«Доктор Веб»:
обзор вирусной активности для мобильных устройств за 2023 год

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

В 2023 году самыми распространенными Android-угрозами стали троянские программы, демонстрирующие рекламу. Шпионские троянские приложения по сравнению с предыдущим годом снизили свою активность и стали вторыми по числу детектирований на защищаемых антивирусом Dr.Web устройствах. Несмотря на то, что банковские трояны также выявлялись реже, они по-прежнему представляют серьезную опасность для пользователей по всему миру, поскольку данный тип угроз продолжает развиваться. В минувшем году было выявлено большое число новых семейств Android-банкеров, многие из них целенаправленно атаковали, например, российских и иранских пользователей.

Вместе с тем сохранялась высокая активность мошенников — те использовали всевозможные вредоносные приложения, с помощью которых реализовывали разнообразные мошеннические схемы.

В очередной раз киберпреступники не оставили без внимания и каталог Google Play. В течение года вирусная лаборатория «Доктор Веб» обнаружила в нем более 400 троянских программ, которые суммарно были загружены по меньшей мере 428 000 000 раз.

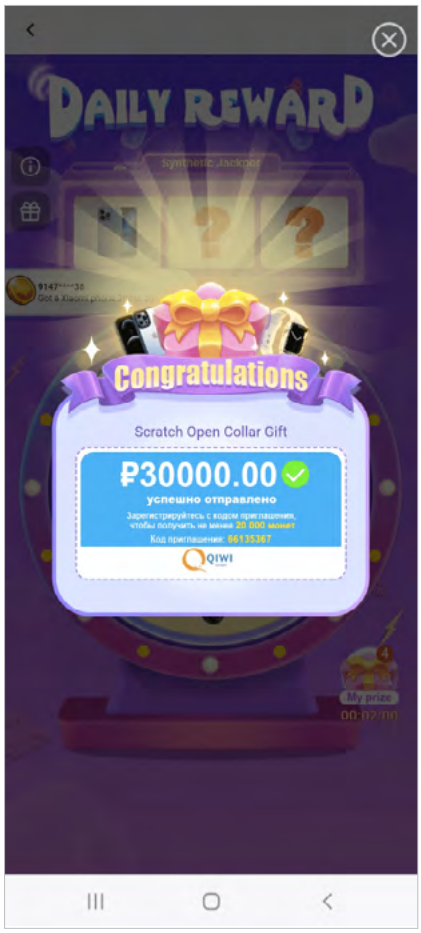
Кроме того, наши специалисты выявили очередные троянские программы, предназначенные для кражи криптовалют, при этом злоумышленников вновь интересовали владельцы устройств не только под управлением Android, но и операционной системы iOS.

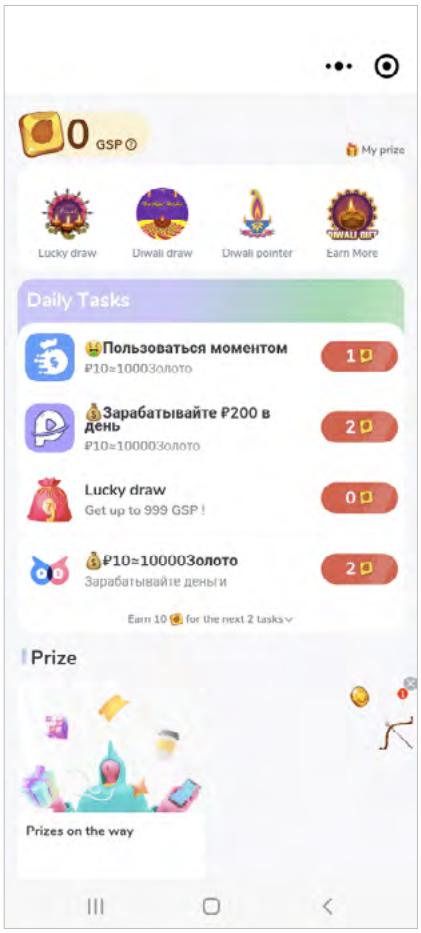
Тенденции прошедшего года

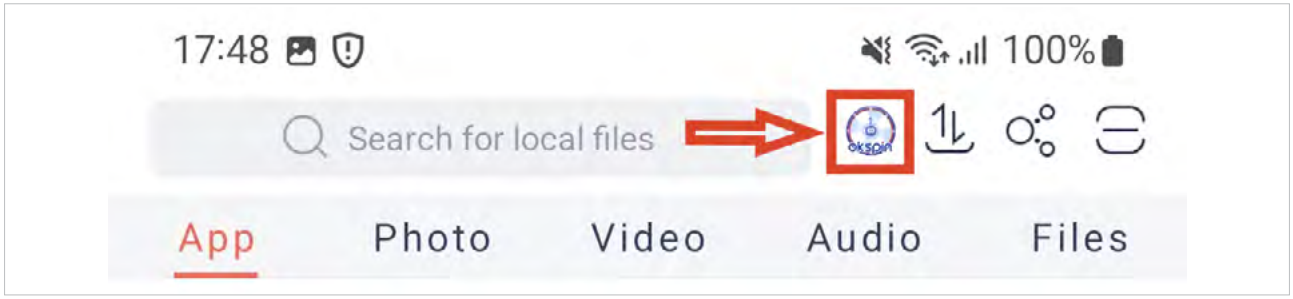
- Рост активности рекламных троянских программ
- Снижение активности банковских троянских приложений
- Появление новых семейств Android-банкеров, целью которых были пользователи из России и Ирана
- Появление множества новых угроз в каталоге Google Play
- Сохранение высокой активности мошенников
- Появление новых троянских программ для кражи криптовалют у пользователей

Наиболее интересные события 2023 года

В мае прошлого года компания «Доктор Веб» выявила в Google Play более 100 приложений с программным модулем SpinOk, который позиционировался как специализированная маркетинговая платформа для встраивания в Android-игры и программы. Этот инструмент предназначался для удержания пользователей в приложениях с помощью мини-игр, системы заданий и якобы розыгрышей призов. Однако модуль обладал шпионской функциональностью и потому был добавлен в вирусную базу Dr.Web как Android.Spy.SpinOk. Он собирал информацию о хранящихся на Android-устройствах файлах и мог передавать их злоумышленникам, а также подменять и загружать содержимое буфера обмена на удаленный сервер. Кроме того, модуль демонстрировал рекламу в виде баннеров, примеры которых показаны ниже.



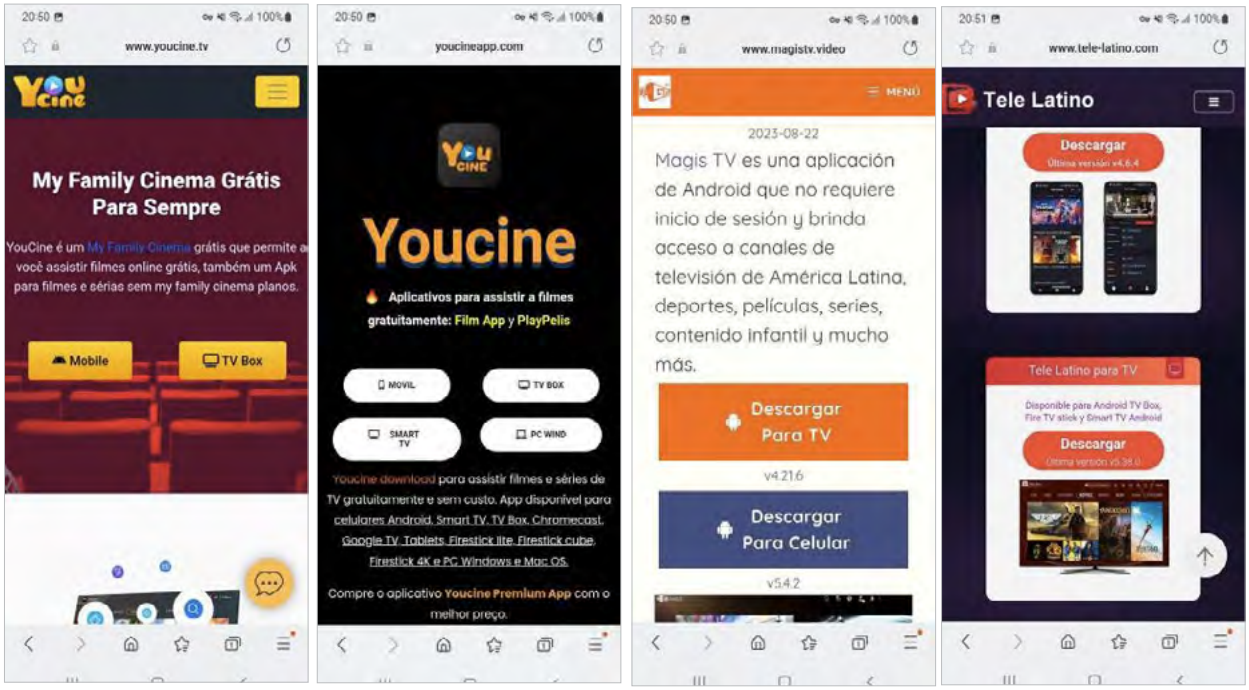




«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

В общей сложности найденные приложения с Android.Spy.SpinOk были загружены более 421 000 000 раз. После обращения в нашу компанию разработчик SpinOk внес исправления в модуль, вследствие чего актуальная на тот момент версия платформы 2.4.2 уже не содержала троянской функциональности.

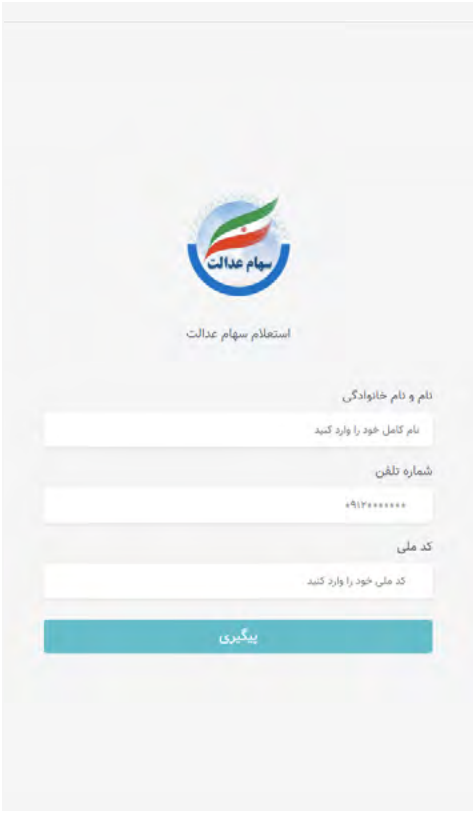
В начале прошлого сентября компания «Доктор Веб» опубликовала исследование бэкдора Android.Pandora.2, который нацелен преимущественно на испаноязычных пользователей. Массовые случаи атак с его участием фиксировались в марте 2023 года. Первые модификации этой троянской программы были добавлены в вирусную базу антивируса Dr.Web еще в июле 2017 года. Android.Pandora.2 и его различные модификации заражают смарт-телевизоры и приставки с Android TV, попадая на них через скомпрометированные версии прошивок, а также при установке троянских версий программ для нелегального просмотра видео онлайн. Примеры сайтов, распространяющих бэкдора, показаны ниже:



Троян создает ботнет из зараженных устройств и способен по команде злоумышленников проводить DDoS-атаки различных типов. Также он может выполнять ряд других действий — например, устанавливать собственные обновления и заменять системный файл hosts. Проведенный нашими специалистами анализ показал, что при создании трояна вирусописатели использовали наработки авторов Linux.Mirai, взяв за основу часть его кода. В свою очередь, Linux.Mirai с 2016 года широко применяется для заражения устройств «интернета вещей» (IoT-устройств) и проведения DDoS-атак на различные веб-сайты.

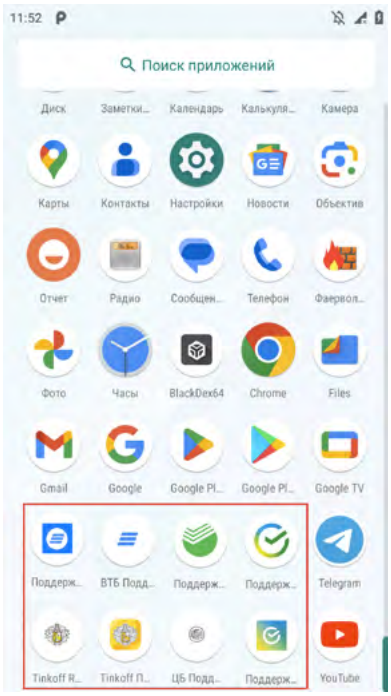
В том же месяце вирусные аналитики «Доктор Веб» сообщили о случаях распространения многофункциональных троянов-шпионов Android.Spy.Lydia, нацеленных на иранских пользователей. Представители этого семейства маскируются под финансовую платформу для онлайн-торговли и по команде атакующих способны выполнять различные вредоносные дей-

ствия. Например, перехватывать и отправлять СМС, собирать сведения о контактах в телефонной книге, похищать содержимое буфера обмена, загружать фишинговые сайты и т. д. Трояны Android.Spy.Lydia могут применяться во всевозможных мошеннических схемах и использоваться для кражи персональных данных. Кроме того, с их помощью злоумышленники могут похищать деньги своих жертв.



В конце сентября наша компания предупредила об участившихся случаях мошенничества с применением программ для удаленного администрирования мобильных устройств, с помощью которых злоумышленники получали полный контроль над Android-устройствами. Притворяясь сотрудниками поддержки кредитных организаций, киберпреступники сообщали потенциальным жертвам о «подозрительной активности» с их банковскими счетами и предлагали найти и загрузить в Google Play то или иное «приложение поддержки банка». На самом деле этой программой был инструмент для удаленного доступа к рабочему столу, чаще всего — RustDesk Remote Desktop. После блокировки этой утилиты в Google Play злоумышленники стали распространять ее через мошеннические сайты. При этом в некоторых случаях для большей убедительности они модифицировали программу, заменяя ее имя и значок на соответствующие тому или иному банку. Такие троянские версии программы детектируются как Android.FakeApp.1426.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год



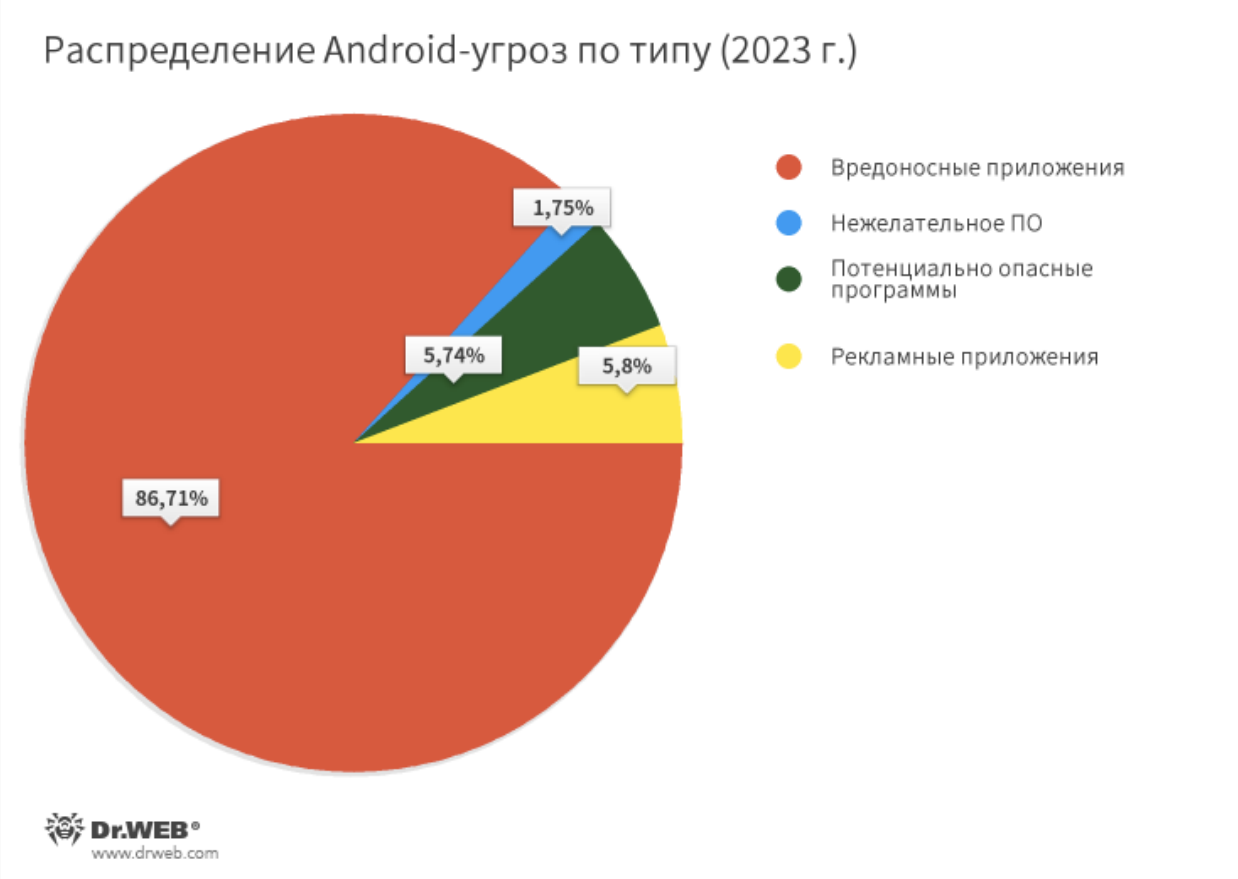
Вместе с тем в 2023 году специалисты «Доктор Веб» продолжили выявлять вредоносные сайты, через которые киберпреступники распространяли поддельные приложения криптокошельков для Android- и iOS-устройств с целью кражи криптовалюты.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

Статистика

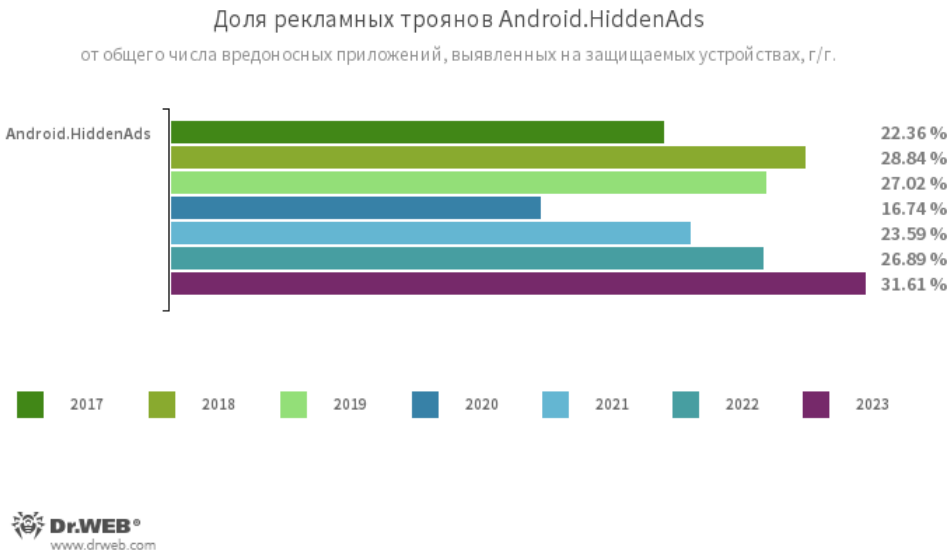
В 2023 году наиболее распространенными Android-угрозами вновь стали вредоносные программы — на их долю пришлось 86,71% от общего числа детектирований антивируса Dr.Web. На втором месте с долей в 5,80% расположились рекламные приложения. Третьими по распространенности стали потенциально опасные программы — они выявлялись на защищаемых устройствах в 5,74% случаев. В 1,75% случаев пользователи сталкивались с нежелательными программами.

Распределение угроз по типу на основе данных статистики детектирований Dr.Web для мобильных устройств Android наглядно представлено на следующей диаграмме:



Вредоносные приложения

Самыми распространенными вредоносными Android-приложениями стали рекламные трояны семейства Android.HiddenAds. По сравнению с 2022 годом их доля в общем объеме выявленных антивирусом Dr.Web вредоносных программ возросла на 4,72 п. п. и составила 31,61%.



Наиболее активным представителем семейства стал Android.HiddenAds.3697 — он обнаруживался на защищаемых устройствах в 10,72% случаев. Различные варианты этой вредоносной программы на протяжении нескольких лет остаются лидерами по числу детектирований. Например, в 2021 году распространение получила модификация Android.HiddenAds.1994, а в 2022-м — Android.HiddenAds.3018. Вместе с Android.HiddenAds.3697 в 2023 году наши специалисты выявили ряд других версий этого трояна. Среди них — Android.HiddenAds.3697, Android.HiddenAds.3831, Android.HiddenAds.3851 и Android.HiddenAds.3956. Не исключено, что со временем одна из них также сможет занять лидирующие позиции.

Вторыми по распространенности стали обладающие шпионской функциональностью трояны семейства Android.Spy. По сравнению с 2022 годом их доля в общем объеме выявленных антивирусом Dr.Web вредоносных программ снизилась на 14,01 п. п. и составила 28,22%. Наиболее активным среди них был Android.Spy.5106 — на него пришлось 20,80% всех детектирований вредоносного ПО. А с учетом более ранних вариантов трояна, Android.Spy.4498 и Android.Spy.4837, его доля составила 24,32% — почти четверть случаев обнаружения.

На третьем месте расположились рекламные трояны семейства Android.MobiDash. По сравнению с годом ранее их доля в суммарном объеме детектирований вредоносного ПО выросла на 5,25 п. п. до 10,06%.

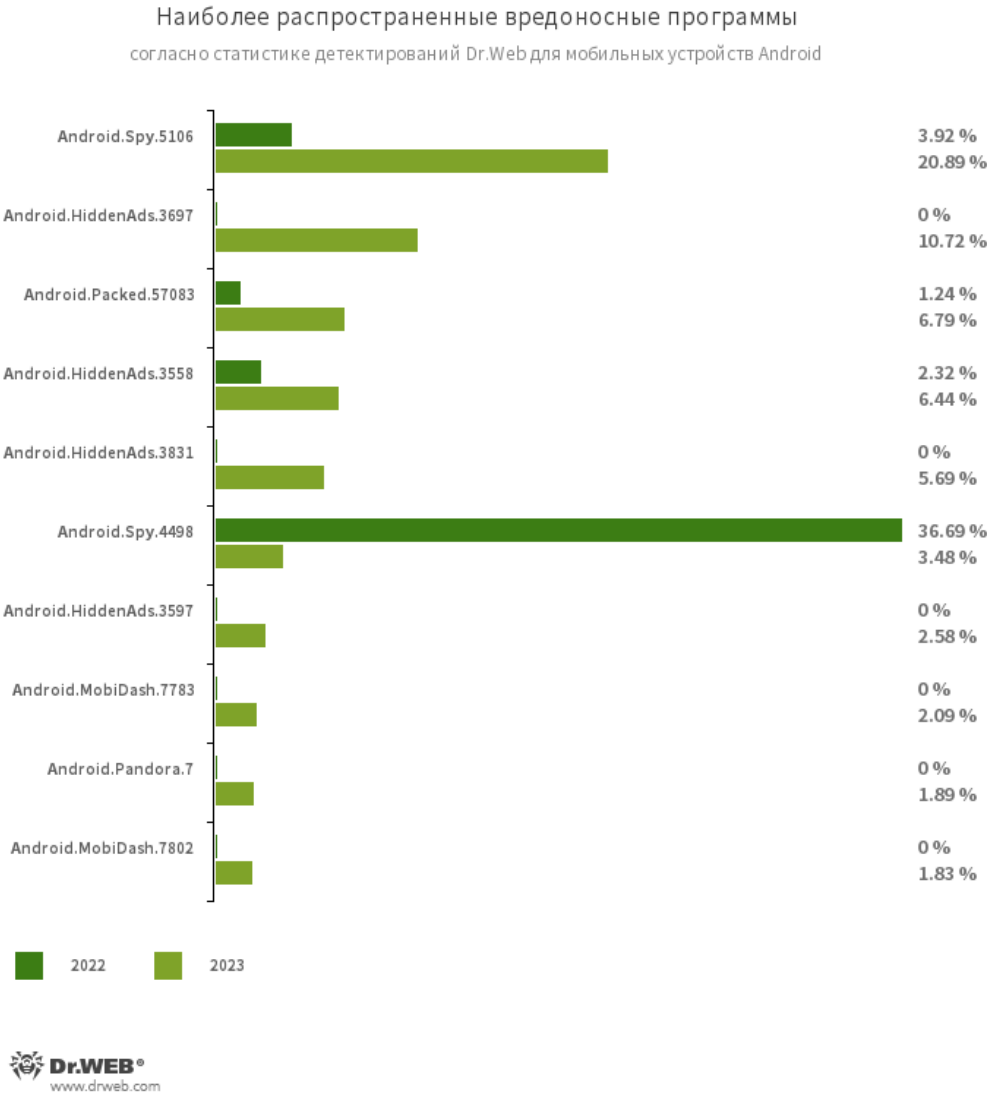
В 2023 году продолжилось снижение активности вредоносных приложений, предназначенных для загрузки и установки других программ, а также способных выполнять произвольный код. Так, доля детектирований троянов Android.DownLoader уменьшилась на 1,58 п. п. до 2,18%, Android.Triada — на 0,99 п. п. до 2,14% и Android.RemoteCode — на 0,01 п. п. до 2,83%. Доля детектирований Android.Mobifun сократилась на 0,33 п. п. до 0,25%, а Android.Xiny — на 0,21 п. п. до 0,27%.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

В то же время возросло число атак с использованием вредоносных программ-подделок Android.FakeApp, которые злоумышленники используют в различных мошеннических схемах. В минувшем году их доля в общем объеме выявленного антивирусом Dr.Web вредоносного ПО возросла на 0,85 п. п. до 1,83%.

В 2023 году снизилась активность троянских программ-вымогателей Android.Locker. Их доля в общем объеме детектирований вредоносного ПО уменьшилась с 1,50% до 1,15%. При этом наблюдалось увеличение количества детектирований Android.Packed — вредоносных программ различного типа, защищенных программными упаковщиками. Число их обнаружений увеличилось на 5,22 п. п. до 7,98%.

Десять наиболее часто детектируемых вредоносных приложений в 2023 году представлены на иллюстрации ниже:



- Android.Spy.5106
- Android.Spy.4498

Детектирование различных 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.3697
- Android.HiddenAds.3558
- Android.HiddenAds.3831
- Android.HiddenAds.3597

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.Packed.57083

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

- Android.MobiDash.7783
- Android.MobiDash.7802

Троянские программы, показывающие надоедливую рекламу. Они представляют собой программные модули, которые разработчики ПО встраивают в приложения.

- Android.Pandora.7

Детектирование вредоносных приложений, скачивающих и устанавливающих троянскую программу-бэкдор Android.Pandora.2. Такие загрузчики злоумышленники часто встраивают в приложения для Smart TV, ориентированные на испаноязычных пользователей.

Нежелательное ПО

Самой распространенной нежелательной программой в 2023 году стала Program.FakeMoney.7 — на нее пришлось 29,90% или почти треть от общего числа детектирований угроз этого типа. Она относится к семейству приложений, которые предлагают пользователям заработать на выполнении различных заданий, но в итоге не выплачивают никаких реальных вознаграждений.

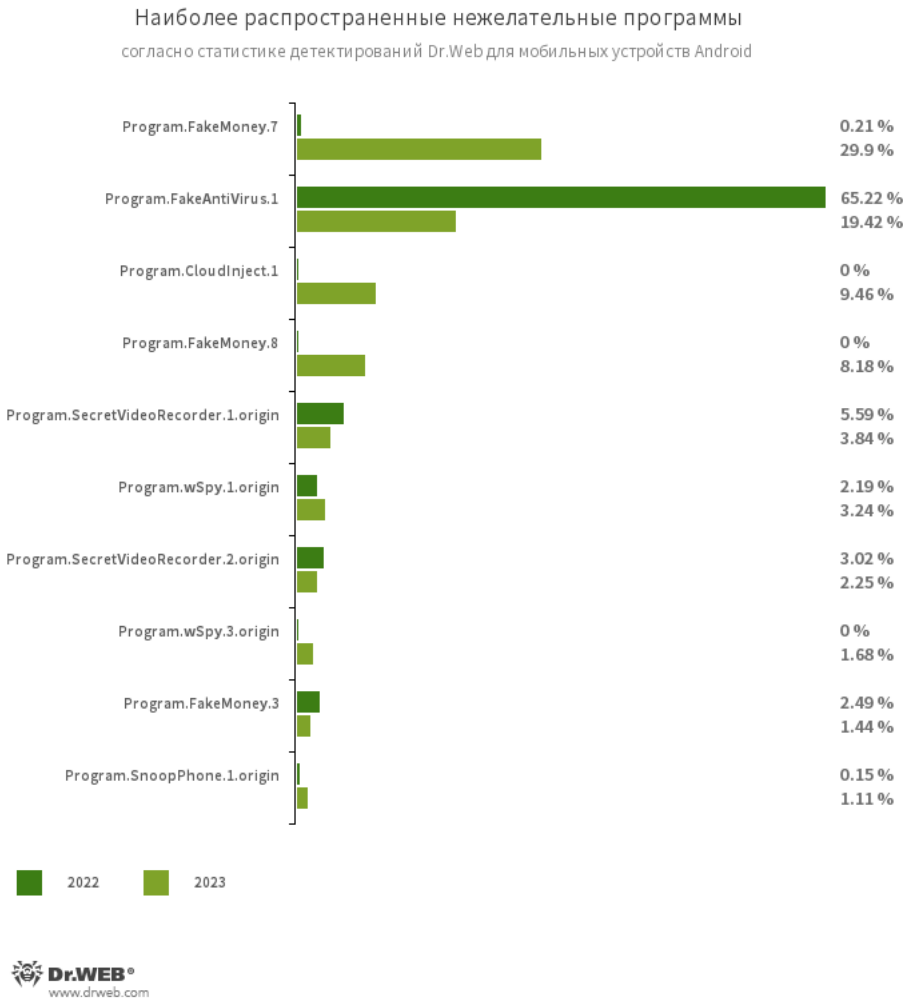
Лидер 2022 года — программа Program.FakeAntiVirus.1 — спустя год опустилась на второе место с долей в 19,42% детектирований. Это приложение имитирует работу антивирусов, обнаруживает несуществующие угрозы и предлагает владельцам Android-устройств купить полную версию для «исправления» якобы выявленных проблем.

На третьем месте с долей в 9,46% расположились программы, которые модифицируются через облачный сервис CludInject — антивирус Dr.Web детектирует такие приложения как Program.CloudInject.1. В процессе модификации к ним добавляются опасные разрешения и обфусцированный код, назначение которого нельзя проконтролировать.

Как и годом ранее, в 2023-м пользователи часто сталкивались с программами, позволяющими следить за их действиями и собирать о них различную информацию. Злоумыш-

ленники могут применять подобные приложения для незаконной слежки за владельцами Android-устройств. На защищаемых Dr.Web устройствах среди такого ПО чаще всего обнаруживались Program.SecretVideoRecorder.1.origin (3,84% случаев), Program.wSpy.1.origin (3,24% случаев), Program.SecretVideoRecorder.2.origin (2,25% случаев), Program.wSpy.3.origin (1,68% случаев), **Program.SnoopPhone.1.origin** (1,11% случаев), Program.Reptilicus.8.origin (0,98% случаев) и **Program.WapSniff.1.origin** (0,83% случаев).

Десять наиболее часто детектируемых нежелательных приложений в 2023 году представлены на следующей диаграмме:



- Program.FakeMoney.7
- Program.FakeMoney.8
- Program.FakeMoney.3

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. Даже когда пользователям это удается, получить выплаты они не могут.

- 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 дистанционного управлять ими — блокировать, показывать настраиваемые диалоги, отслеживать факт установки и удаления другого ПО 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.1.origin
- 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.SnoopPhone.1.origin

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

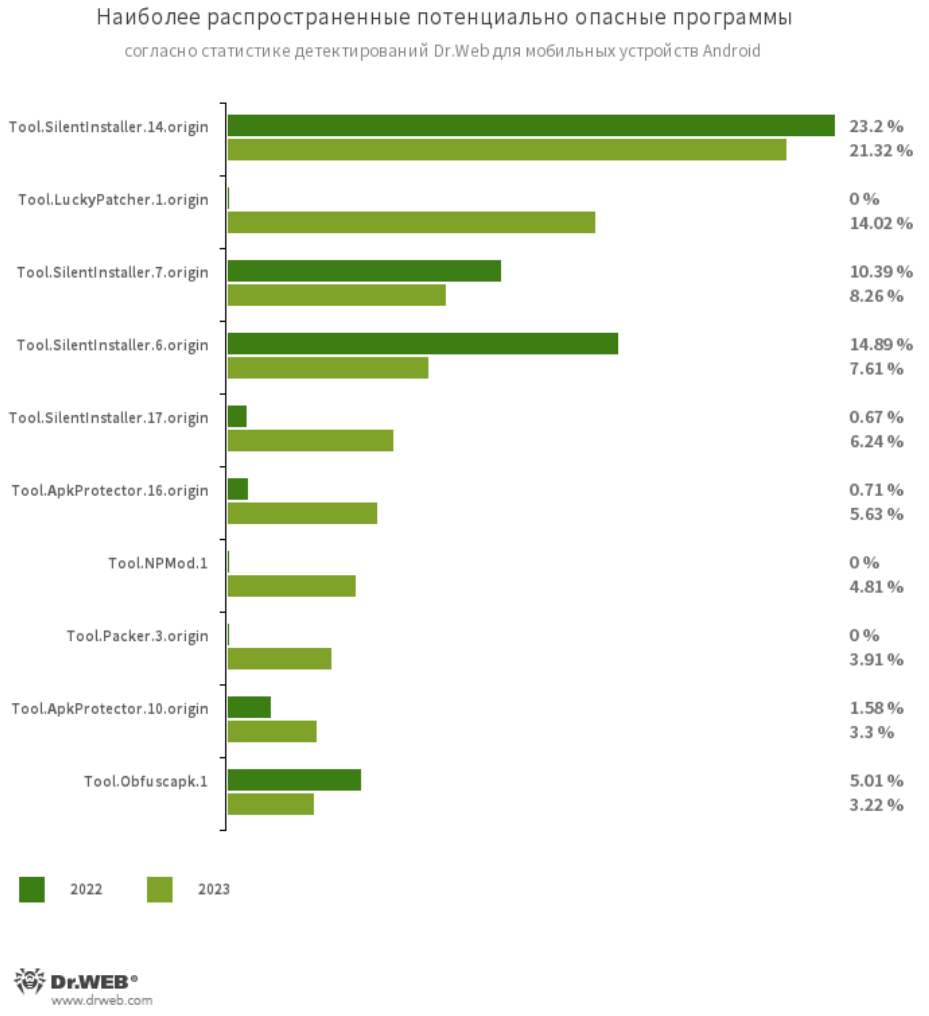
Потенциально опасные программы

В 2023 году наиболее часто детектируемыми потенциально опасными программами вновь стали утилиты Tool.SilentInstaller, позволяющие запускать Android-приложения без их установки. Они не являются вредоносными, однако злоумышленники могут применять их для запуска вредоносного ПО. На них пришлось 48,89% или почти половина детектирований потенциально опасных приложений. При этом по сравнению с 2022 годом их доля снизилась на 17,94 п. п. Вторыми по распространенности стали представители семейства утилит Tool.LuckyPatcher, с помощью которых возможна модификация Android-программ с добавлением в них загружаемых из интернета скриптов. На долю этих инструментов пришлось 14,02% случаев обнаружения потенциально опасного ПО. На третьем месте расположились защищенные упаковщиком

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

Tool.ApkProtector программы — число их детектирований увеличилось на 5,33 п. п. до 10,14%. При этом увеличилось и количество детектирований приложений, защищенных другими семействами программных упаковщиков. Так, доля представителей семейства Tool.Packer возросла с 3,58% до 4,74%, а доля представителей семейства **Tool.Ultima** — с 0,05% до 1,04%.
Другим распространенным потенциально опасным ПО стала утилита NP Manager. Она предназначена для модификации Android-приложений и обхода в них проверки цифровой подписи с помощью встраиваемого в них модуля. Измененные таким образом программы антивирус Dr.Web детектирует как **Tool.NPMod**. Доля подобных приложений составила 4,81%.
В то же время программы, модифицированные с использованием утилиты-обфускатора Tool.Obfuscapk, выявлялись на защищаемых устройствах реже — их доля по сравнению с 2022 годом снизилась с 5,01% до 3,22%.

Десять наиболее распространенных потенциально опасных приложений, обнаруженных на Android-устройствах в 2023 году, представлены на иллюстрации ниже.



- Tool.SilentInstaller.14.origin
- Tool.SilentInstaller.7.origin
- Tool.SilentInstaller.6.origin

- Tool.SilentInstaller.17.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.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.ApkProtector.16.origin
- Tool.ApkProtector.10.origin

Детектирование Android-приложений, защищенных программным упаковщиком ApkProtector. Этот упаковщик не является вредоносным, однако злоумышленники могут использовать его при создании троянских и нежелательных программ, чтобы антивирусам было сложнее их обнаружить.

- **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.Packer.3.origin

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

- Tool.Obfuscapk.1

Детектирование приложений, защищенных утилитой-обфускатором Obfuscapk. Эта утилита используется для автоматической модификации и запутывания исходного кода Android-приложений, чтобы усложнить их обратный инжиниринг. Злоумышленники применяют ее для защиты вредоносных и других опасных программ от обнаружения антивирусами.

Рекламные приложения

Самым популярным рекламным ПО в 2023 году стало семейство встраиваемых в Android-программы рекламных модулей Adware.Adpush, на которые пришлось более трети детектирований — 35,82% (по сравнению с 2022 годом их доля снизилась на 24,88 п. п.). Вторыми по распространенности оказались представители нового семейства Adware.MagicPush с долей в 9,58%. На третьем месте с показателем 8,59% (доля увеличилась на 3,24 п. п.) расположились модули Adware.Airpush.

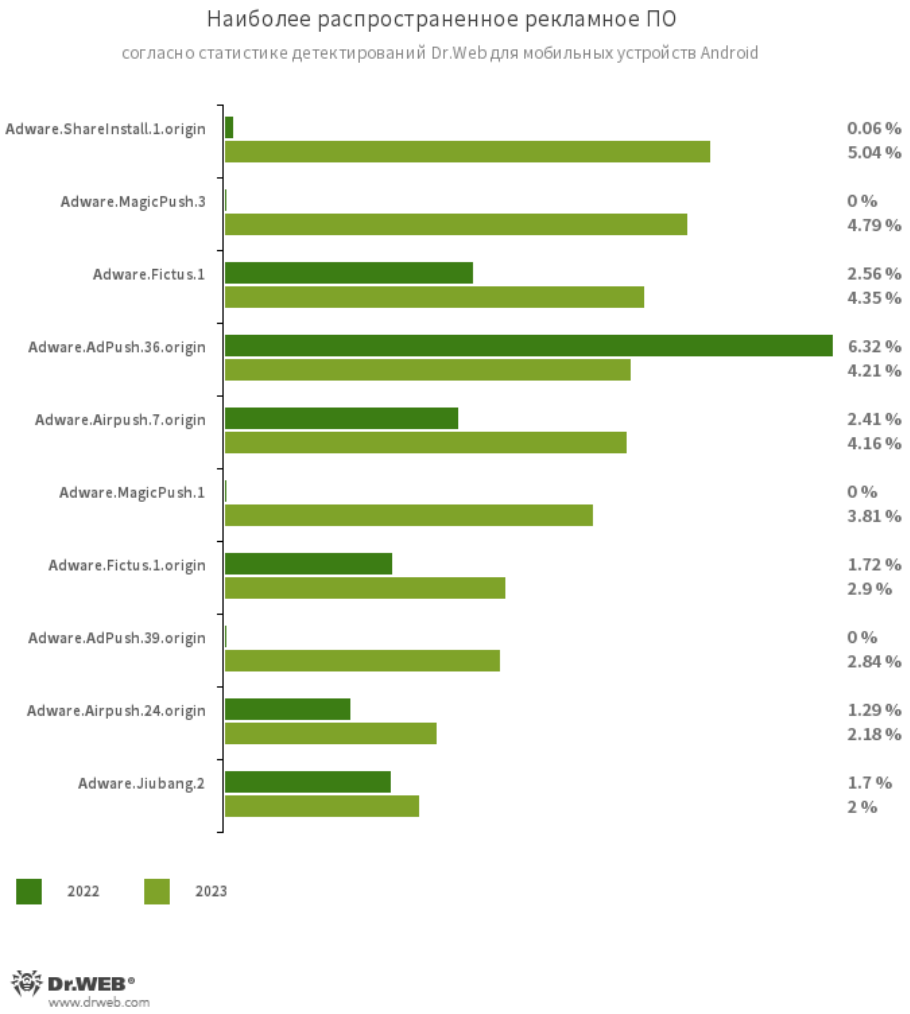
Среди лидеров также были представители семейств **Adware.ShareInstall**, доля которых уве-

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

личилась с 0,06% до 5,04%, Adware.Fictus (рост с 2,58% до 4,41%), Adware.Leadbolt (рост с 3,31% до 4,37%), **Adware.Jiubang** (рост с 2,83% до 3,22%) и Adware.Youmi (рост с 0,06% до 2,20%).

В то же время модули Adware.SspSdk, которые годом ранее занимали вторую строчку, в 2023 году не попали даже в первую десятку самых распространенных семейств. На них пришлось 1,49% выявленного на защищаемых Android-устройствах рекламного ПО.

Десять наиболее распространенных рекламных приложений, обнаруженных на Android-устройствах в 2023 году, представлены на следующей диаграмме:



- Adware.ShareInstall.1.origin

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

- Adware.MagicPush.1
- Adware.MagicPush.3

Рекламный модуль, встраиваемый в Android-приложения. Он демонстрирует всплывающие баннеры поверх интерфейса операционной системы, когда эти программы не используются. Такие баннеры содержат вводящую в заблуждение информацию. Чаще всего в них сообщается о якобы обнаруженных подозрительных файлах либо говорится о необходимости заблокировать спам или оптимизировать энергопотребление устройства. Для этого пользователю предлагается зайти в соответствующее приложение, в которое встроен один из этих модулей. При открытии программы отображается реклама.

- 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.36.origin
- 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 быть похожи на 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
- Adware.Airpush.24.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.Jiubang.2**

Рекламный модуль, встраиваемый в Android-программы. Он демонстрирует баннеры с объявлениями поверх окон других приложений.

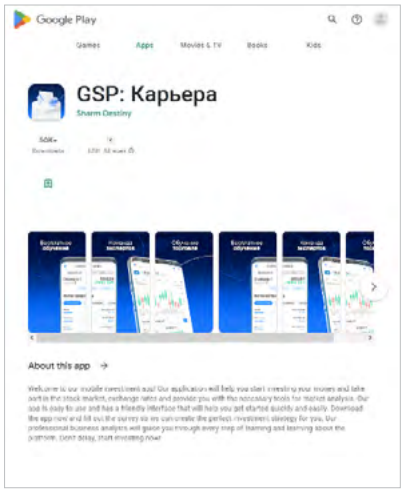
Угрозы в Google Play

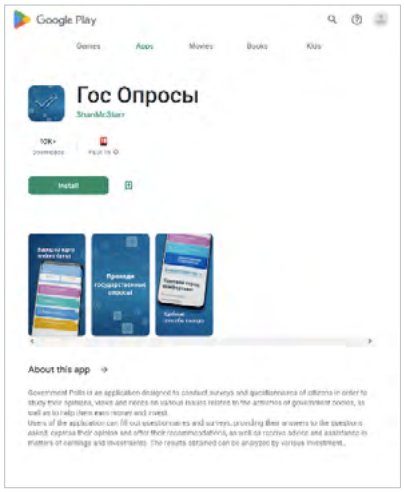
В 2023 году вирусная лаборатория компании «Доктор Веб» обнаружила в каталоге Google Play свыше 440 вредоносных приложений, которые в общей сложности были загружены не менее 428 434 576 раз. Наряду с множеством программ со встроенным троянским модулем Android.Spy.SpinOk, отмеченных в одном из предыдущих разделов обзора, наши специалисты выявили сотни троянов семейства Android.FakeApp. Применяемые киберпреступниками при реализации различных мошеннических схем, эти вредоносные приложения распространялись под видом самого разнообразного ПО. При определенных условиях они действитель-

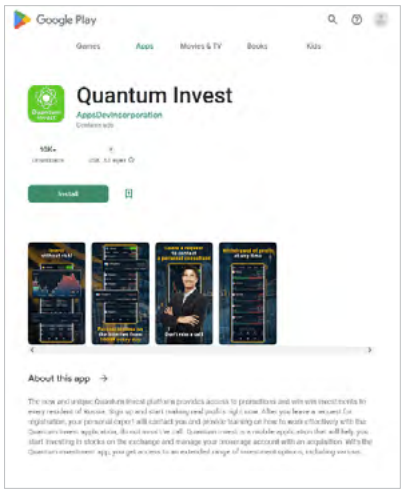
«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

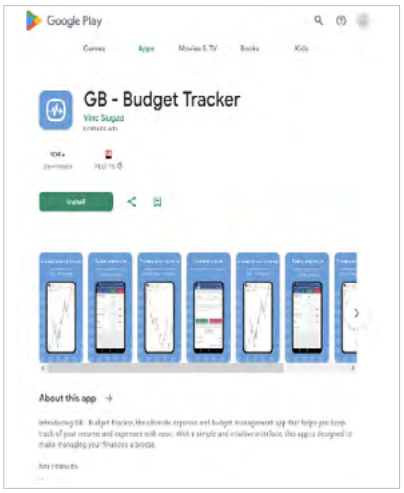
но могли предоставлять обещанную функциональность, но их основной задачей была загрузка целевых сайтов по команде удаленного сервера.

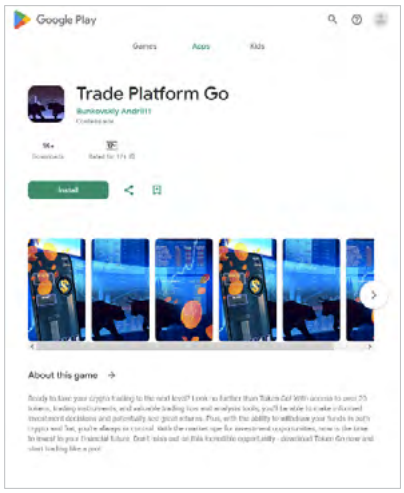
Многие из этих троянов злоумышленники выдавали за программы финансовой тематики — обучающие пособия и справочники, программы для ведения домашней бухгалтерии, инструменты для доступа к биржевой информации и торговле, приложения для прохождения специализированных опросов и т. п.







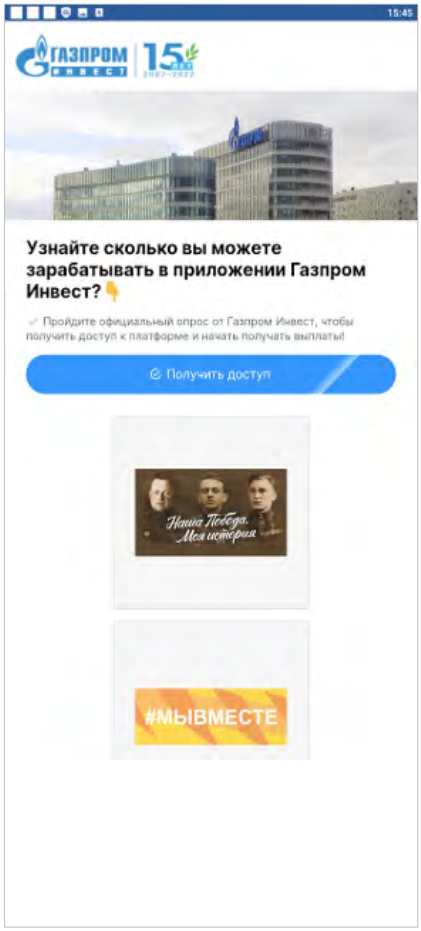


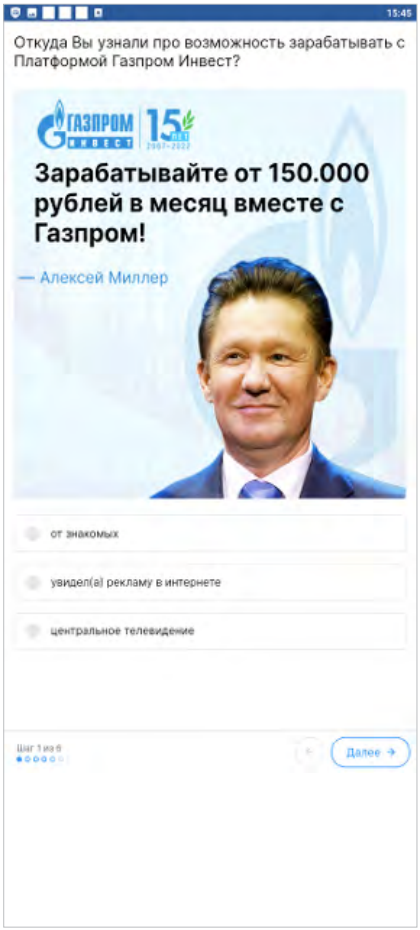


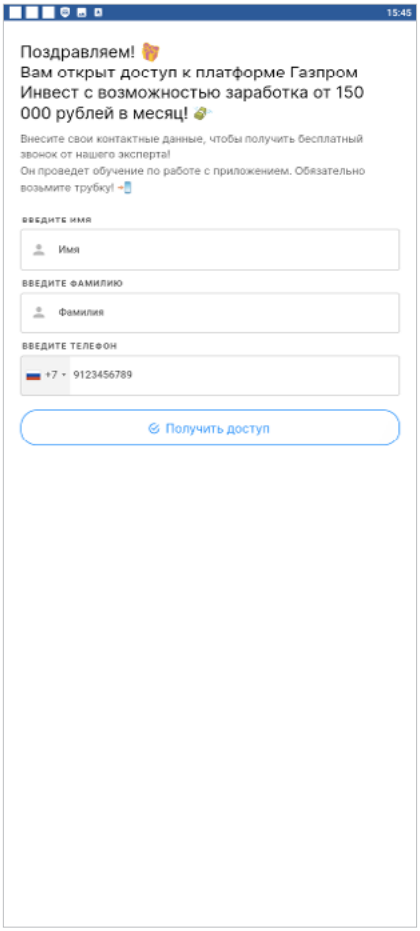
Такие программы-подделки могли загружать мошеннические сайты, на которых потенциальным жертвам якобы от имени известных компаний предлагалось заработать на инвестициях, торговле криптовалютами, а в некоторых случаях — даже получить «в подарок» акции компаний или некие выплаты от государства. Для «доступа» к той или иной услуге пользователи вначале должны были ответить на несколько вопросов, после чего предоставить персональные данные.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

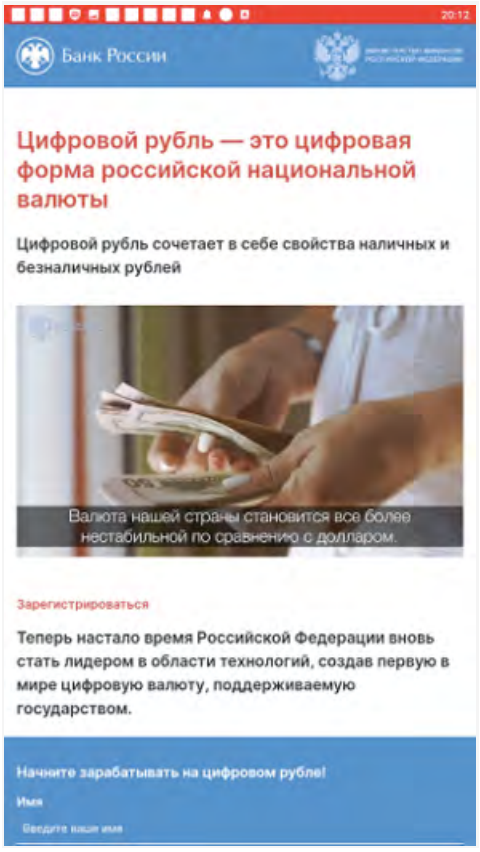
Ниже представлены примеры загружаемых этими троянами мошеннических сайтов. В первом случае злоумышленники предлагали пользователям получить доступ к некой инвестиционной платформе, якобы имеющей отношение к крупной российской нефтегазовой компании. Во втором — мошенники якобы от имени Центрального банка Российской Федерации предлагали «начать зарабатывать на цифровом рубле».

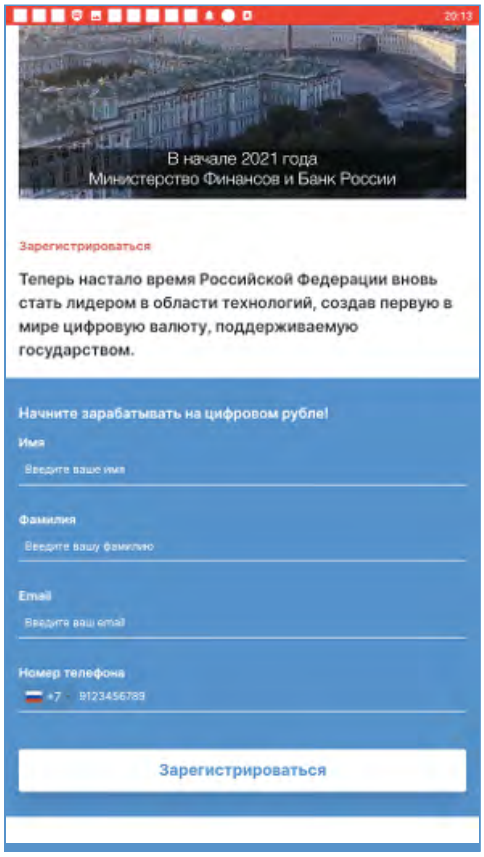




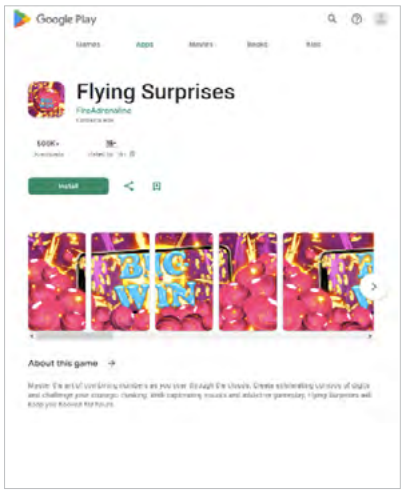


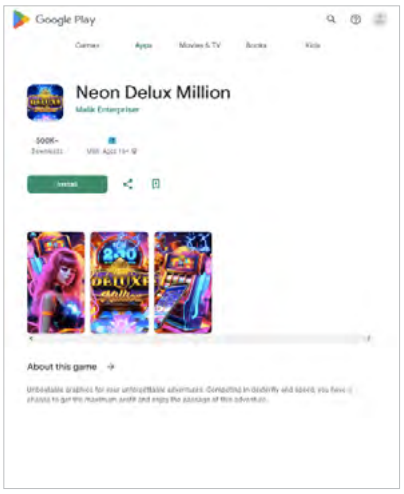
«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

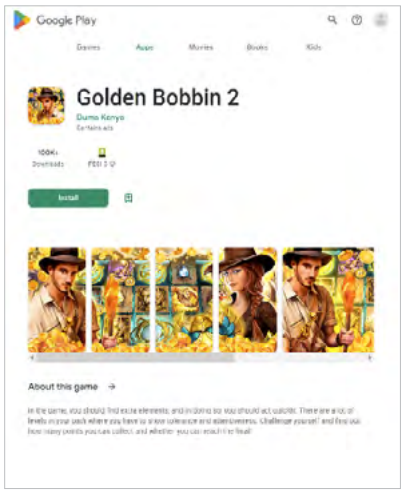




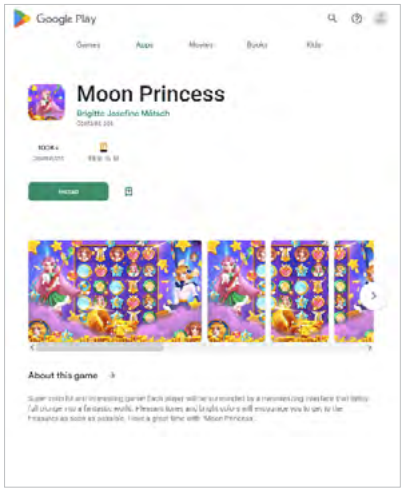
Часть программ-подделок распространялась под видом игр — они могли загружать сайты онлайн-казино и букмекеров.

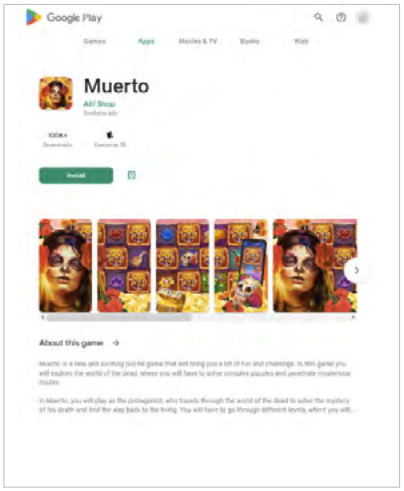


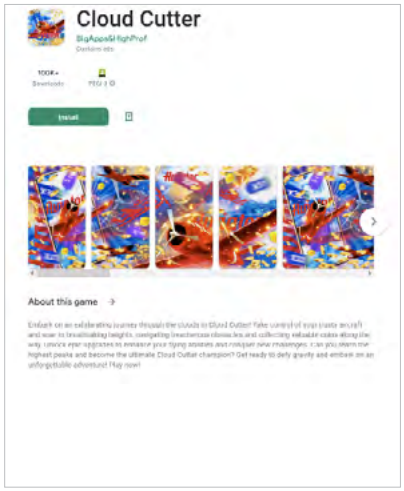




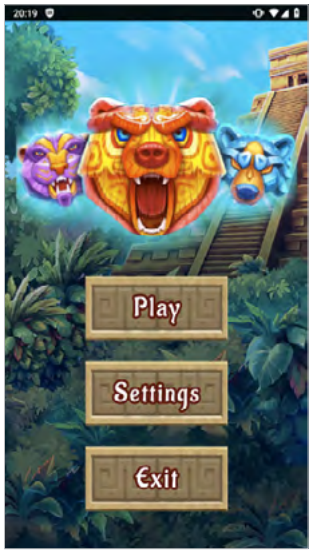
«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год



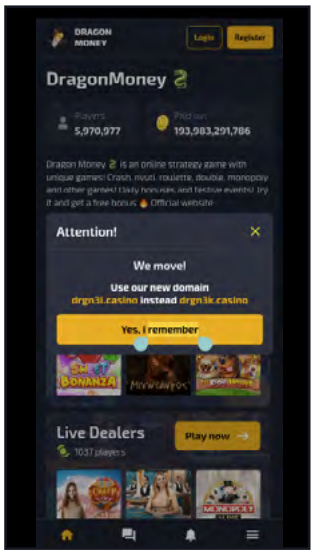


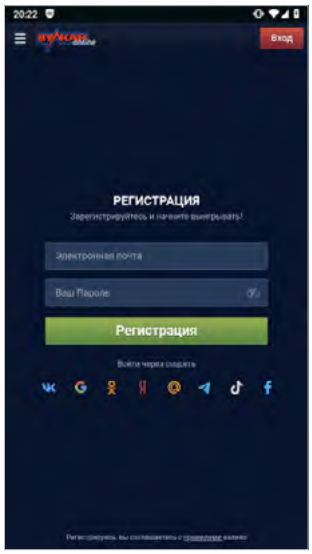


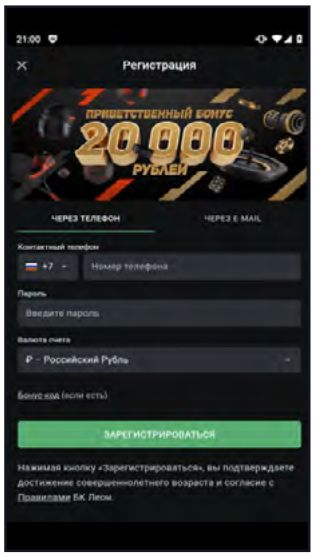
Примеры работы таких троянских приложений в качестве игр:

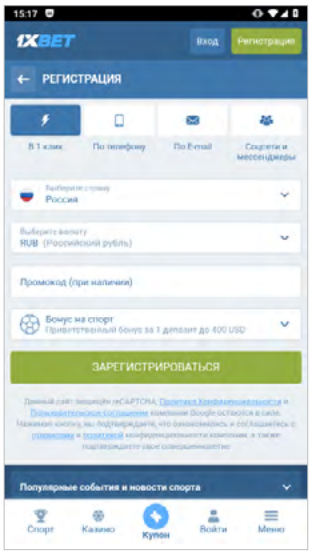


Примеры загружаемых ими сайтов букмекерских контор и онлайн-казино:



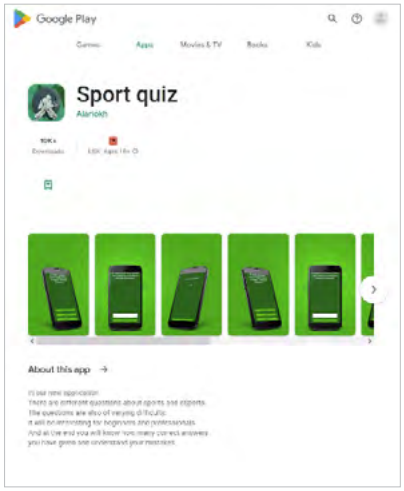


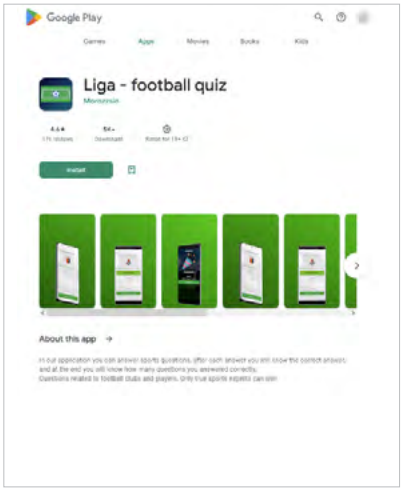


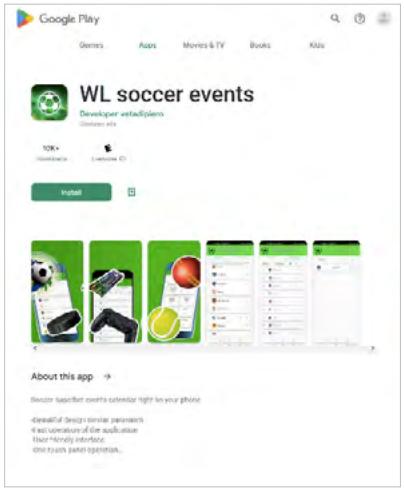


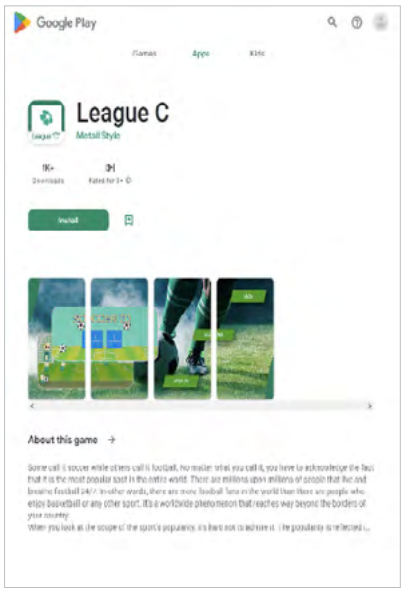
«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

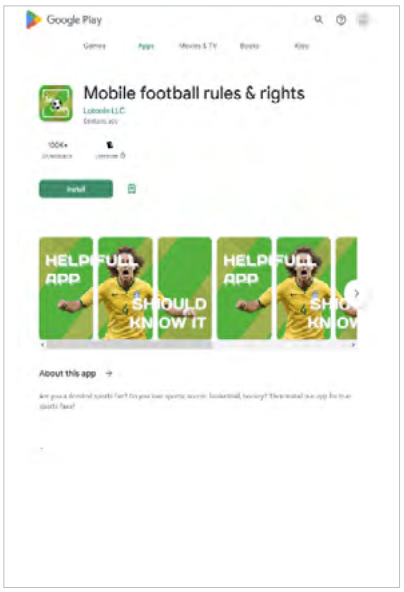
Другие трояны Android.FakeApp распространялись под видом программ спортивной тематики, в том числе — официального ПО легальных букмекерских контор, всевозможных справочников по различным видам спорта, приложений с информацией о матчах, программ для чтения спортивных новостей и т. д.:

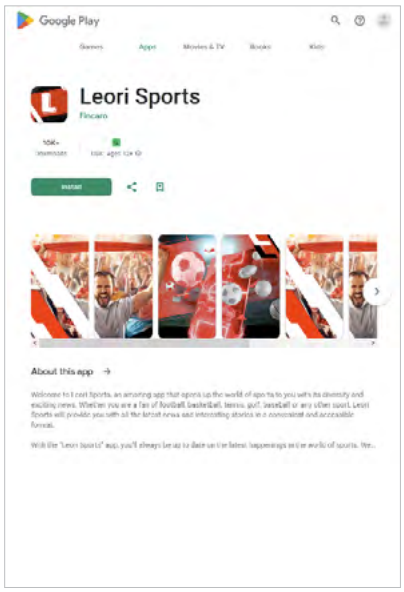








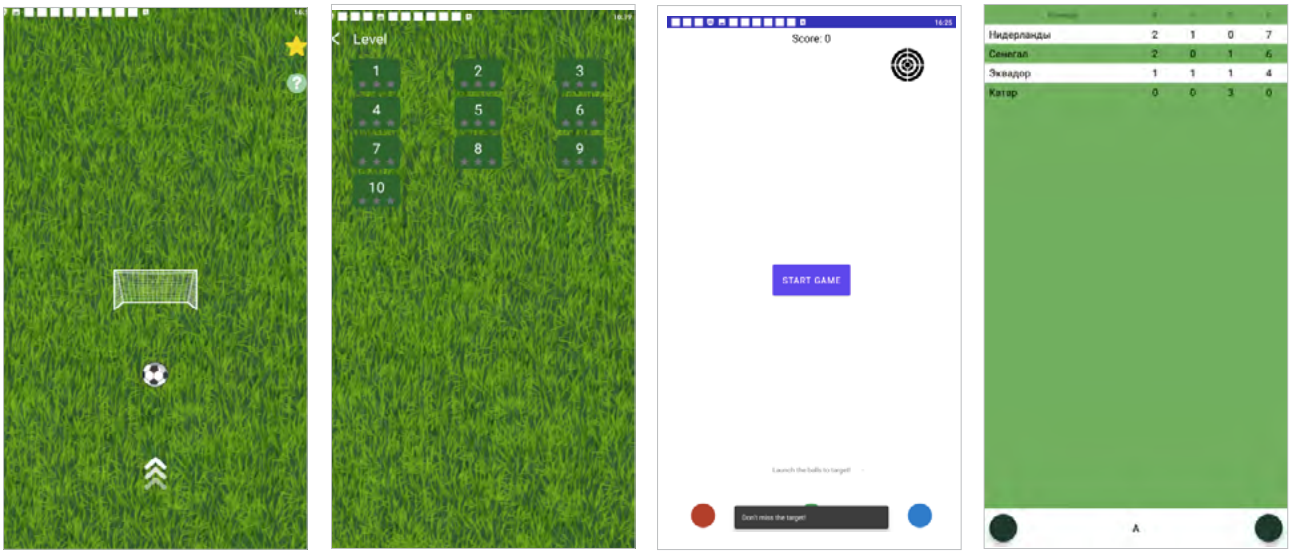




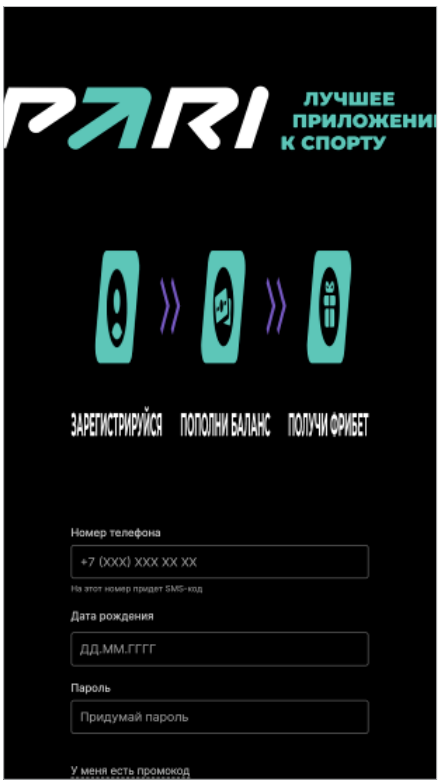
Они могли работать и как безобидное ПО (при этом их функциональность могла отличаться от заявленной), и загружать различные интернет-ресурсы.

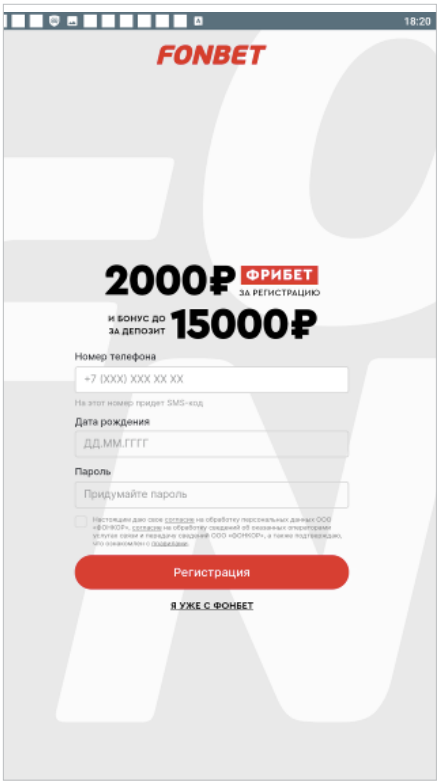
«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

Ниже представлены примеры работы этих троянов в качестве безобидных приложений: два из них запустились как игры, а третий продемонстрировал таблицу с информацией о футбольных матчах.



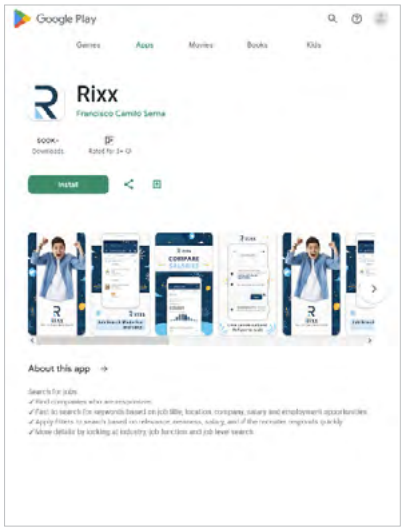
Эти же программы позднее стали загружать сайты, предлагающие воспользоваться услугами букмекеров:

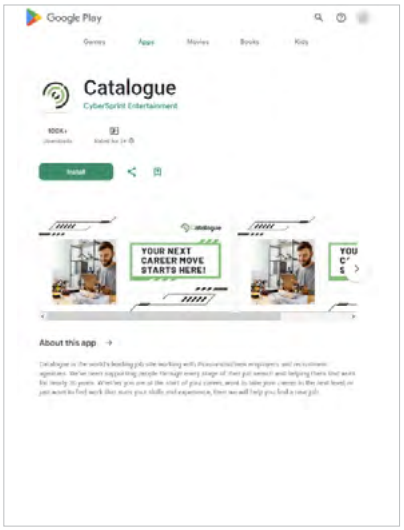


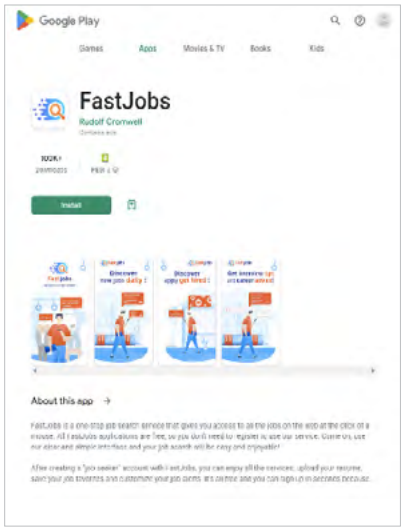


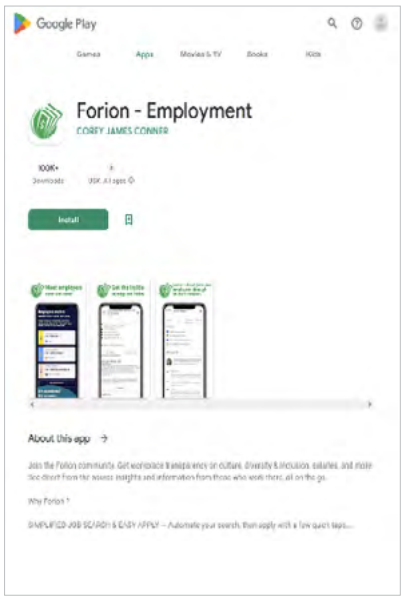
«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

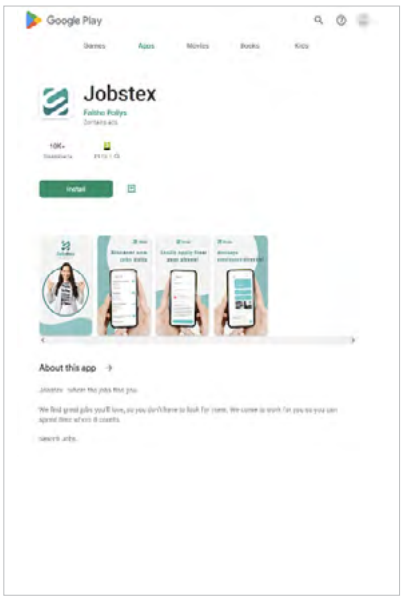
Некоторые приложения-подделки пользователи устанавливали, думая, что те являются программами для поиска вакансий:

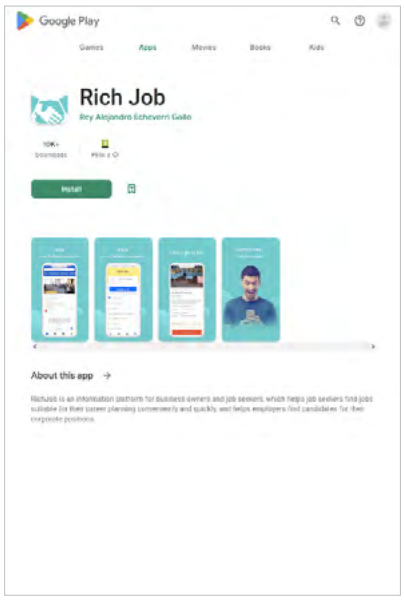






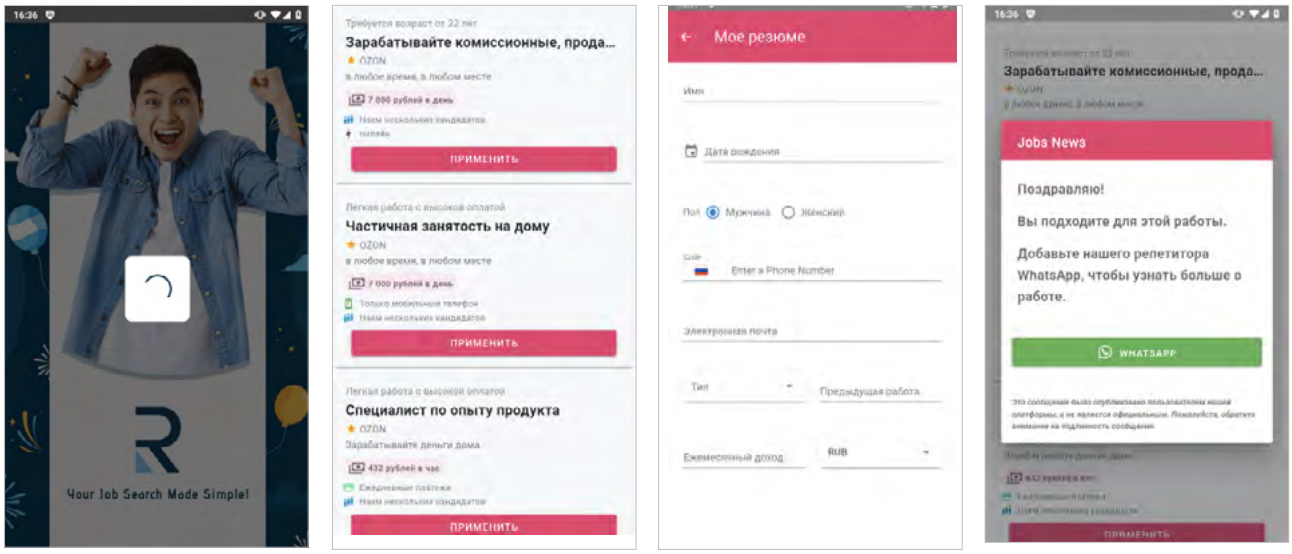




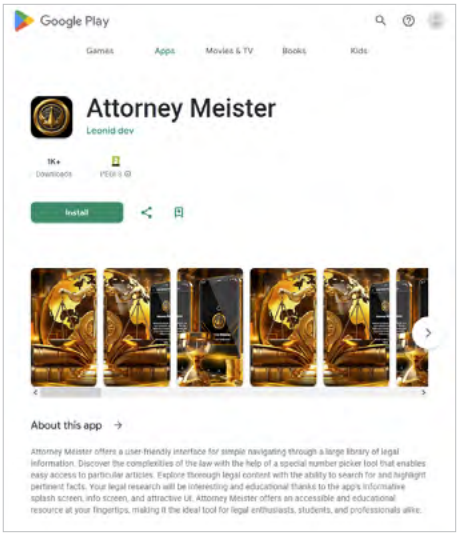


«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

Подобные варианты троянов Android.FakeApp демонстрируют потенциальным жертвам поддельные списки вакансий, которые загружаются с мошеннических сайтов. Когда пользователи пытаются откликнуться на одно из «объявлений», им либо предлагается связаться с «работодателем» через мессенджеры — например, WhatsApp или Telegram, либо указать персональные данные в специальной форме — якобы для составления и отправки резюме.

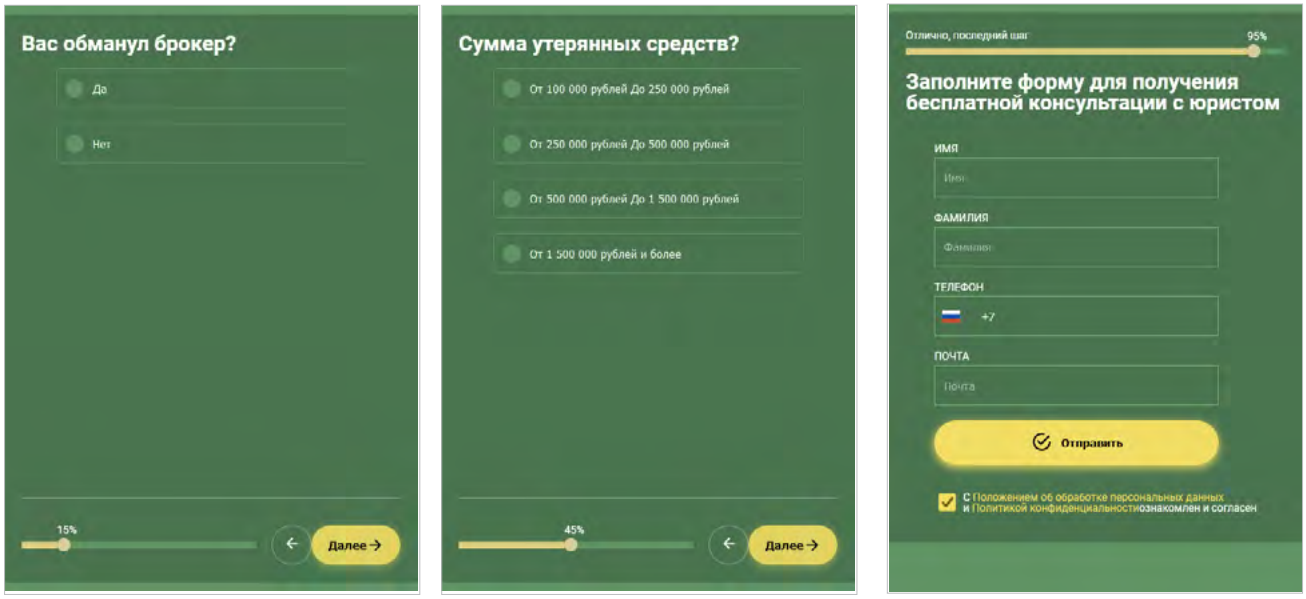


В то же время в 2023 году тематика программ-подделок Android.FakeApp, которые загружали мошеннические интернет-ресурсы, продолжила расширяться. Так, на фоне многолетних попыток киберпреступников заманить пользователей на фиктивные финансовые сайты наши специалисты отметили появление вариантов троянов, которые выдавались за юридические приложения — например, справочники. Они якобы могли помочь жертвам «инвестиционных» мошенников вернуть утраченные деньги. На самом деле эти приложения загружали очередные мошеннические сайты, работающие по уже известной схеме. Их посетители должны были ответить на несколько вопросов, после чего оставить персональные данные — в данном случае «для получения бесплатной консультации с юристом».

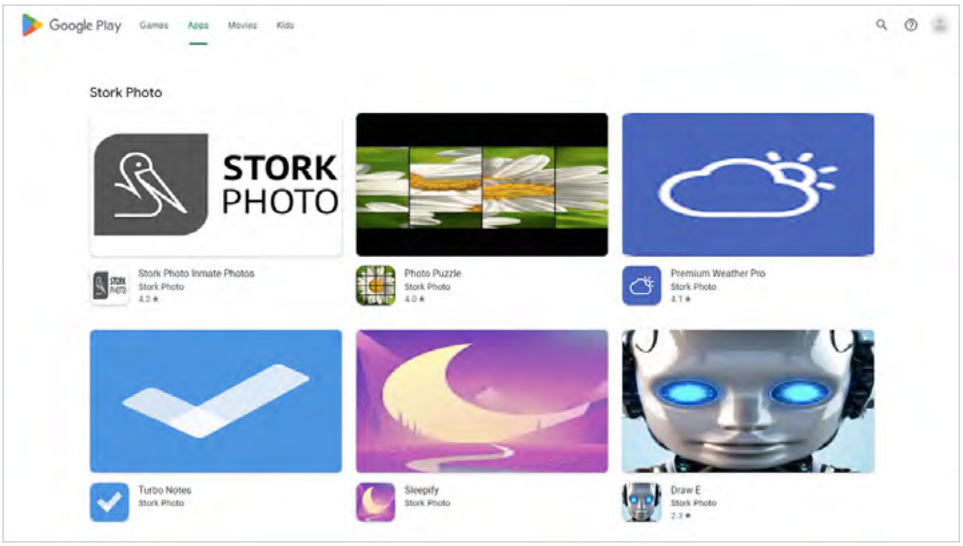


«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

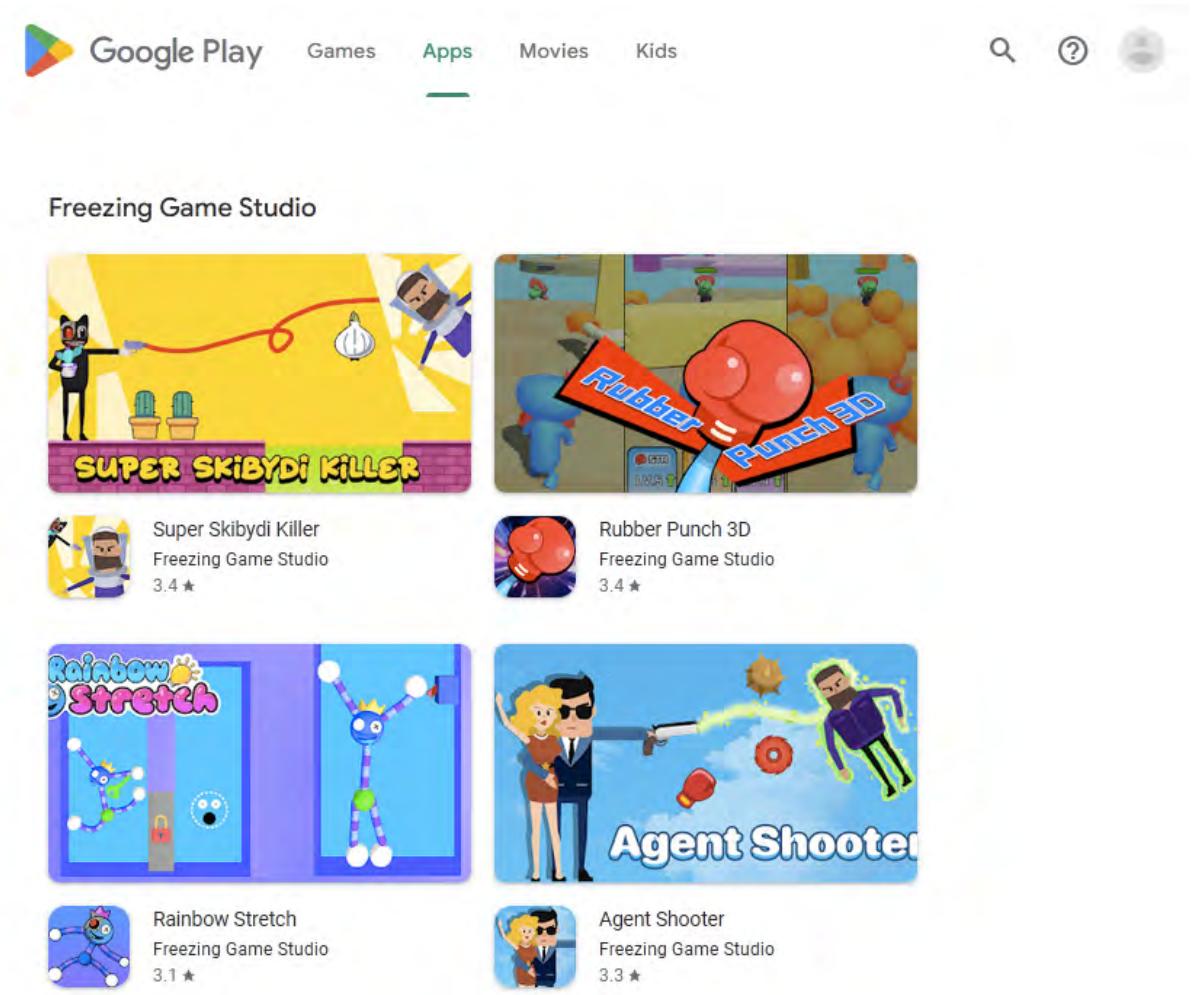
Пример сайта «юридической помощи», через который жертвы мошенников в сфере инвестиций якобы могли проконсультироваться с юристом и получить шанс вернуть утраченные деньги:



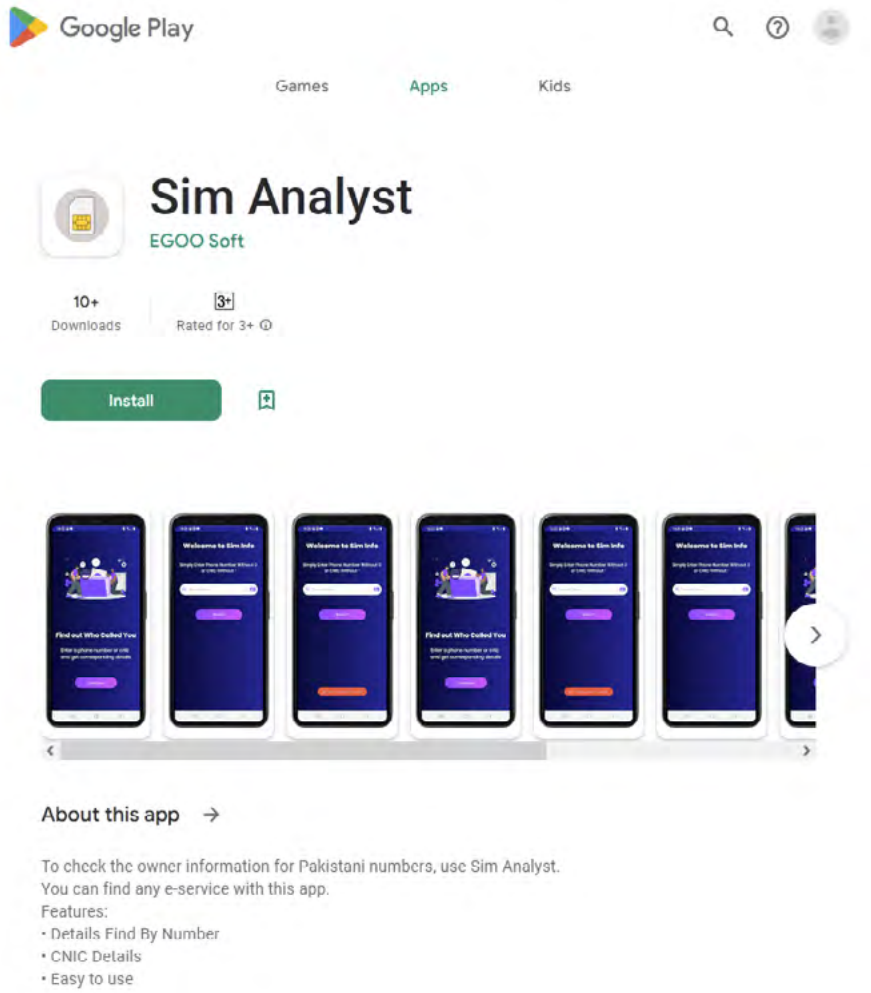
Вирусная лаборатория компании «Доктор Веб» в 2023 году также выявила в Google Play ряд других вредоносных программ. В их числе были трояны нового семейства Android.Proxy.4gproxy, которые превращали зараженные устройства в прокси-серверы и незаметно передавали через них сторонний трафик. В эти вредоносные программы была встроена утилита 4gproxy (добавлена в вирусную базу Dr.Web как потенциально опасное ПО Tool.4gproxy), которая позволяет использовать Android-устройства в качестве прокси-сервера. Она не является вредоносной и может применяться в безобидных целях. Однако в случае с троянами Android.Proxy.4gproxy работа с прокси выполнялась без участия пользователей и их явного согласия.



Кроме того, наши специалисты обнаружили несколько новых рекламных троянов семейства Android.HiddenAds — Android.HiddenAds.3785, Android.HiddenAds.3781, Android.HiddenAds.3786 и Android.HiddenAds.3787. После установки на Android-устройства они пытались скрыться от пользователей, подменяя свои значки на домашнем экране прозрачной версией и заменяли их названия на пустые. При этом они также могли выдавать себя за браузер Google Chrome, для чего использовали копию его значка для замены своих собственных. При нажатии на такой видоизмененный значок трояны вводили жертв в заблуждение, запуская браузер и одновременно продолжая работать в фоновом режиме. Тем самым они не только снижали свою заметность, но и имели больше шансов на длительную активность: если по какой-либо причине их работа остановилась бы, пользователи могли их перезапустить, думая, что запускают именно браузер. Подобная функциональность встречалась, например, и в трояне Android.HiddenAds.3766, который также распространялся через Google Play.



Другой выявленной угрозой стала троянская программа-шпион Android.Spy.1092.origin, созданная на базе утилиты дистанционного контроля (RAT) AhMyth Android Rat. Она распространялась под видом приложения Sim Analyst, с помощью которого пакистанские пользователи якобы могли находить информацию о других абонентах по номерам их телефонов.

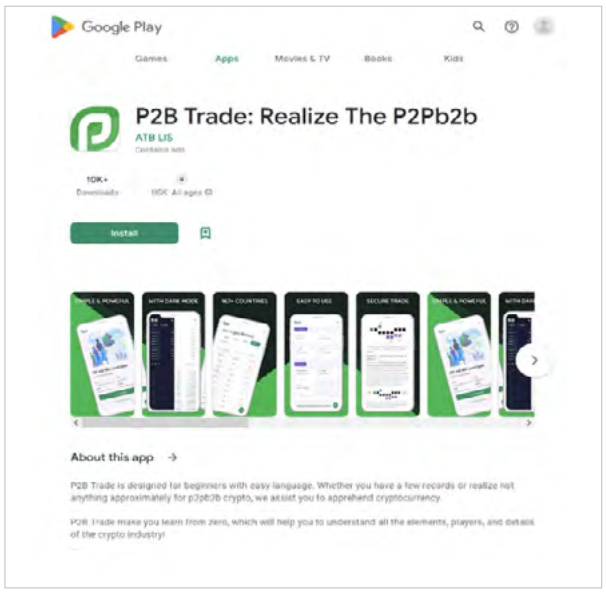


Стандартная версия шпионской утилиты AhMyth Android Rat предоставляет широкую функциональность. Например, она позволяет отслеживать местоположение устройства, фотографировать через встроенную камеру и записывать окружение через микрофон, перехватывать СМС, а также получать информацию о звонках и контактах в телефонной книге. Однако поскольку распространяемые через Google Play приложения имеют ограничение доступа к ряду чувствительных функций, у найденной нашими вирусными аналитиками версии шпиона возможности оказались скромнее. Он мог отслеживать местоположение устройства, похищать содержимое уведомлений, различные медиафайлы, такие как фото и видео, а также файлы, которые были переданы через мессенджеры и хранились локально на устройстве.

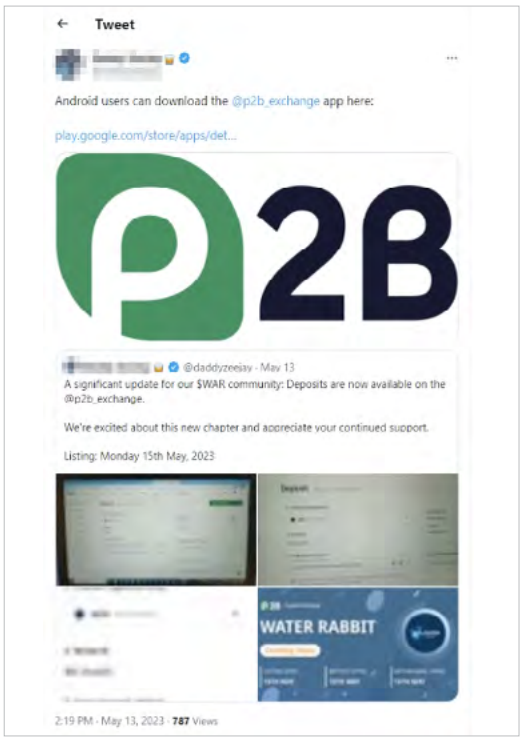
«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

Также наши специалисты обнаружили в Google Play троянскую программу Android.CoinSteal.105, предназначенную для кражи криптовалют. Злоумышленники пытались выдать ее за официальное приложение криптобиржи P2B, P2B official, распространяя под схожим именем — P2B Trade: Realize The P2Pb2b.

На изображении слева — страница поддельной программы, справа — оригинала.



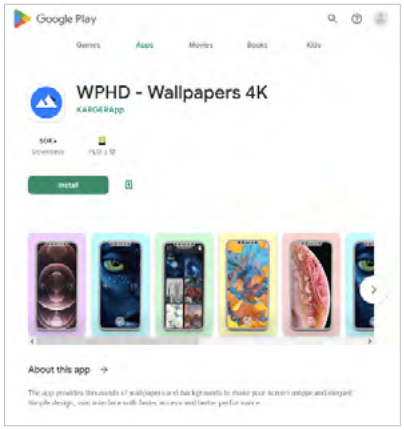
При этом подделку даже рекламировали криптоблогеры, в результате чего число ее установок оказалось вдвое больше, чем у настоящего приложения.

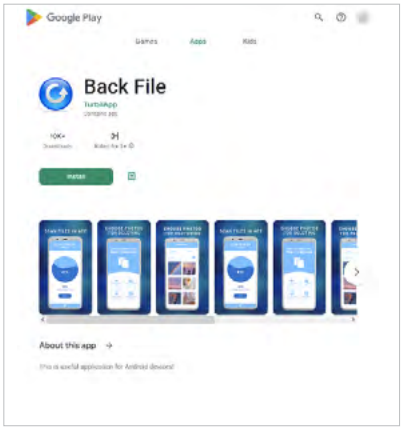


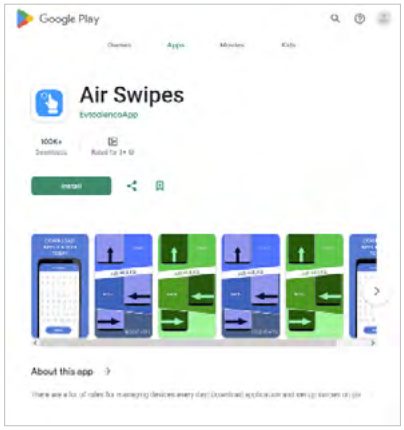
«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

При запуске Android.CoinSteal.105 открывал в WebView заданный злоумышленниками сайт системы распределения трафика, с которого выполнялась цепочка перенаправлений на другие интернет-ресурсы. Например, он загружал официальный сайт криптобиржи P2B, https://p2pb2b.com. Троян внедрял в него JS-скрипты, с помощью которых подменял адреса криптокошельков, вводимых пользователями для вывода криптовалют. При этом целевыми потенциально могли быть и другие веб-сайты — мошеннические, сайты с рекламой и т. д.

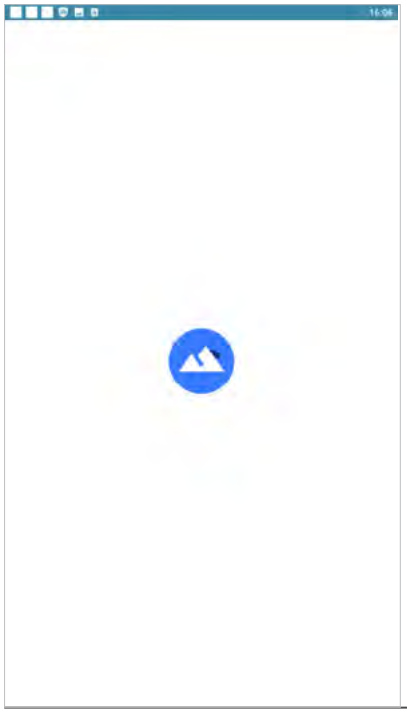
Среди выявленных вирусной лабораторией «Доктор Веб» угроз в Google Play оказались и новые трояны семейства Android.Subscription — Android.Subscription.19, Android.Subscription.20 и Android.Subscription.21. Они распространялись под видом безобидных программ и загружали сайты партнерских сервисов для подписки владельцев Android-устройств на платные услуги. Такие трояны либо подключают услугу самостоятельно, либо предлагают потенциальным жертвам указать номер мобильного телефона.

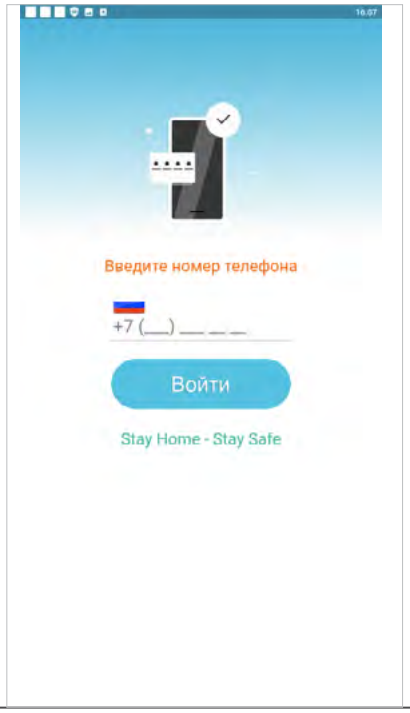


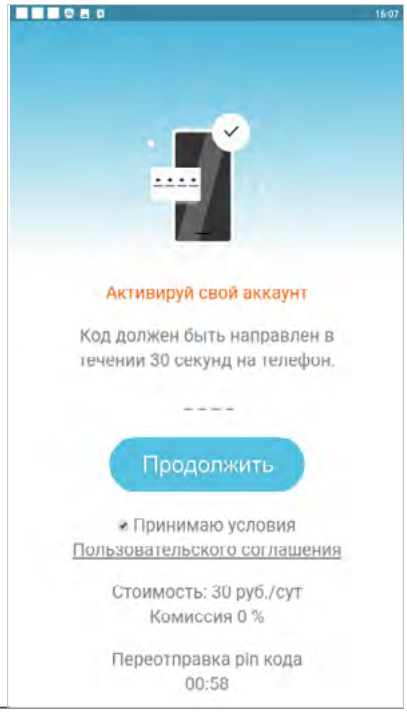




Примеры сайтов, загружаемых этими вредоносными приложениями для подключения платных сервисов:



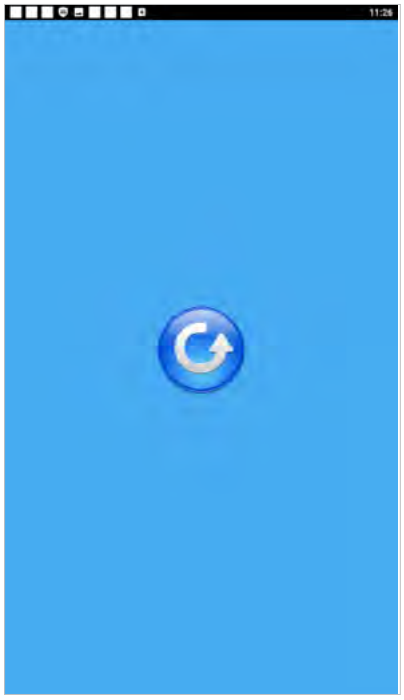


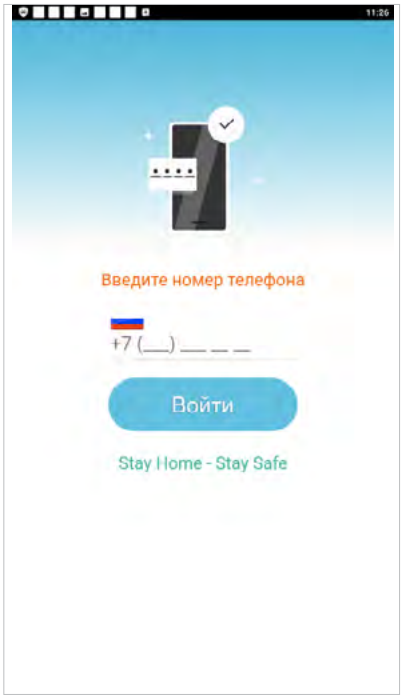


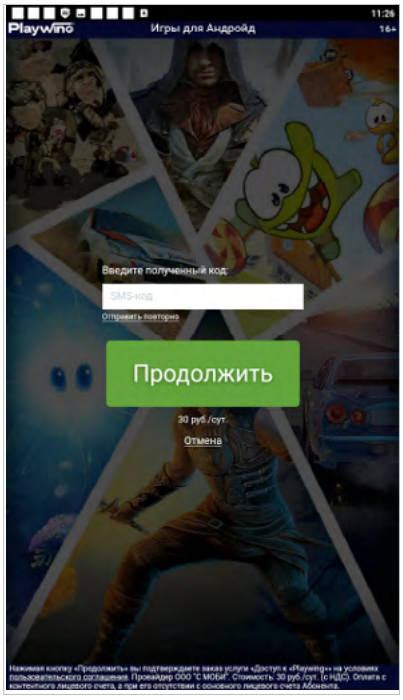
Узнайте больше

Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека

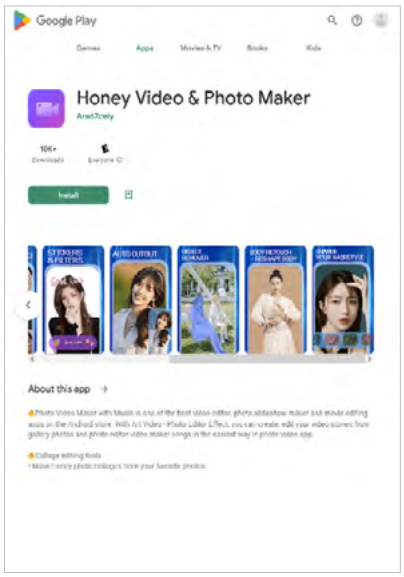
«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

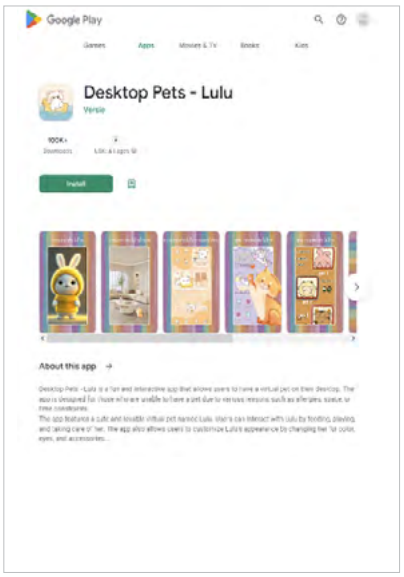


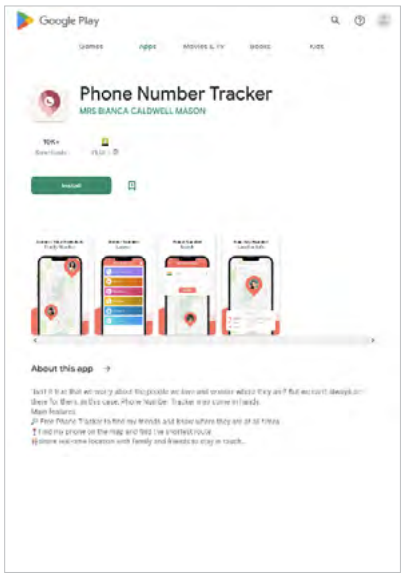




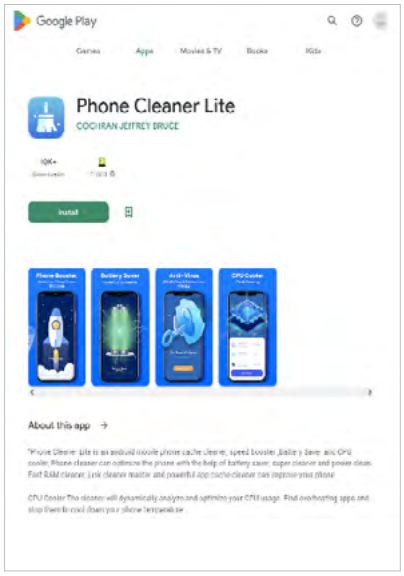
Вместе с тем в течение 2023 года в Google Play выявлялись и другие вредоносные приложения, которые подписывали пользователей на платные услуги, в частности — свыше 20 троянов семейств Android.Joker и Android.Harly. Среди них были Android.Joker.1991, Android.Joker.2000, Android.Joker.2117, Android.Joker.2152, Android.Joker.2176, Android.Joker.2217, Android.Harly.13, Android.Harly.25, Android.Harly.66, Android.Harly.80 и другие.

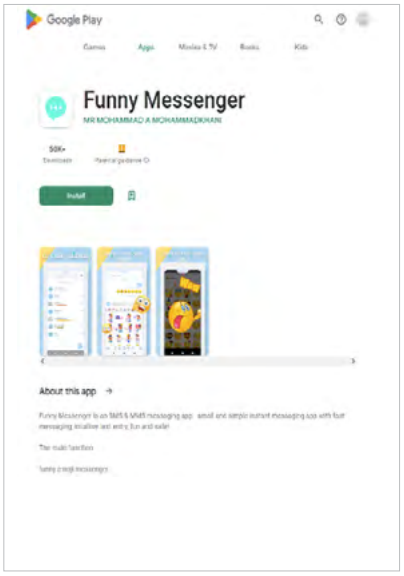


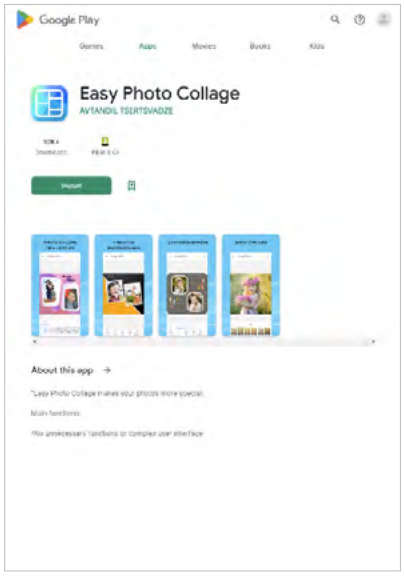




«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год







Банковские трояны

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в 2023 году число выявленных банковских троянов снизилось на 46,97% по сравнению с предыдущим годом. При этом их доля от общего числа обнаруженных на защищаемых устройствах вредоносных программ составила 3,58%, что на 0,84 п. п. меньше, чем годом ранее. Наибольшая активность банковских троянов пришлась на первое полугодие с максимальным числом детектирований в январе. После резкого спада в феврале их активность вновь начала расти, достигнув локального пика уже в апреле. Вслед за очередным снижением числа атак в мае количество выявляемых банковских троянов до конца года сохранялось примерно на одном уровне.

В течение 2023 года сохранялась активность наиболее популярных банковских троянов, которые киберпреступники применяли годом ранее. Так, фиксировались атаки с использованием семейств Anubis (Android.BankBot.670.origin, Android.BankBot.794.origin,

Android.BankBot.967.origin), Coper, S.O.V.A. (Android.BankBot.992.origin), Hydra (Android.BankBot.1048.origin), Ermac (Android.BankBot.970.origin, Android.BankBot.1037.origin) и Alien (Android.BankBot.745.origin, Android.BankBot.873.origin, Android.BankBot.1078.origin). Злоумышленники также распространяли вредоносные программы Cerberus (Android.BankBot.8705, Android.BankBot.1052.origin), Sharkbot (Android.BankBot.977.origin) и GodFather (Android.BankBot.1064.origin, Android.BankBot.1077.origin).

В странах Латинской Америки распространение вновь получили банковские трояны Banbra (Android.BankBot.1073.origin), а пользователи из Бразилии также сталкивались с семейством PixPirate (Android.BankBot.1026.origin).

Распространенное семейство MoqHao (Android.Banker.5063, Android.Banker.487.origin, Android.Banker.533.origin, Android.Banker.657.origin), география атак которого охватывает множество стран, активно применялось против пользователей Android из Юго-Восточной Азии и Азиатско-Тихоокеанского региона. При этом южнокорейские пользователи также сталкивались с различными представителями семейств Fakecalls (Android.BankBot.761.origin, Android.BankBot.919.origin, Android.BankBot.1002.origin) и Wroba (Android.Banker.360.origin). Семейство Wroba (Android.BankBot.907.origin) использовалось для атак и на жителей Японии. А владельцев Android-устройств из Китая атаковал троян Android.Banker.480.origin.

Вместе с тем наши специалисты наблюдали новые тенденции в атаках банковских троянов. Одной из наиболее заметных стало появление новых семейств, многие из которых были нацелены на пользователей из России. К таким вредоносным приложениям относились Android.Banker.5127 и Android.Banker.5273, созданные с помощью программы-планировщика событий Tasker, Android.Banker.597.origin, Android.Banker.592.origin и Android.Banker.5235, маскировавшиеся под всевозможные сервисы, например — KoronaPay, Дайвинчик 18+, Yandex, Ростелеком и OnlyFans, и ряд других троянов.

В атаках на российских пользователей также применялись Android.Banker.637.origin, Android.Banker.632.origin, Android.Banker.633.origin и Android.Banker.635.origin — их злоумышленники распространяли под видом самых разнообразных программ. Например, выдавали их за ПО, якобы имеющее отношение к различным стриминговым сервисам (в частности STAR), программы категории «для взрослых», модификации официального Android-клиента социальной сети ВКонтакте (VK-моды), тематические программы по сериалу «Слово Пацана. Кровь на асфальте», который в 2023 году получил популярность в России и странах бывшего СССР, и т. п.

Кроме того, распространение в России получили банковские трояны Android.BankBot.1062.origin, Android.BankBot.1093.origin и Android.BankBot.1098.origin, которые впоследствии расширили географию атак на пользователей из Узбекистана.

В то же время вирусные аналитики «Доктор Веб» отметили появление большого числа банковских троянов, нацеленных на иранских пользователей. Среди них были Android.BankBot.1088.origin, Android.BankBot.14871, Android.BankBot.1083.origin, Android.Banker.5292, Android.Banker.5233, Android.Banker.5276 и Android.Banker.5379. Кроме того, злоумышленники распространяли Android-банкеров Tambir (Android.BankBot.1099.origin), предназначенных для атак на турецких владельцев Android-устройств.

Заметная активность наблюдалась и со стороны банковских троянов семейства Rewardsteal (Android.Banker.562.origin, Android.Banker.5138, Android.Banker.5141, Android.Banker.588.origin, Android.Banker.611.origin). Среди них чаще всего встречались модификации, нацеленные на пользователей кредитных организаций ICICI Bank, HDFC Bank, SBI, Axis bank, Citi bank, RBL bank.

Перспективы и тенденции

Поскольку основной мотивацией киберпреступников остается материальная выгода, в 2024 году следует ожидать появления новых вредоносных программ, помогающих им увеличить нелегальный заработок. Наиболее вероятными кандидатами на эту роль станут очередные рекламные троянские программы, банковские трояны, мошеннические и шпионские приложения.

Сохранится угроза появления новых вредоносных программ в каталоге Google Play, при этом нельзя исключать более активного использования злоумышленниками других источников распространения угроз, в частности вредоносных сайтов.

С большой вероятностью стоит ожидать появления и новых троянов, нацеленных на кражу криптовалют у владельцев как Android-устройств, так и устройств под управлением iOS.

Чтобы защититься от атак злоумышленников, обезопасить деньги и конфиденциальные данные, установите антивирус Dr.Web на все поддерживаемые устройства. Компания «Доктор Веб» со своей стороны продолжит следить за тенденциями в мире киберугроз и информировать наших пользователей о важных событиях в сфере информационной безопасности.

Индикаторы компрометации

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2023 год

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