«Доктор Веб»:
обзор вирусной активности для мобильных устройств в январе 2023 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2023 года

2 марта 2023 года

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в январе 2023 года пользователи стали чаще сталкиваться с рекламными троянскими приложениями. Наиболее распространенными среди них вновь оказались представители семейства Android.HiddenAds, при этом они обнаруживались на 18,04% чаще, чем в декабре прошлого года.

По сравнению с последним месяцем 2022-го также возросла активность банковских троянских приложений и программ-вымогателей. Первые обнаруживались на 2,63% чаще, вторые — на 20,71%. В то же время наблюдалось незначительное снижение активности вредоносных шпионских программ.

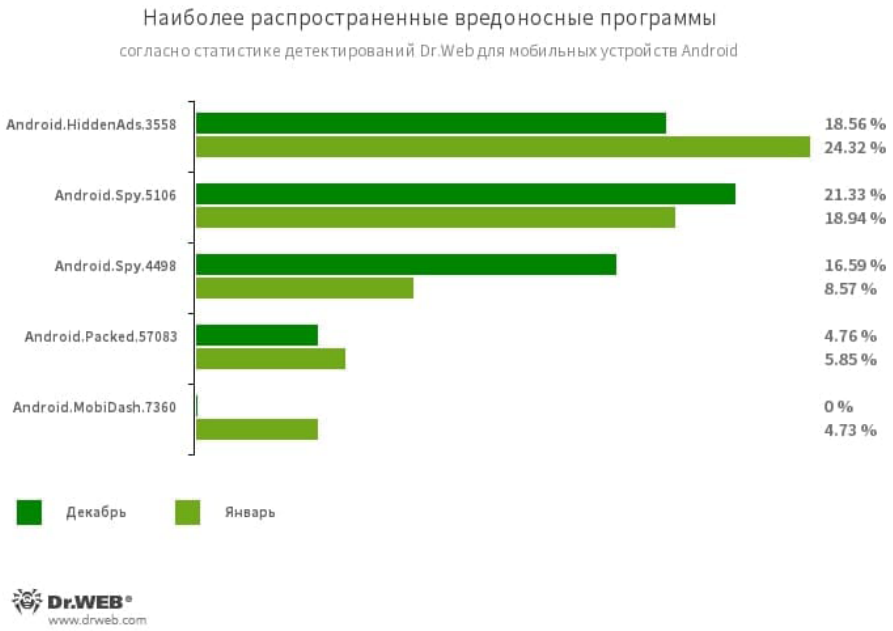
В течение месяца вирусная лаборатория компании «Доктор Веб» выявила в каталоге Google Play множество новых угроз, включая мошеннические приложения и троянские программы, которые подписывали пользователей на платные услуги.

ГЛАВНЫЕ ТЕНДЕНЦИИ ЯНВАРЯ

- Рост активности вредоносных программ, демонстрирующих рекламу
- Рост активности банковских троянских приложений и программ-вымогателей
- Снижение активности шпионских приложений
- Появление новых угроз в каталоге Google Play

«Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2023 года

По данным антивирусных продуктов Dr.Web для Android



Android.HiddenAds.3558

Троянская программа для показа навязчивой рекламы. Представители этого семейства часто распространяются под видом безобидных приложений и в некоторых случаях устанавливаются в системный каталог другими вредоносными программами. Попадая на Android-устройства, такие рекламные трояны обычно скрывают от пользователя свое присутствие в системе — например, «прячут» значок приложения из меню главного экрана.

Android.Spy.5106

Android.Spy.4498

Детектирование различных вариантов трояна, который представляет собой видоизмененные версии неофициальных модификаций приложения WhatsApp. Эта вредоносная программа может похищать содержимое уведомлений, предлагать установку программ из неизвестных источников, а во время использования мессенджера — демонстрировать диалоговые окна с дистанционно настраиваемым содержимым.

Android.Packed.57083

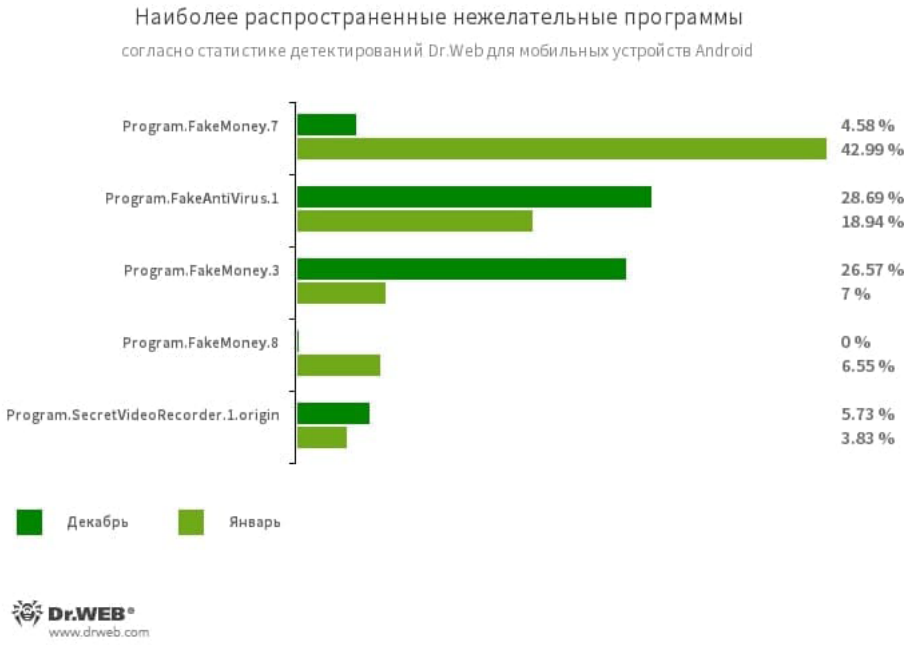
Детектирование вредоносных приложений, защищенных программным упаковщиком ApkProtector. Среди них встречаются банковские трояны, шпионское и другое вредоносное ПО.

Android.MobiDash.7360

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

«Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2023 года

По данным антивирусных продуктов Dr.Web для Android



Program.FakeMoney.7

Program.FakeMoney.3

Program.FakeMoney.8

Детектирование приложений, якобы позволяющих зарабатывать на выполнении тех или иных действий или заданий. Они 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

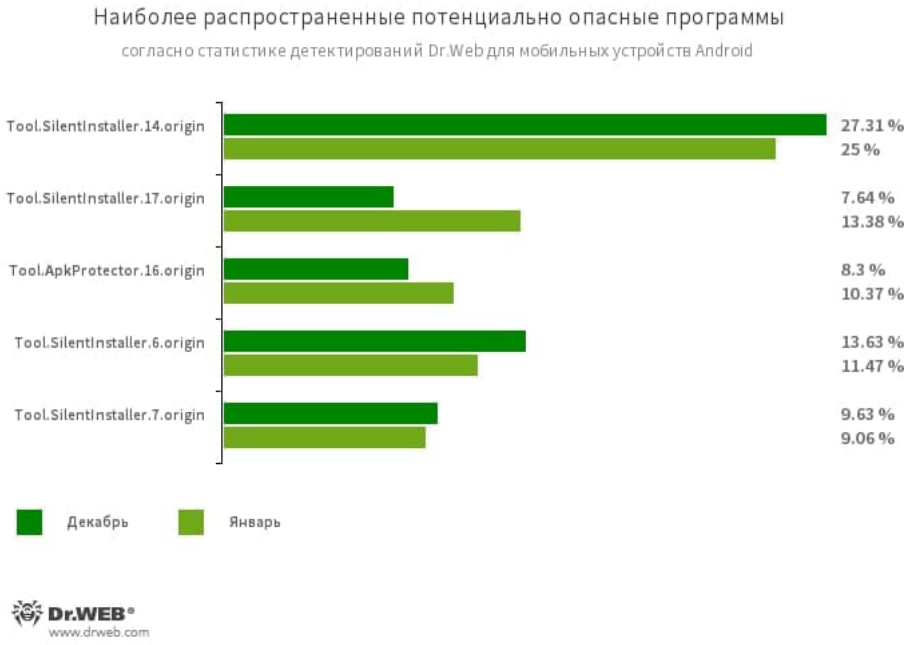
Детектирование рекламных программ, которые имитируют работу антивирусного ПО. Такие программы могут сообщать о несуществующих угрозах и вводить пользователей в заблуждение, требуя оплатить покупку полной версии.

Program.SecretVideoRecorder.1.origin

Детектирование различных версий приложения для фоновой фото- и видеосъемки через встроенные камеры Android-устройств. Эта программа может работать незаметно, позволяя отключить уведомления о записи, а также изменять значок и описание приложения на фальшивые. Такая функциональность делает ее потенциально опасной.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2023 года

По данным антивирусных продуктов Dr.Web для Android



Tool.SilentInstaller.14.origin

Tool.SilentInstaller.17.origin

Tool.SilentInstaller.6.origin

Tool.SilentInstaller.7.origin

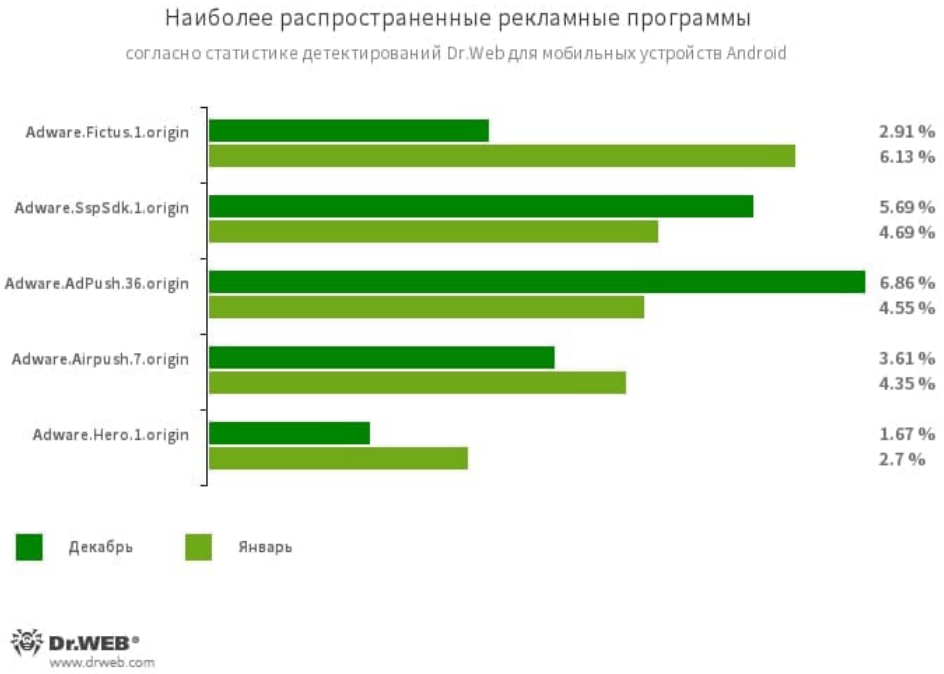
Потенциально опасные программные платформы, которые позволяют приложениям запускать APK-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

Tool.ApkProtector.16.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.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2023 года

По данным антивирусных продуктов Dr.Web для Android



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.SspSdk.1.origin

Специализированный рекламный модуль, встраиваемый в Android-приложения. Он демонстрирует рекламу, когда содержащие его программы закрыты. В результате пользователям сложнее определить источник надоедливых объявлений.

Adware.AdPush.36.origin

Представитель семейства рекламных модулей, которые могут быть интегрированы в Android-программы. Он демонстрирует рекламные уведомления, вводящие пользователей в заблуждение. Например, такие уведомления могут быть похожи на сообщения от операционной системы. Кроме того, модули этого семейства собирают ряд конфиденциальных данных, а также способны загружать другие приложения и инициировать их установку.

По данным антивирусных продуктов Dr.Web для Android

Adware.Airpush.7.origin

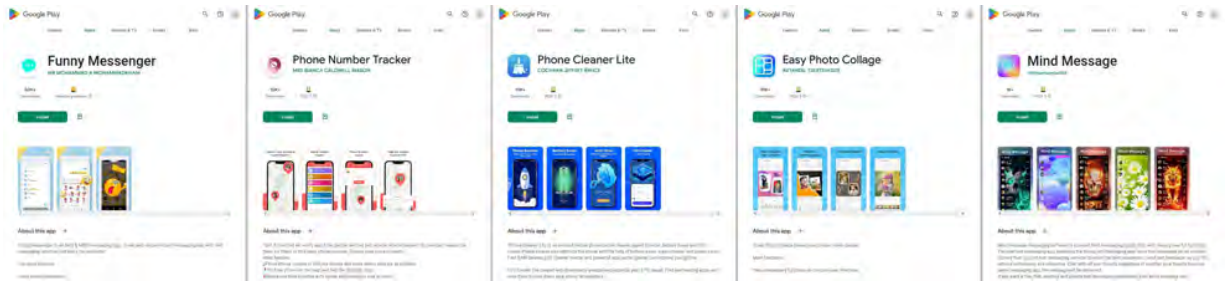
Представитель семейства рекламных модулей, встраиваемых в Android-приложения и демонстрирующих разнообразную рекламу. В зависимости от их версии и модификации это могут быть рекламные уведомления, всплывающие окна или баннеры. С помощью данных модулей злоумышленники часто распространяют вредоносные программы,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

Adware.Hero.1.origin

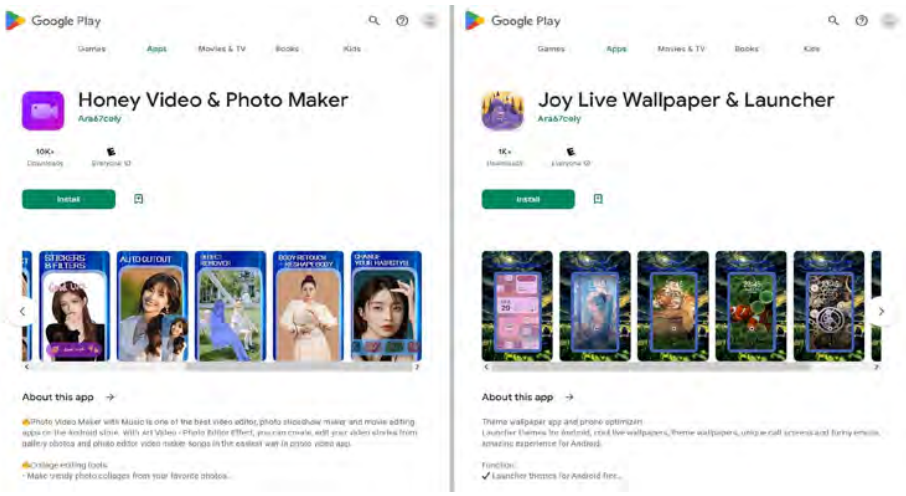
Один из компонентов семейства модульных рекламных приложений, которые демонстрируют нежелательную рекламу в виде push-уведомлений и баннеров на экране Android-устройств. Кроме того, они способны устанавливать и удалять программы при наличии соответствующих системных полномочий.

Угрозы в Google Play

В январе 2023 года вирусная лаборатория компании «Доктор Веб» зафиксировала множество новых угроз в каталоге Google Play. Среди них — схожие по функциональности многокомпонентные троянские программы семейств Android.Joker и Android.Harly, подписывающие жертв на платные услуги. Первые загружают вспомогательные модули из интернета, в то время как вторые хранят их в зашифрованном виде среди собственных ресурсов. Так, получивший по классификации Dr.Web имя Android.Joker.1991 троян скрывался в приложении Phone Number Tracker для отслеживания местоположения абонентов по номерам телефонов. Вредоносная программа Android.Joker.1998 распространялась под видом утилиты Phone Cleaner Lite для оптимизации работы системы. Android.Joker.1999 и Android.Joker.2008 злоумышленники выдавали за СМС-мессенджеры Funny Messenger и Mind Message. А под видом редактора изображений Easy Photo Collage пользователи устанавливали трояна Android.Joker.2000.



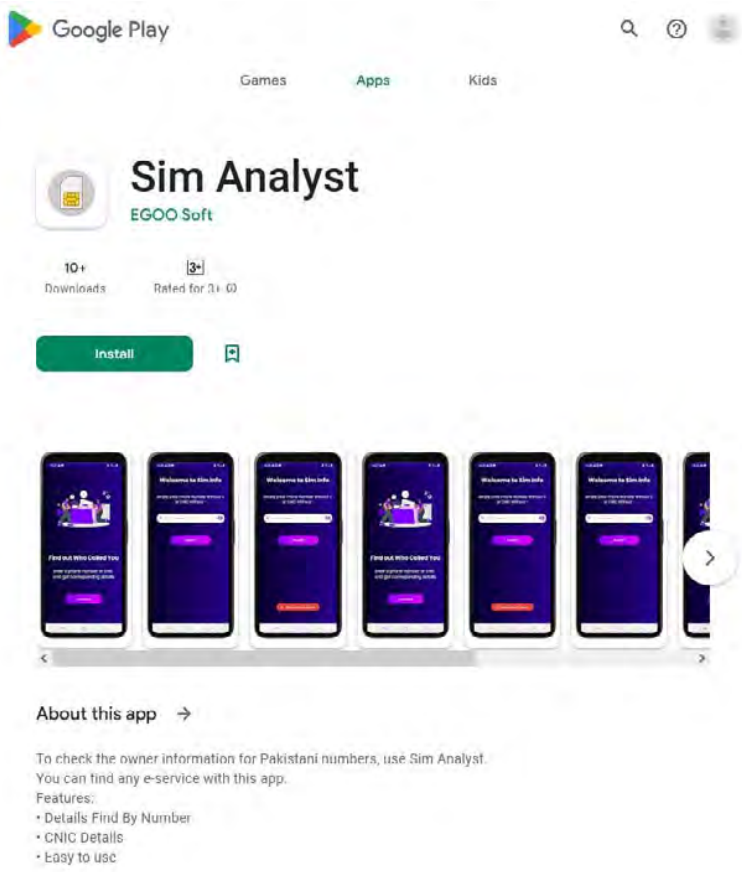
В свою очередь, Android.Harly.13 и Android.Harly.25 скрывались в видеоредакторе Honey Video & Photo Maker и альтернативном лончере Joy Live Wallpaper & Launcher соответственно.



Другой выявленной угрозой стала программа Sim Analyst, с помощью которой пакистанские пользователи якобы могли находить информацию о других абонентах по их номерам

Угрозы в Google Play

телефонов. На самом деле под видом этого инструмента злоумышленники распространяли шпионское приложение на базе утилиты дистанционного контроля (RAT) AhMyth Android Rat. Эта троянская программа была добавлена в вирусную базу Dr.Web как Android.Spy.1092.origin.



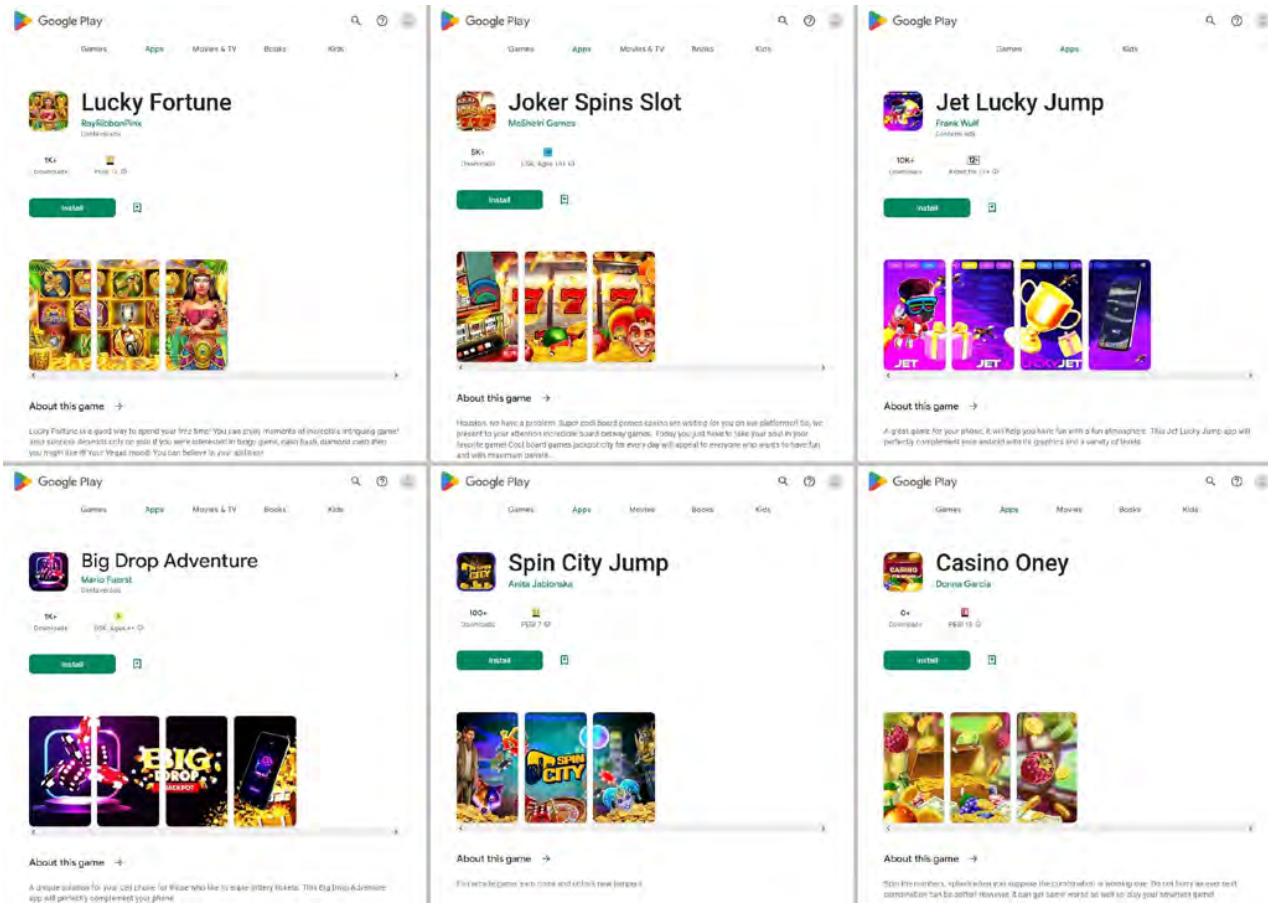
В базовом виде шпионская утилита AhMyth Android Rat обладает широким набором возможностей. Например, позволяет отслеживать местоположение устройства, фотографировать через встроенную камеру и записывать окружение через микрофон, перехватывать СМС, а также получать информацию о звонках и о контактах в телефонной книге. Однако поскольку распространяемые через Google Play приложения имеют ограничение доступа к ряду чувствительных функций, у данной версии шпиона возможности были скромнее. Так, он мог отслеживать местоположение устройства, похищать содержимое из уведомлений, различные медиафайлы, такие как фото и видео, а также файлы, которые были переданы через мессенджеры и хранились локально на устройстве.

Кроме того, наши специалисты обнаружили более двух десятков программ-подделок

«Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2023 года

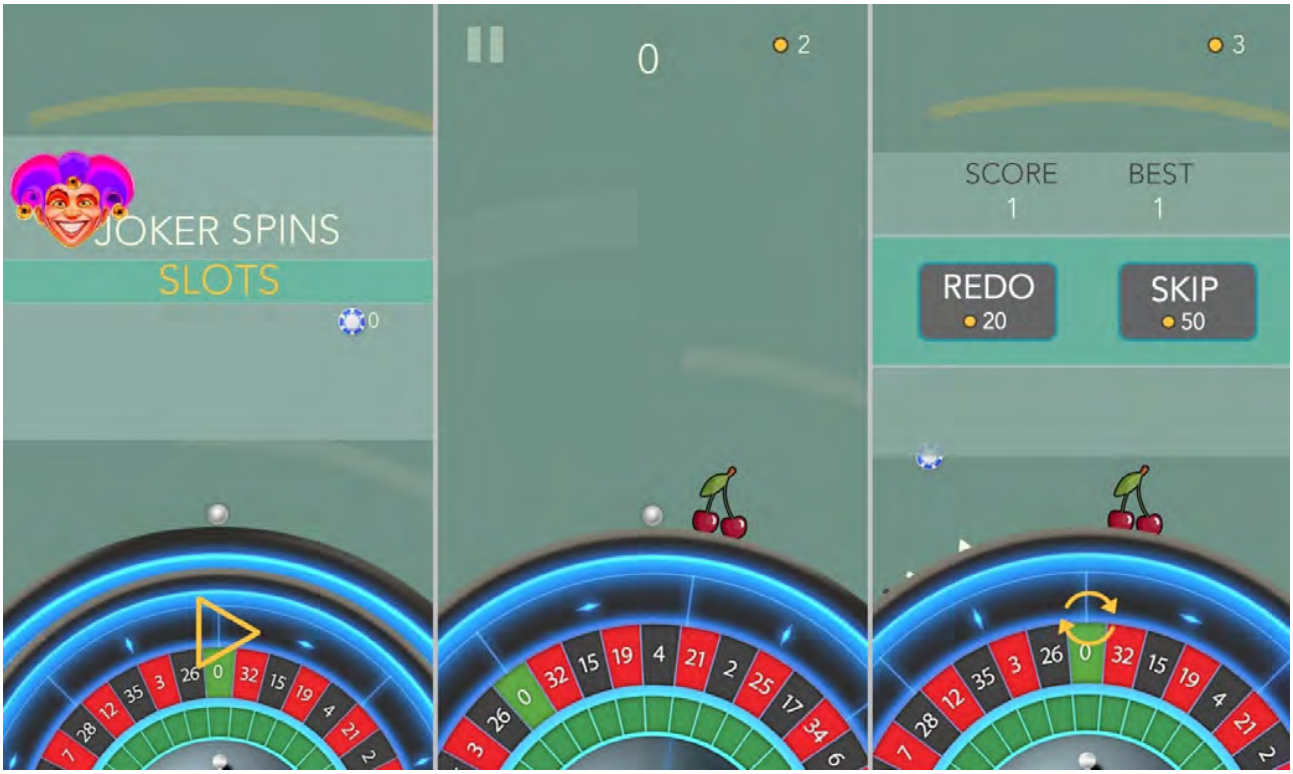
Угрозы в Google Play

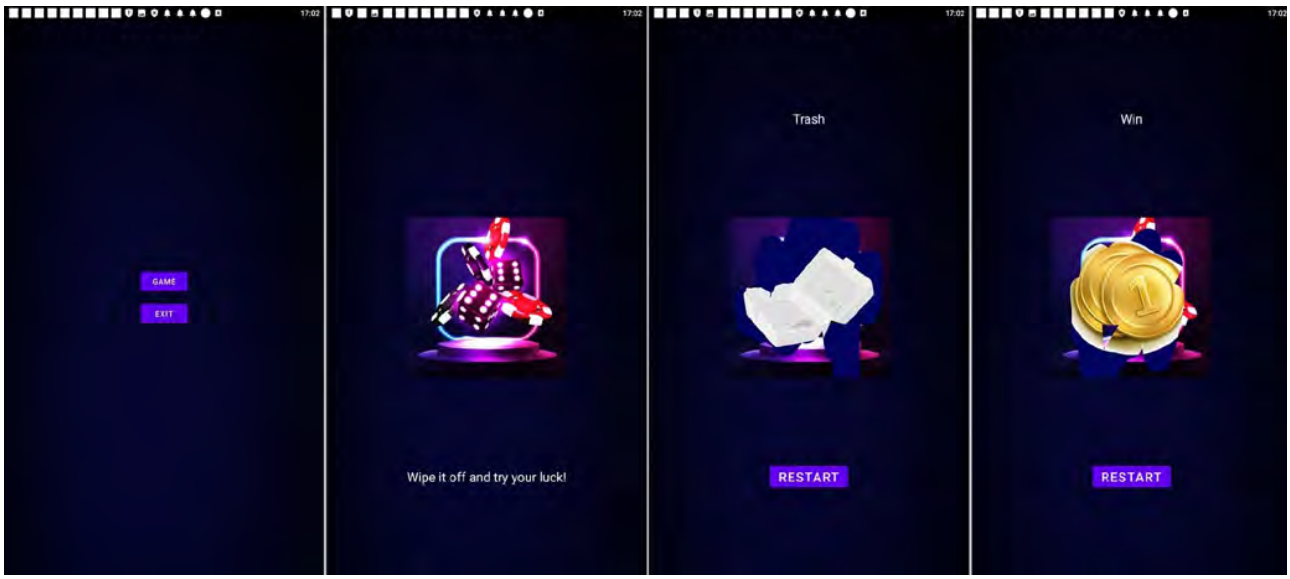
Android.FakeApp, которые злоумышленники использовали в мошеннических целях. Они распространялись под видом широкого спектра приложений и по команде удаленного сервера могли загружать различные веб-сайты, в том числе фишинговые.
Некоторые из этих программ преподносились в качестве игр:



При определенных условиях вместо ожидаемой функциональности они могли демонстрировать сайты онлайн-казино — например, если были установлены при переходе по специально сформированной ссылке из рекламного объявления.
Ниже представлены примеры такого поведения: в одних случаях пользователи видят игру, в других — сайты казино.

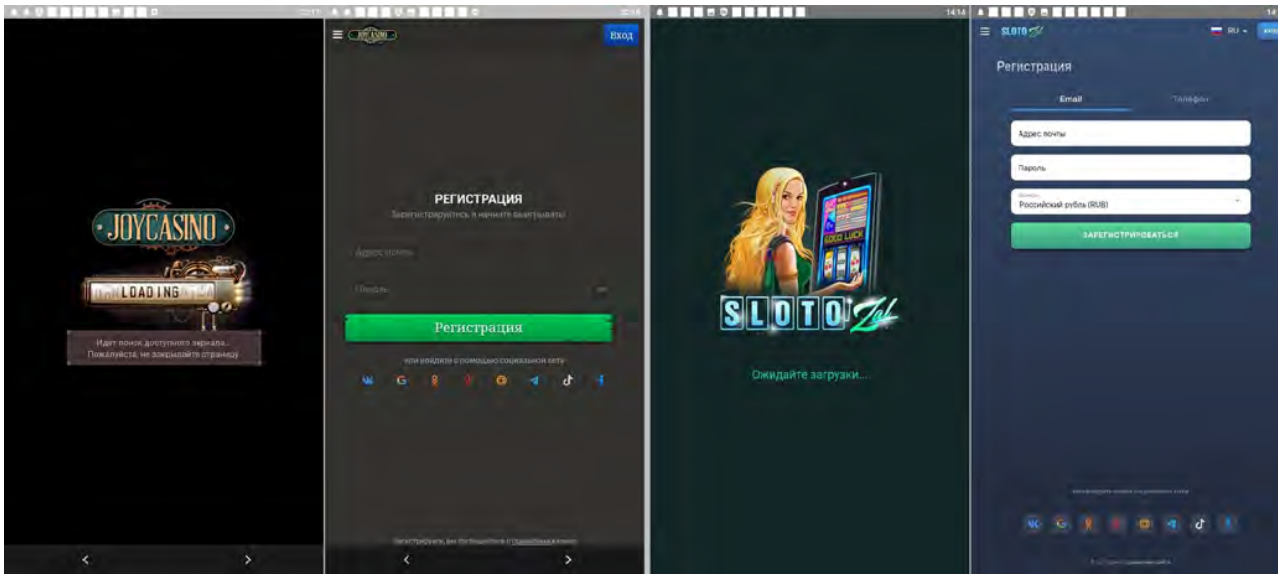
Угрозы в Google Play



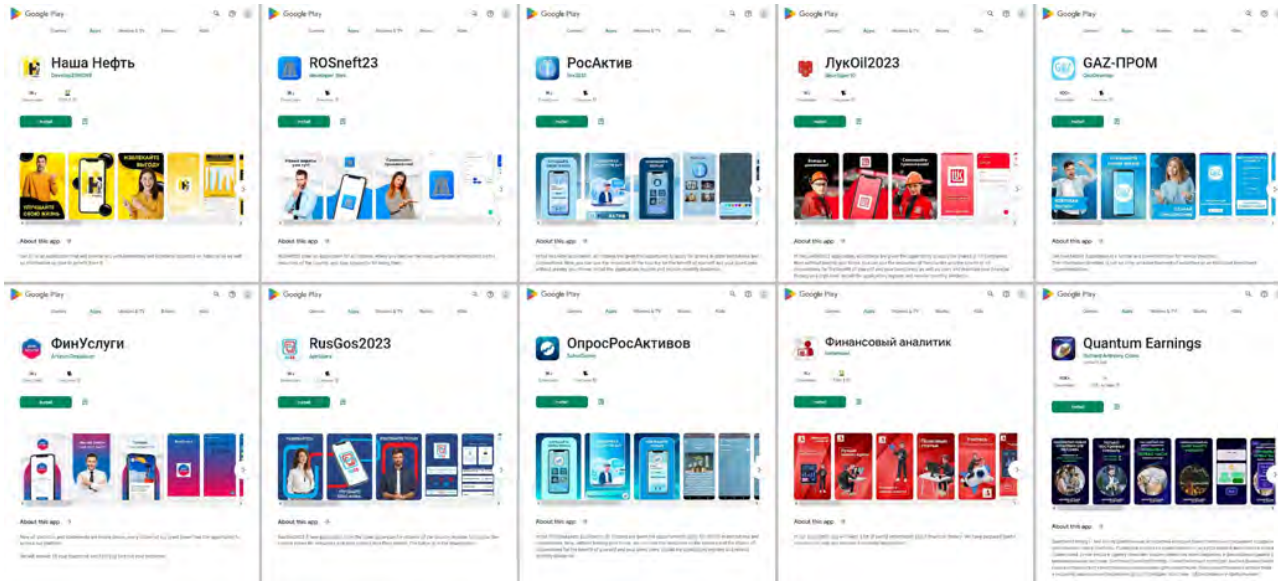


«Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2023 года

Угрозы в Google Play



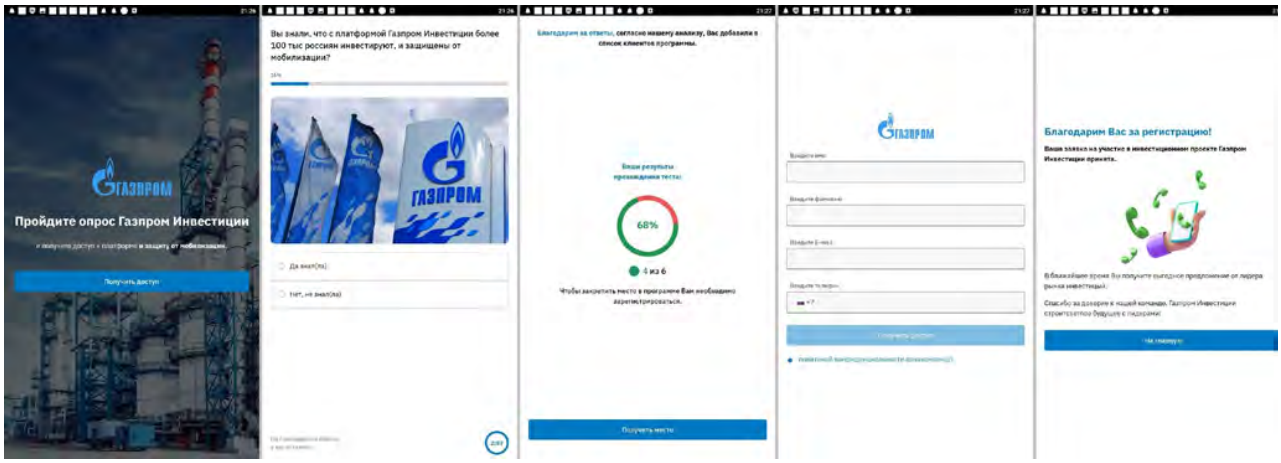
Другие приложения-подделки распространялись под видом финансовых приложений и инструментов для саморазвития. С их помощью пользователи якобы могли вести домашнюю бухгалтерию, участвовать в различных опросах, пройти обучение и повысить финансовую грамотность, начать инвестировать, либо получить бесплатные акции. На самом деле главной целью этих программ была загрузка мошеннических сайтов.



«Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2023 года

Угрозы в Google Play

Примеры загружаемых мошеннических сайтов представлены ниже. Потенциальным жертвам демонстрируется вводящая в заблуждение информация, либо предлагается пройти предварительный опрос. Затем — зарегистрировать учетную запись, указав персональные данные. В конце требуется ожидать звонка «специалиста» или поступления некоего «выгодного предложения».



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

Индикаторы компрометации

«Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2023 года

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 | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах

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