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

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

6 апреля 2023 года

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в феврале 2023 года возросла активность рекламных троянских приложений семейства Android.HiddenAds — на 26,95% по сравнению с январем. В то же время на 7,27% снизилась активность рекламных вредоносных программ Android.MobiDash.

Реже на защищаемых Dr.Web устройствах выявлялись банковские троянские приложения и программы-вымогатели — на 70,57% и 14,63% соответственно. Кроме того, на 33,93% снизилась активность шпионских троянских приложений, наиболее распространенными среди которых стали различные варианты трояна, атакующего пользователей некоторых неофициальных модификаций мессенджера WhatsApp.

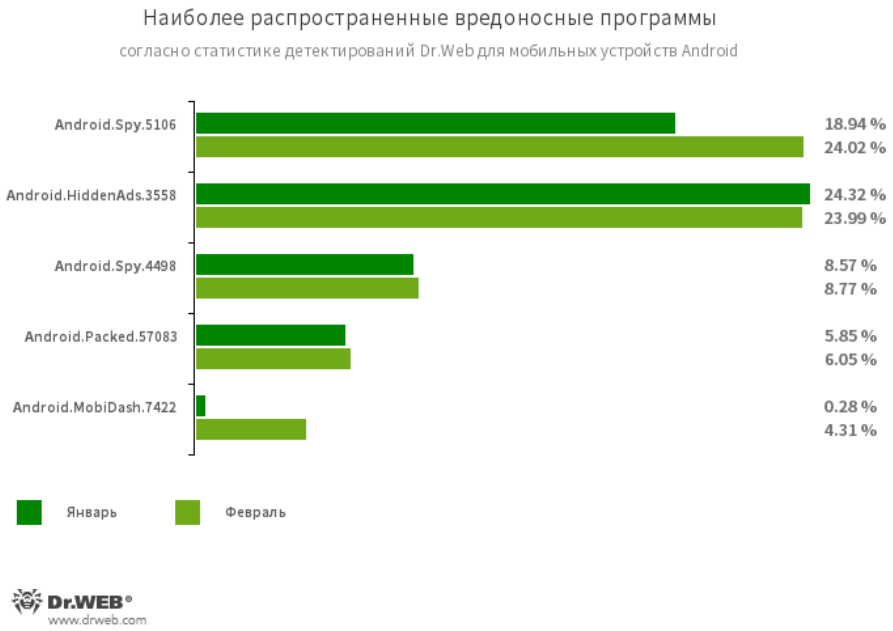
В течение февраля вирусная лаборатория компании «Доктор Веб» выявила в каталоге Google Play свыше 70 вредоносных приложений. Большинство принадлежало к семейству мошеннических программ Android.FakeApp. Были среди них и троянские приложения, которые подписывали жертв на платные услуги.

ГЛАВНЫЕ ТЕНДЕНЦИИ ФЕВРАЛЯ

- Рост активности рекламных троянских программ
- Снижение активности банковских троянских приложений и программ-вымогателей
- Снижение активности шпионских приложений
- Выявление множества угроз в каталоге Google Play

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

По данным антивирусных продуктов Dr.Web для Android



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.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.Packed.57083

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

Android.MobiDash.7422

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 феврале 2023 года

По данным антивирусных продуктов Dr.Web для Android

Program.FakeMoney.7

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.wSpy.1.origin

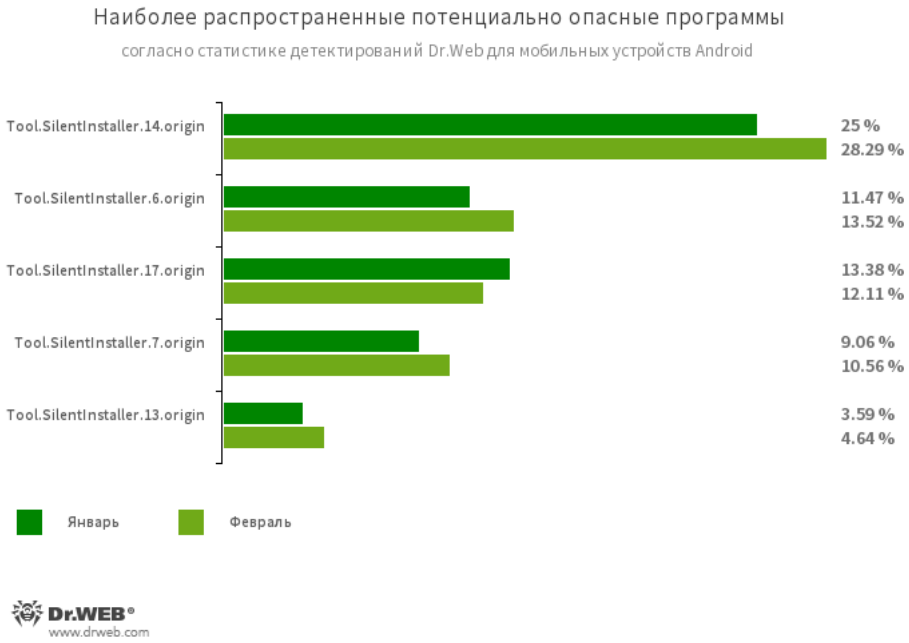
Коммерческая программа-шпион для скрытого наблюдения за владельцами Android-устройств. Она позволяет читать переписку (сообщения в популярных мессенджерах и СМС), прослушивать окружение, отслеживать местоположение устройства, следить за историей веб-браузера, получать доступ к телефонной книге и контактам, фотографиям и видео, делать скриншоты экрана и фотографии через камеру устройства, а также имеет функцию кейлоггера.

Program.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 феврале 2023 года

По данным антивирусных продуктов Dr.Web для Android

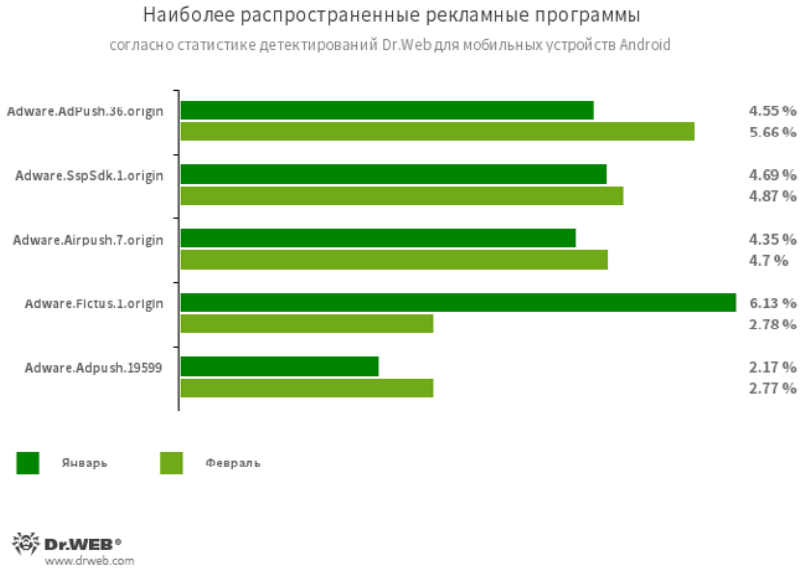


Tool.SilentInstaller.14.origin
Tool.SilentInstaller.6.origin
Tool.SilentInstaller.17.origin
Tool.SilentInstaller.7.origin
Tool.SilentInstaller.13.origin

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

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

По данным антивирусных продуктов Dr.Web для Android



Adware.AdPush.36.origin
Adware.Adpush.19599

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, данные модули собирают ряд конфиденциальных данных, а также способны загружать другие приложения и инициировать их установку.

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.Airpush.7.origin

Представитель семейства рекламных модулей, встраиваемых в Android-приложения и демонстрирующих 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.

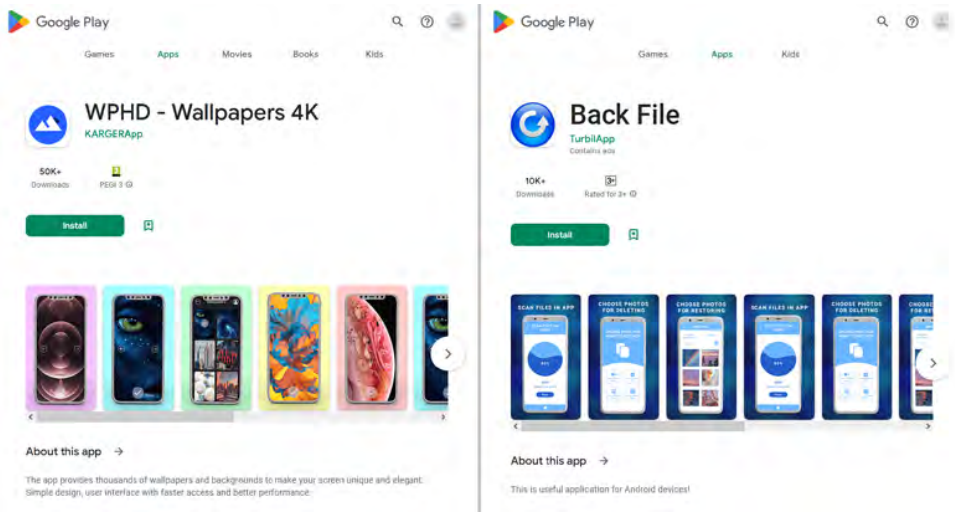
Adware.Fictus.1.origin

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.

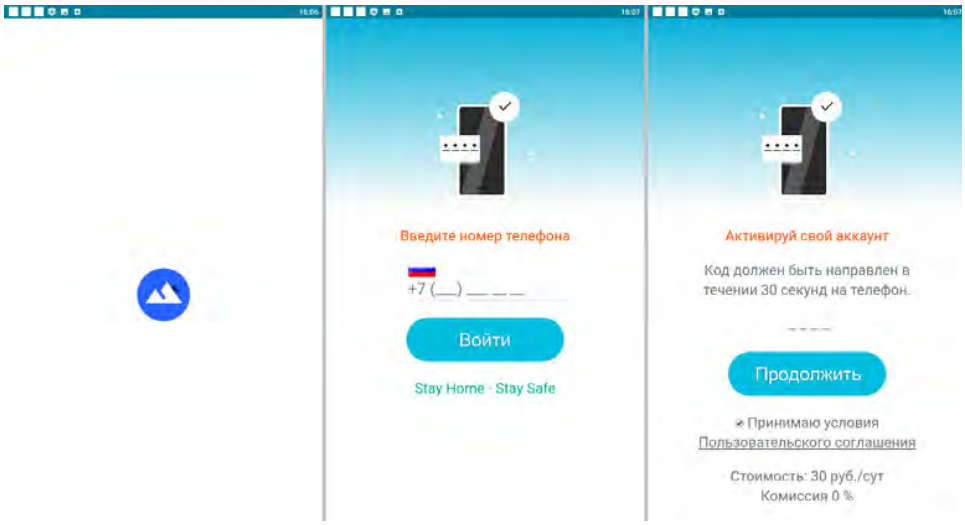
«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2023 года

Угрозы в Google Play

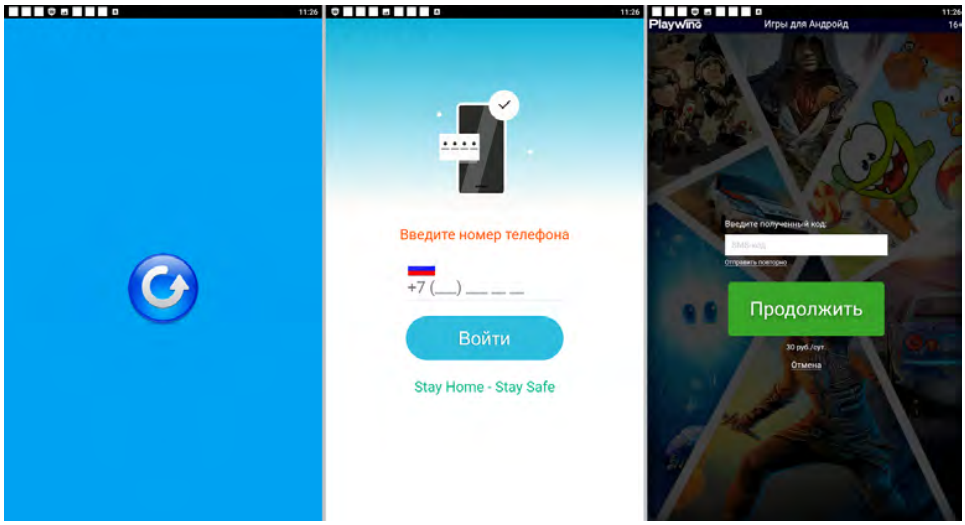
В феврале 2023 года вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play очередные вредоносные приложения, подписывавшие владельцев Android-устройств на платные услуги. Так, троянские программы семейства Android.Subscription — Android.Subscription.19 и Android.Subscription.20 — распространялись под видом сборника изображений WPHD - Wallpapers 4K и утилиты для восстановления удаленных файлов Back File.



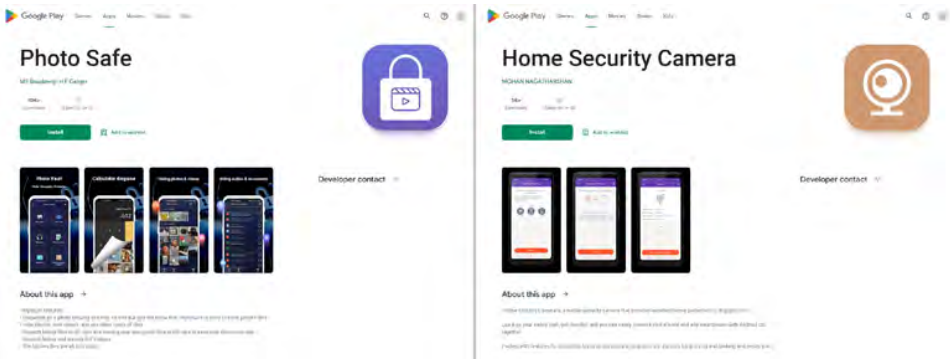
Вредоносные приложения этого типа при запуске загружают сайты платных сервисов и пытаются оформить подписку либо автоматически, либо предлагая пользователям указать номер мобильного телефона. Ниже представлены примеры веб-сайтов, которые обнаруженные троянские программы загружали с целью оформления платной подписки:



Угрозы в Google Play



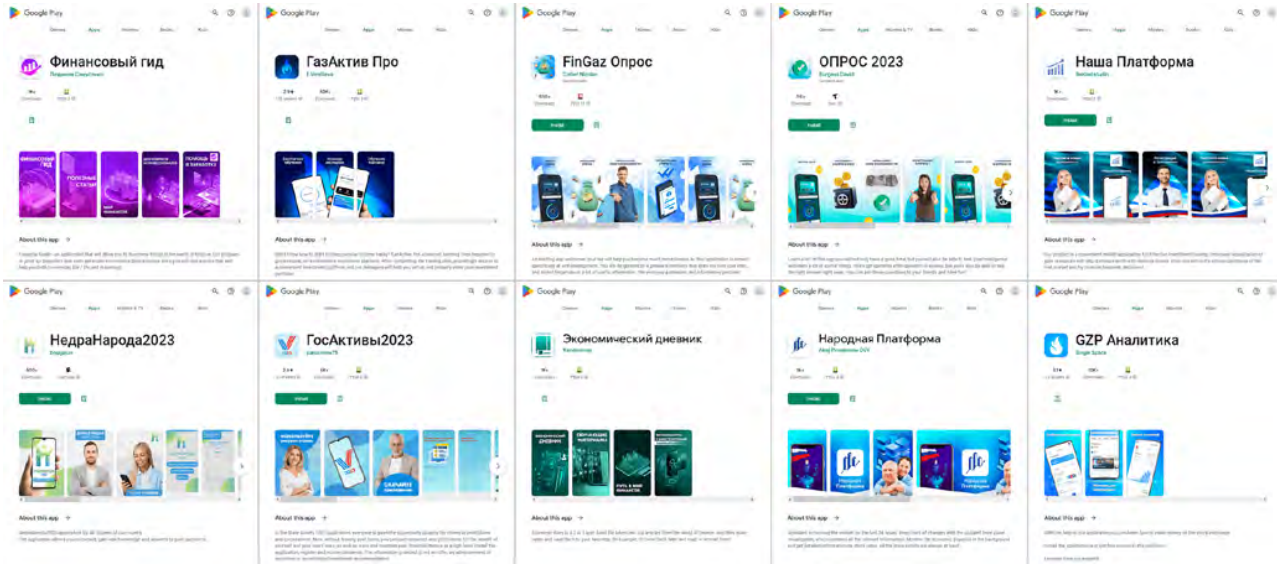
А новые представители семейства Android.Joker, получившие имена Android.Joker.2038 и Android.Joker.2039, скрывались в приложении Photo Safe для защиты файлов от несанкционированного доступа и в программе Home Security Camera, которая позволяла управлять камерами наблюдения через смартфон или использовать само устройство в режиме видеонаблюдения. Эти вредоносные программы загружают сайты целевых сервисов незаметно, после чего самостоятельно подключают жертв к платным услугам.



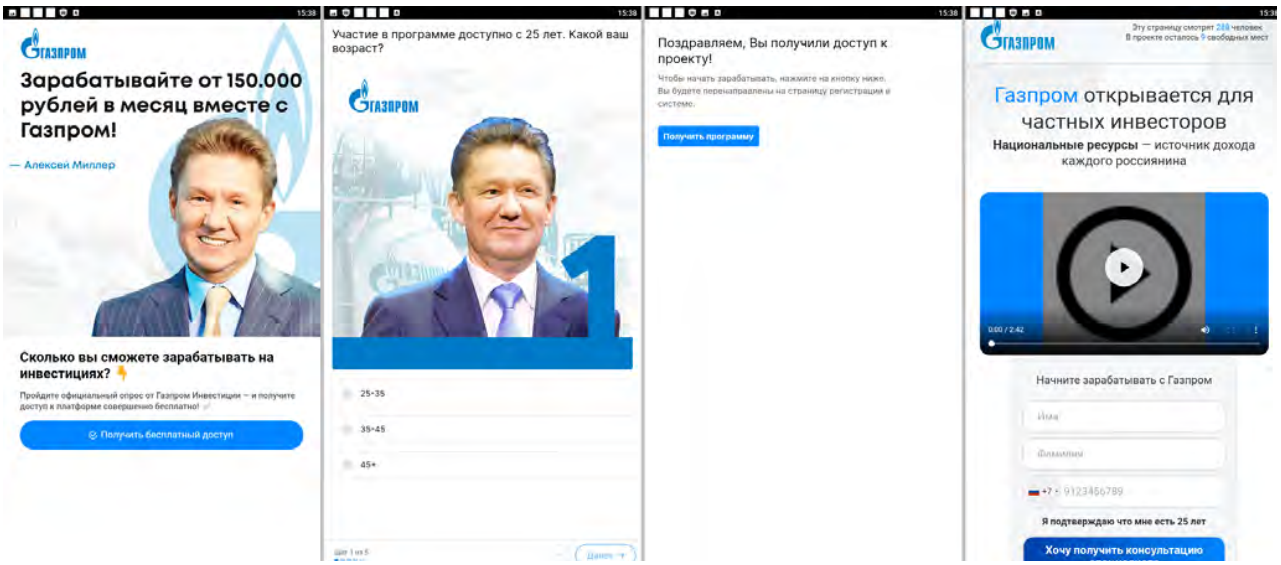
Кроме того, наши специалисты обнаружили десятки программ-подделок семейства Android.FakeApp, которые распространялись под видом разнообразного ПО. Многие из них злоумышленники выдавали за всевозможные приложения финансовой тематики — справочники и обучающие пособия, программы для прохождения опросов, торговли и просмотра данных о котировках, инструменты для ведения домашней бухгалтерии и т. д. Среди них — Android.FakeApp.1219, Android.FakeApp.1220, Android.FakeApp.1221, Android.FakeApp.1226, Android.FakeApp.1228, Android.FakeApp.1229, Android.FakeApp.1231, Android.FakeApp.1232, Android.FakeApp.1241 и другие.

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

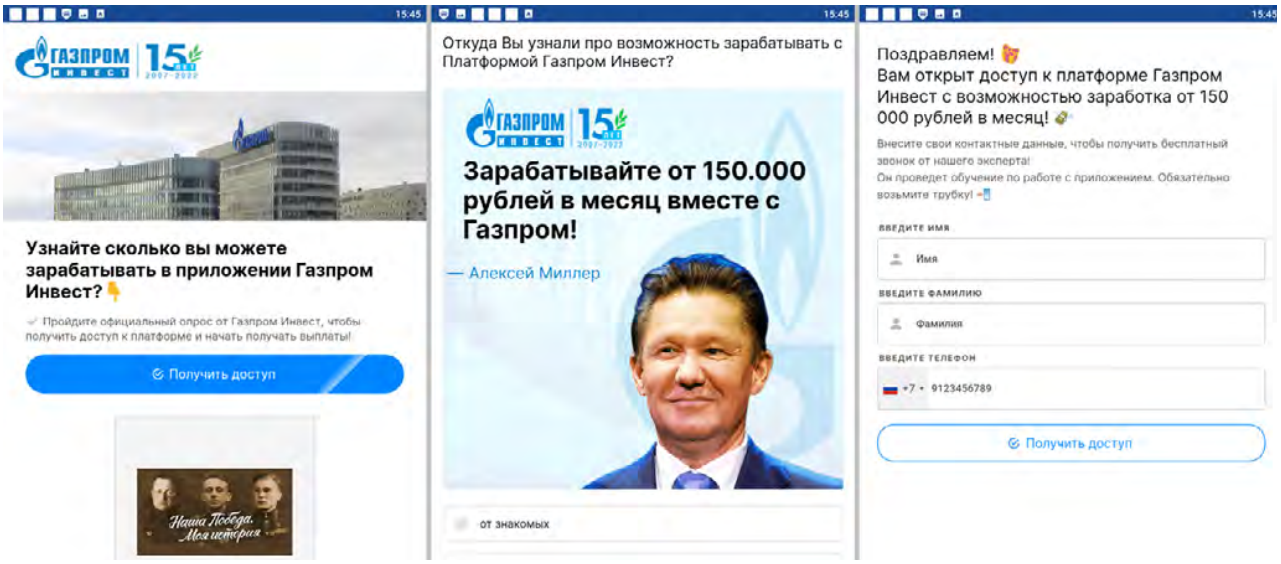
Угрозы в Google Play



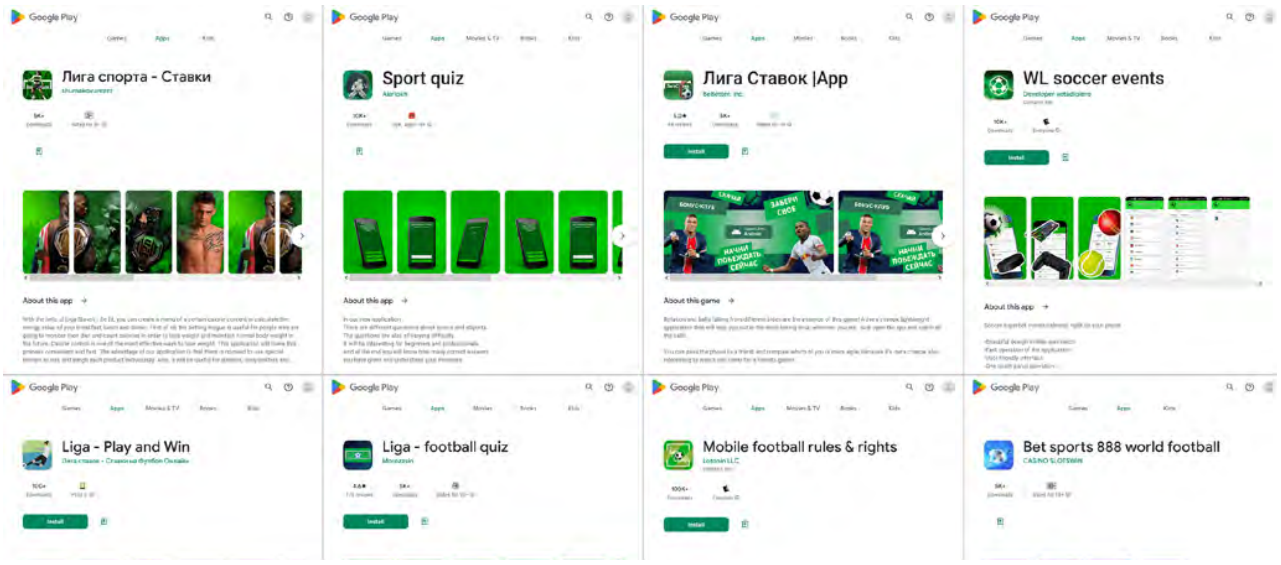
Если пользователи устанавливали их при переходе по специальной ссылке (например, из рекламного объявления), то при запуске программ загружались мошеннические сайты. На них потенциальным жертвам предлагалось пройти небольшой опрос и получить доступ к «инвестиционной платформе», зарегистрировав учетную запись с указанием персональных данных. Если же установка программ была органической (то есть пользователи находили и устанавливали такие подделки по собственной инициативе), некоторые из них вместо загрузки сайтов мошенников демонстрировали ожидаемую функциональность.
Примеры загружаемых ими мошеннических сайтов:



Угрозы в Google Play



Ряд программ злоумышленники преподносили в качестве приложений спортивной тематики или официального ПО букмекерских контор.

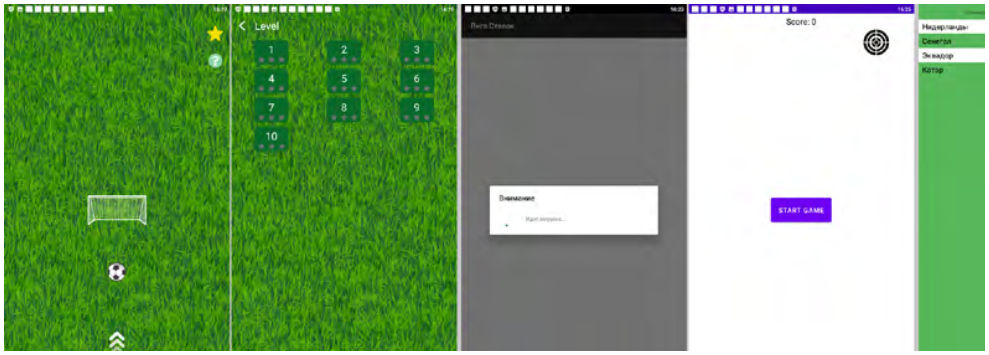


Некоторые из них (Android.FakeApp.1192, Android.FakeApp.1193, Android.FakeApp.1194, Android.FakeApp.22.origin, Android.FakeApp.1195, Android.FakeApp.1196 и другие) выполняли проверку устройств, на которых работали. Если они обнаруживали, что эти устройства тестовые (например, с отсутствующей SIM-картой или модели линейки Nexus), то активировали безобидную функциональность — запускали игры, викторины (так называемые квизы), загру-

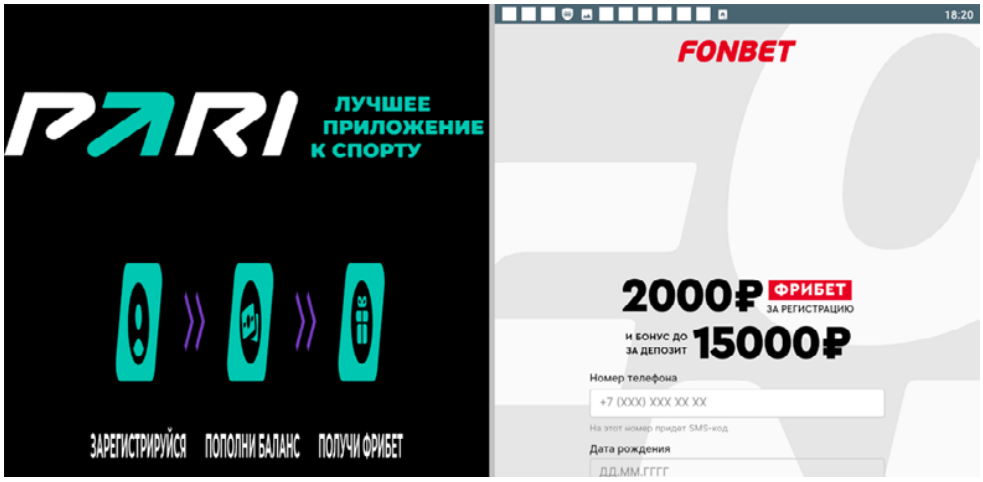
Угрозы в Google Play

жали спортивные таблицы, информацию о матчах и т. д. В противном случае они открывали в WebView или браузере сайты, адреса которых получали из базы данных Firebase. Другие такие программы-подделки (Android.FakeApp.1197, Android.FakeApp.1198, Android.FakeApp.1199, Android.FakeApp.1200, Android.FakeApp.1201, Android.FakeApp.1202, Android.FakeApp.1204, Android.FakeApp.1209, Android.FakeApp.1212 и другие) соединялись с удаленным сервером, который принимал решение о запуске скрытых безобидных функций или загрузке того или иного сайта. А троянская программа Android.FakeApp.1203 получала ссылки для загрузки сайтов из облачного сервиса Firebase Remote Config. Ниже представлены примеры работы этих программ.

Запуск игр и загрузка таблицы футбольных матчей:

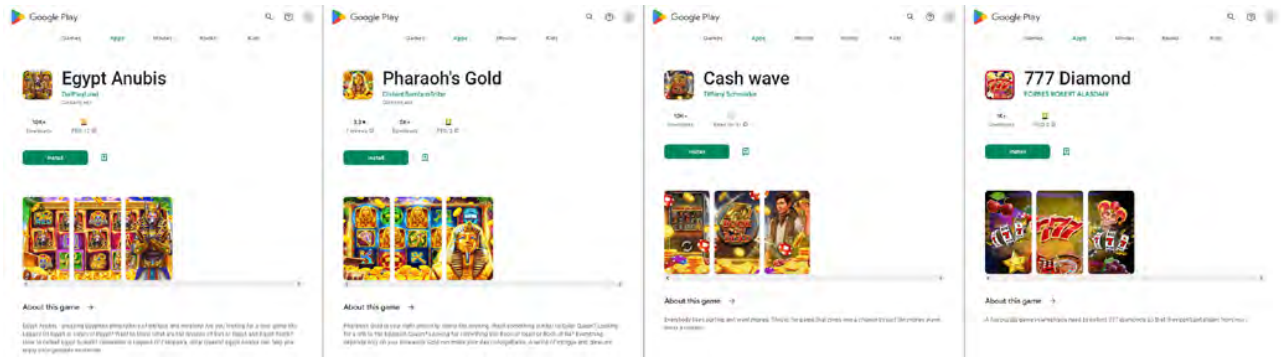


Те же самые приложения загружают сайты букмекеров:

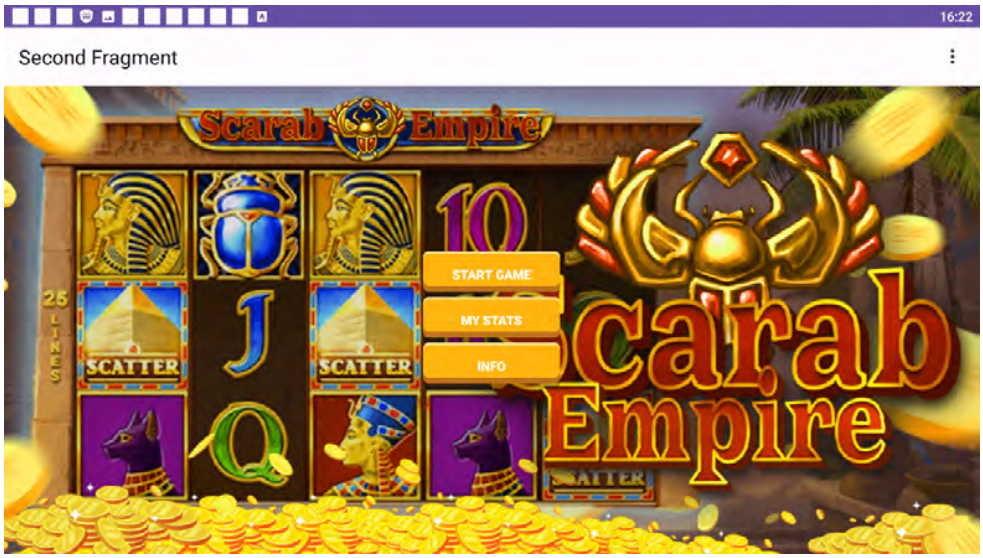


Распространявшиеся под видом игр программы-подделки Android.FakeApp.1222, Android.FakeApp.1224, Android.FakeApp.1225 и Android.FakeApp.1235 вместо игровой функциональности могли загружать в браузере Google Chrome сайты онлайн-казино.

Угрозы в Google Play



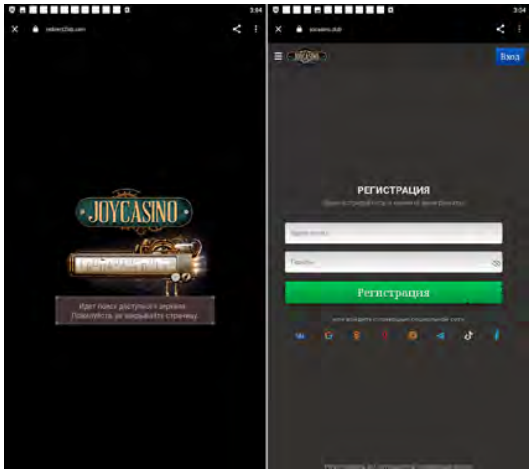
Пример работы одной из них в режиме игры:



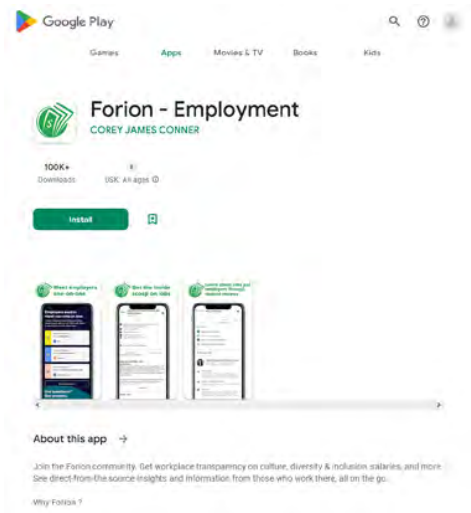
«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2023 года

Угрозы в Google Play

Примеры загружаемых ими веб-страниц:



Была среди выявленных подделок и очередная программа, которая распространялась под видом инструмента поиска работы и загружала мошеннические сайты со списком ненастоящих вакансий. Когда пользователи выбирали одно из объявлений, им предлагалось либо оставить свои контактные данные, заполнив специальную форму, либо связаться с «работодателем» напрямую через мессенджер. Эта подделка является одной из модификаций троянского приложения, известного с конца 2022 года, и детектируется Dr.Web как Android.FakeApp.1133.



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 феврале 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