые рекламные программы. В их числе были приложения и игры со встроенным рекламным модулем Adware.StrawAd, способным демонстрировать объявления от различных поставщиков услуг.



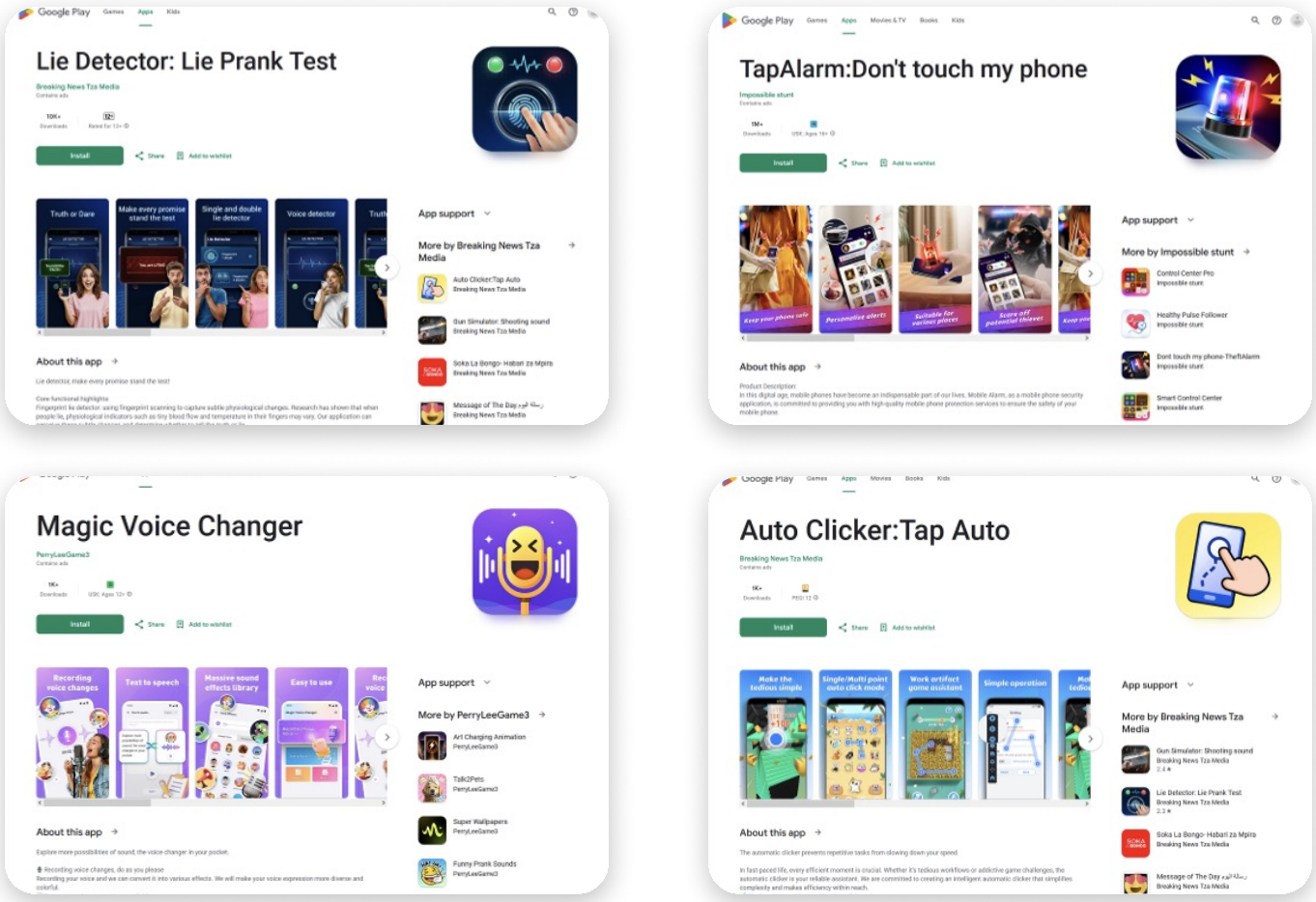






Примеры игр с рекламным модулем Adware.StrawAd: Crazy Sandwich Runner (Adware.StrawAd.1), Poppy Punch Playtime (Adware.StrawAd.3), Finger Heart Matching (Adware.StrawAd.6), Toimon Battle Playground (Adware.StrawAd.9)

В Google Play также распространялись рекламные приложения Adware.Basement, объявления от которых часто ведут на вредоносные и мошеннические сайты. Примечательно, что это семейство имеет общую кодовую базу с нежелательными программами Program.FakeMoney.11.



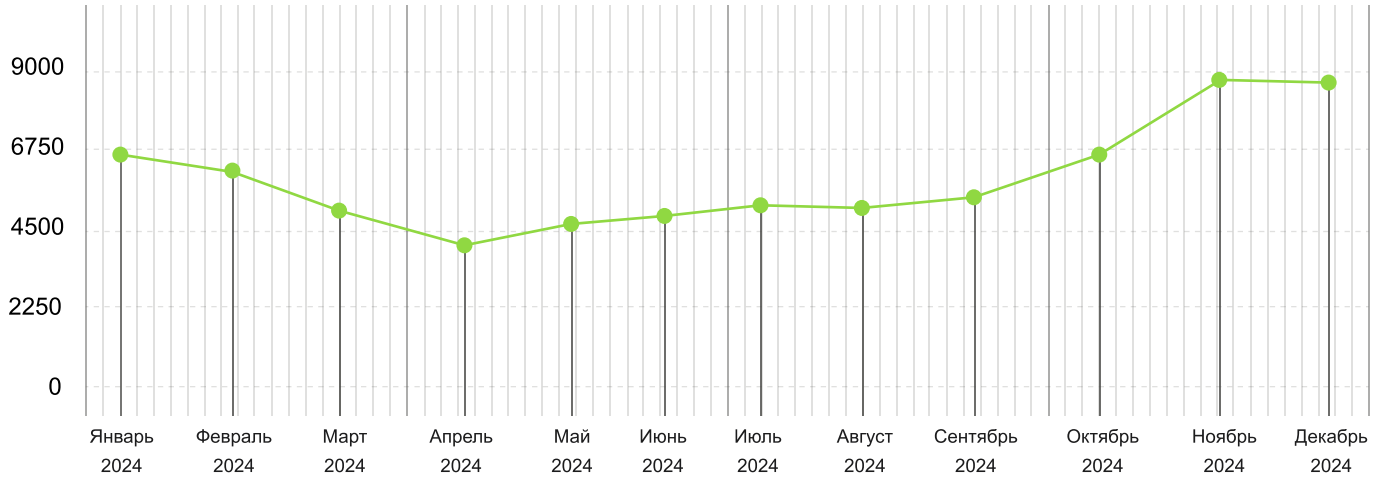
Примеры нежелательных рекламных программ Adware.Basement: Lie Detector: Lie Prank Test, TapAlarm:Don't touch my phone и Magic Voice Changer — Adware.Basement.1, Auto Clicker:Tap Auto — Adware.Basement.2

Банковские трояны

По данным статистики детектирований Dr.Web Security Space для мобильных устройств в 2024 году доля банковских троянов от общего числа зафиксированных вредоносных программ составила 6,29%, что на 2,71 п. п. больше, чем годом ранее. С января их активность планомерно снижалась, но с середины весны количество атак вновь стало расти. В течение III квартала их активность оставалась практически неизменной, после чего продолжила увеличиваться, достигнув годового максимума в ноябре.

Динамика обнаружения

банковских троянских приложений на Android-устройствах в 2024 году

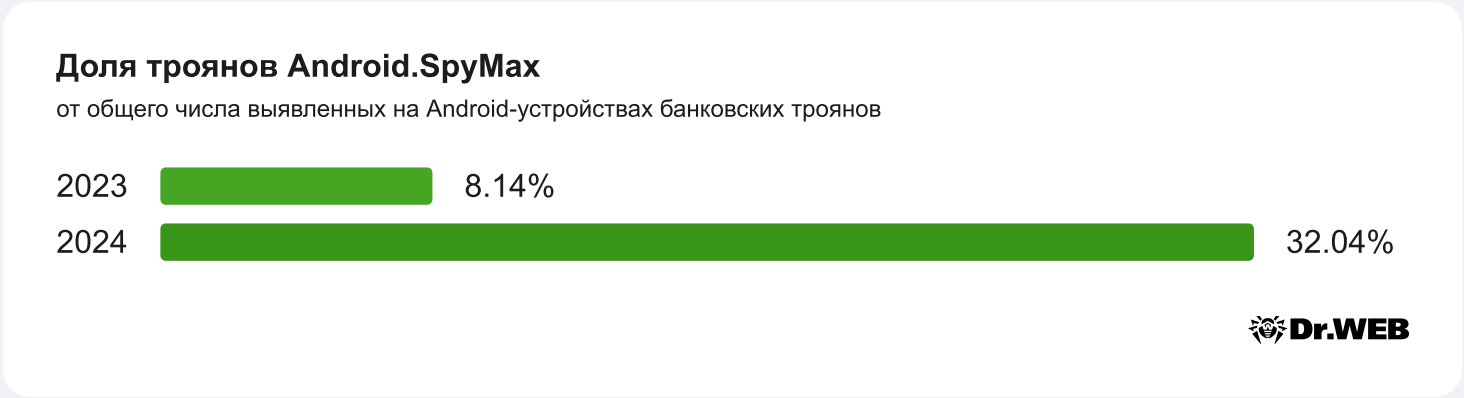


В 2024 году широкое распространение вновь получили известные семейства банковских троянов. Среди них — вредоносные программы Coper, Hydra (Android.BankBot.1048.origin, Android.BankBot.563.origin), Ermac (Android.BankBot.1015.origin, Android.BankBot.15017), Alien (Android.BankBot.745.origin, Android.BankBot.1078.origin), Anubis (Android.BankBot.670.origin).
Кроме того, наблюдались атаки с использованием семейств Cerberus (Android.BankBot.11404), GodFather (Android.BankBot.GodFather.3, Android.BankBot.GodFather.14.origin) и Zanubis (Android.BankBot.Zanubis.7.origin).

В течение года злоумышленники активно распространяли троянов-шпионов Android.SpyMax, которые обладают широким набором вредоносных функций, в том числе возможностью удаленно управлять зараженными устройствами. Они широко применяются и в качестве банковских троянов. Это семейство изначально включало многофункционального RAT-трояна SpyNote (RAT — Remote Administration Trojan, троян удаленного доступа). Однако после утечки его исходного кода на его основе стали появляться всевозможные модификации — например, CraxsRAT и G700 RAT. Статистика детектирований Dr.Web Security Space для мобильных устройств показывает, что представители этого семейства активизировались во второй половине 2023 года, и с тех пор число их детектирований продолжало расти практически каждый месяц. Данная тенденция пока сохраняется.

Трояны Android.SpyMax нацелены на пользователей по всему миру. В минувшем году они были замечены в том числе в многочисленных атаках на российских пользователей — 46,23% детектирований семейства пришлось именно на данную аудиторию. Также эти вредоносные программы наиболее активно распространялись среди бразильских (35,46% детектирований) и турецких (5,80% детектирований) владельцев Android-устройств.

Примечательно, что распространение этих вредоносных программ в России в основном происходит не при помощи спама или классических вариантов фишинга, а в ходе одного из этапов телефонного мошенничества. Вначале звонящие потенциальной жертве злоумышленники традиционно пытаются убедить ее в том, что являются сотрудниками банка или правоохранительных органов. Они информируют о якобы возникшей проблеме — попытке кражи денег с банковского счета или незапланированном оформлении кредита, либо, наоборот, сообщают «хорошие новости» о якобы полагающихся выплатах от государства. Когда мошенники понимают, что пользователь им поверил, они побуждают его установить «обновление антивируса», «банковское приложение» или иную программу — например, для «обеспечения безопасной транзакции». В такой программе на самом деле скрывается троян Android.SpyMax.



Пользователи из России в 2024 году также сталкивались с семействами банкеров Falcon (Android.BankBot.988.origin, Android.Banker.5703) и Mamont (Android.Banker.637.origin, Android.Banker.712.origin). Кроме того, были отмечены атаки банковских троянов Android.Banker.791.origin и Android.Banker.829.origin на владельцев Android-устройств из России и Узбекистана, а также банкера Android.Banker.802.origin на пользователей России, Азербайджана и Узбекистана. Целью трояна Android.Banker.757.origin были пользователи из России, Узбекистана, Таджикистана и Казахстана.

Наши специалисты вновь фиксировали атаки троянов MoqHao (Android.Banker.367.origin, Android.Banker.430.origin, Android.Banker.470.origin, Android.Banker.593.origin), нацеленных на пользователей из многих стран, включая государства Юго-Восточной Азии и Азиатско-Тихоокеанского региона. На эту же аудиторию были направлены атаки и других троянов. Например, южнокорейские владельцы Android-устройств сталкивались с семействами Fakecalls (Android.BankBot.919.origin, Android.BankBot.14423, Android.Banker.5297), IOBot (Android.BankBot.IOBot.1.origin) и Wroba (Android.Banker.360.origin). Прочие модификации Wroba (Android.BankBot.907.origin, Android.BankBot.1128.origin) атаковали пользователей из Японии.

Жителям Китая в числе прочих угрожал троян Android.Banker.480.origin, а вьетнамским пользователям — Android.BankBot.1111.origin. В то же время злоумышленники применяли троянов TgToxic (Android.BankBot.TgToxic.1) для атак на клиентов кредитных организаций Индонезии, Таиланда и Тайваня, а трояна GoldDigger (Android.BankBot.GoldDigger.3) — на пользователей из Таиланда и Вьетнама.

Вновь были зафиксированы атаки на иранских пользователей — те сталкивались с такими банкерами как Android.Banker.709.origin, Android.Banker.5292, Android.Banker.777.origin, Android.BankBot.1106.origin и рядом других. А в атаках на турецких клиентов банков наряду с другими троянами были также отмечены представители семейства Tambir (Android.BankBot.1104.origin, Android.BankBot.1099.origin, Android.BankBot.1117.origin).

Среди индийских владельцев Android-устройств распространение получили банкеры Android.Banker.797.origin, Android.Banker.817.origin и Android.Banker.5435 — они маскировались под ПО, якобы имеющее отношение к кредитным организациям Airtel Payments Bank, PM KISAN и IndusInd Bank. Кроме того, сохранилась активность банковских троянов Rewardsteal (Android.Banker.719.origin, Android.Banker.5147, Android.Banker.5443) основной целю которых являются индийские клиенты банков Axis bank, HDFC Bank, SBI, ICICI Bank, RBL bank и Citi bank.

В странах Латинской Америки вновь была отмечена активность троянов PixPirate (Android.BankBot.1026.origin), которые атакуют клиентов бразильских банков.

На европейскиих пользователей, в частности, были нацелены трояны Anatsa (Android.BankBot.Anatsa.1.origin) и Copybara (Android.BankBot.15140, Android.BankBot.1100.origin). Последние преимущественно атакуют жителей Италии, Великобритании и Испании.

В течение 2024 года вирусные аналитики «Доктор Веб» фиксировали рост популярности некоторых методов защиты вредоносных Android-программ — преимущественно банковских троянов — от анализа и детектирования. В частности, злоумышленники выполняли различные манипуляции с форматом ZIP — основой APK-файлов. В результате многие инструменты статического анализа, которые применяют стандартные алгоритмы работы с ZIP-архивами, оказываются неспособны корректно обработать такие «поврежденные» файлы.
В то же время трояны воспринимаются операционной системой Android как обычные программы, корректно устанавливаются и работают.

Одной из распространенных техник стала манипуляция с полями `compression method` и `compressed size` в структуре заголовка локального файла внутри APK. Злоумышленники намеренно указывают неверные значения полей `compressed size` и `uncompressed size` (сжатый размер и размер без сжатия), либо записывают некорректный или несуществующий метод сжатия в поле `compression method`. В другом варианте для архива может быть указан метод без сжатия, при этом поля заголовков `compressed size` и `uncompressed size` не будут совпадать, хотя должны.

Другой популярный метод — использование некорректных данных о диске в записи ECDR (End of Central Directory Record, конец записи центрального каталога) и CD (Central Directory, заголовок файла центрального каталога — здесь находятся данные о файлах и параметрах архива). Оба эти параметра для цельного архива должны совпадать, но киберпреступники могут указывать для них различные значения, как будто это не цельный, а мультиархив.

Распространенной также была техника, когда в заголовках локальных файлов некоторых файлов в архиве указывается флаг, означающий, что эти файлы зашифрованы. В действительности они не зашифрованы, но из-за этого архив при анализе считывается некорректно.

Вместе с манипуляцией структурой APK-файлов вирусописатели также использовали другие способы — например, модификацию конфигурационного файла Android-приложений `AndroidManifest.xml`. В частности, они добавляли мусорные байты `b'\x00'` в структуру атрибутов файла, из-за чего тот считывается некорректно.

Перспективы и тенденции

Прошедший год показал, что киберпреступники по-прежнему активно обогащаются за счет владельцев Android-устройств. Их основными инструментами остаются рекламные и банковские трояны, вредоносные приложения со шпионской функциональностью, а также мошенническое ПО. В этой связи в 2025 году стоит ожидать появления новых угроз такого типа.

Несмотря на предпринимаемые шаги для повышения безопасности Google Play, этот каталог все еще остается одним из источников распространения Android-угроз. Поэтому нельзя исключать появления в нем новых вредоносных и нежелательных приложений.

Выявленный в минувшем году очередной случай заражения ТВ-приставок с ОС Android говорит о том, что вирусописатели используют самые разные векторы атак. Вполне возможно, что злоумышленники не только вновь обратят свой взор на такие устройства, но и продолжат искать другие потенциальные цели среди разнообразия Android-гаджетов.

Не исключено, что вирусописатели продолжат активно внедрять новые способы обхода анализа и детектирования вредоносных программ.

Специалисты компании «Доктор Веб» продолжают следить за развитием «мобильных» киберугроз и обеспечивать защиту наших пользователей. Чтобы повысить свою безопасность, **установите антивирус Dr.Web для мобильных устройств**, который поможет в борьбе с вредоносными, нежелательными и другими опасными программами, мошенниками и прочими угрозами.

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

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
«Доктор Веб» в других странах