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

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

В начале сентября Компания «Доктор Веб» опубликовала исследование Android.Pandora.2 — бэкдора, создающего ботнет из зараженных устройств и способного по команде злоумышленников проводить DDoS-атаки. А в середине месяца наши специалисты рассказали о вредоносных приложениях семейства Android.Spy.Lydia. Это многофункциональные трояны-шпионы, нацеленные на иранских пользователей. Представители семейства маскируются под финансовую платформу для онлайн-торговли и по команде атакующих способны выполнять различные вредоносные действия. 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.

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в сентябре 2023 года активность вредоносных приложений снизилась по сравнению с предыдущим месяцем. Например, рекламные троянские приложения семейств Android.HiddenAds и Android.MobiDash обнаруживались на защищаемых устройствах на 11,73% и 26,30% меньше соответственно. Количество атак шпионских троянских программ уменьшилось на 25,11%, программ-вымогателей Android.Locker — на 10,52%, а банковских троянов — на 4,51%. В то же время владельцы Android-устройств сталкивались с нежелательными рекламными программами на 14,32% чаще.

В течение сентября в каталоге Google Play было выявлено множество новых угроз. Среди них — троянские программы семейства Android.FakeApp, применяемые в различных мошеннических схемах, вредоносные программы семейства Android.Joker, которые подписывают жертв на платные услуги, а также рекламные троянские приложения Android.HiddenAds.

Главные тенденции в сентябре

- Снижение активности вредоносных программ
- Появление новых вредоносных приложений в каталоге Google Play

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

Мобильная угроза месяца

В сентябре компания «Доктор Веб» представила подробности анализа вредоносной программы Android.Pandora.2, которая нацелена преимущественно на испаноязычных пользователей. Первые случаи атак с ее участием были зафиксированы в марте 2023 года.

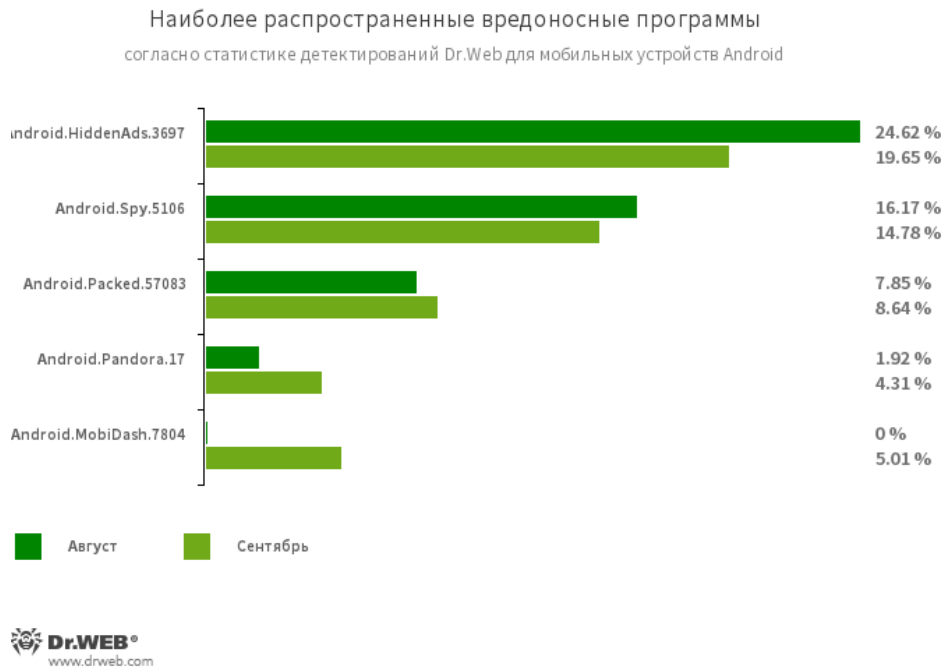
Это троянское приложение заражает смарт-телевизоры и приставки с Android TV, попадая на них через скомпрометированные версии прошивок, а также при установке троянских версий программ для нелегального просмотра видео онлайн.

Основная функция Android.Pandora.2 — проведение по команде злоумышленников DDoS-атак различных типов. Кроме того, эта вредоносная программа может выполнять ряд других действий, например — устанавливать собственные обновления и заменять системный файл hosts.

Исследование вирусных аналитиков «Доктор Веб» показало, что при создании этого трояна вирусописатели использовали наработки авторов Linux.Mirai, взяв за основу часть его кода. Последний с 2016 года широко применяется для заражения IoT-устройств (устройств «интернета вещей») и выполнения DDoS-атак на различные веб-сайты.

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

По данным антивирусных продуктов Dr.Web для Android



Android.HiddenAds.3697

Троянская программа 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.Spy.5106

Троянская программа, представляющая 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.Packed.57083

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

Android.Pandora.17

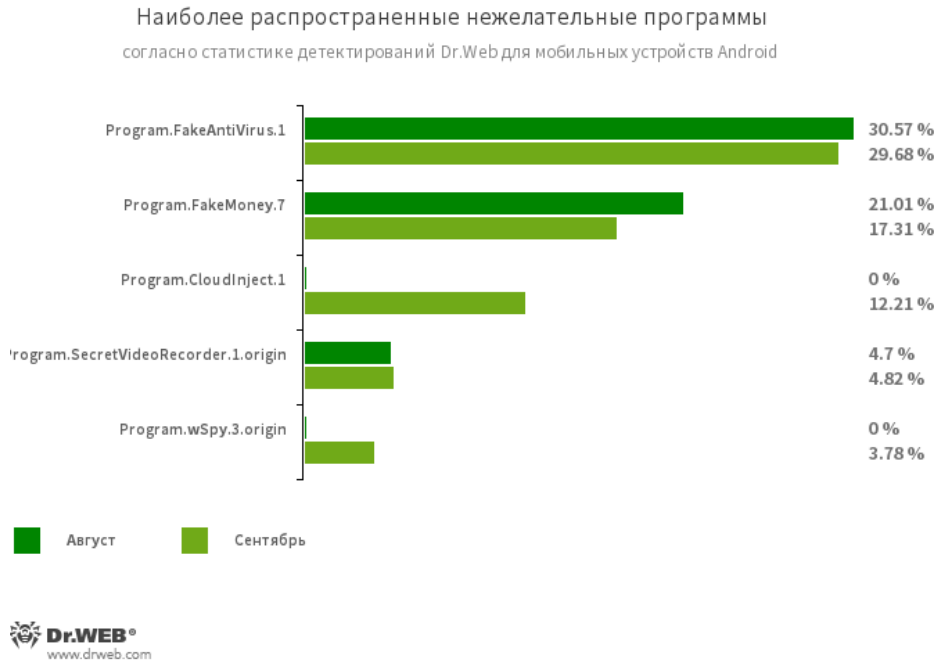
Детектирование вредоносных приложений, скачивающих и устанавливающих троянскую программу-бэкдор Android.Pandora.2. Такие загрузчики злоумышленники часто встраивают в приложения для Smart TV, ориентированные на испаноязычных пользователей.

Android.MobiDash.7804

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 сентябре 2023 года

По данным антивирусных продуктов Dr.Web для Android



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.FakeMoney.7

Детектирование приложений, якобы позволяющих зарабатывать на выполнении тех или иных действий или заданий. Эти программы имитируют начисление вознаграждений, причем для вывода «заработанных» денег требуется накопить определенную сумму. Даже когда пользователям это удается, получить выплаты они не могут.

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 у пользователя появляется возможность дистанционного управлять этими программами — блокировать их, показывать настраиваемые диалоги, отслеживать факт установки и удаления другого ПО и т. д.

По данным антивирусных продуктов Dr.Web для Android

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.

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.

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

По данным антивирусных продуктов Dr.Web для Android

Tool.SilentInstaller.14.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.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.

По данным антивирусных продуктов Dr.Web для Android

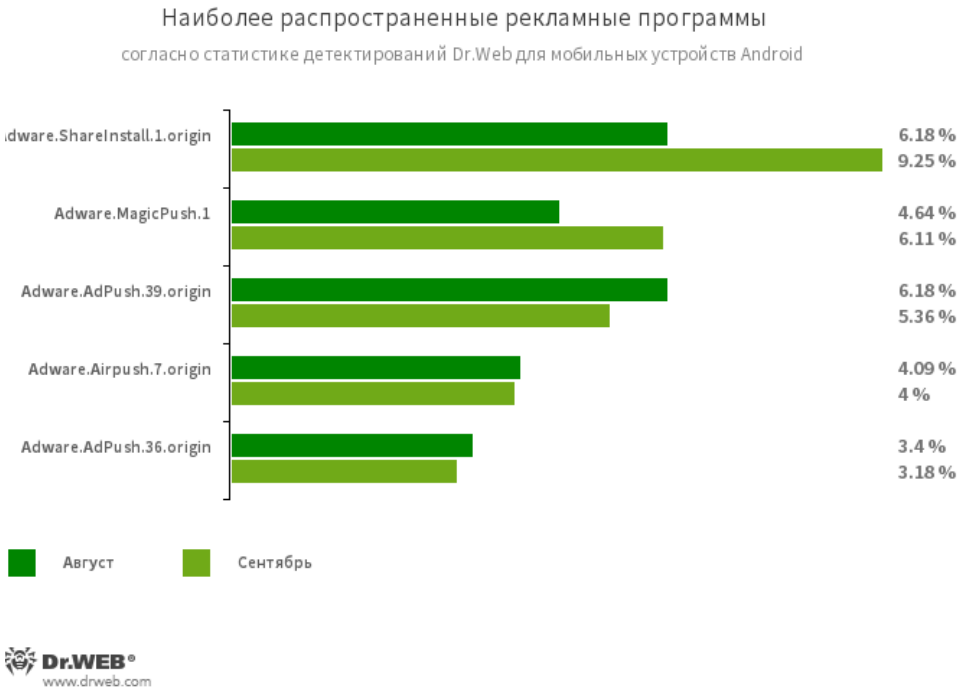
Tool.Packer.3.origin

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

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 сентябре 2023 года



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

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.AdPush.39.origin

Adware.AdPush.36.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.

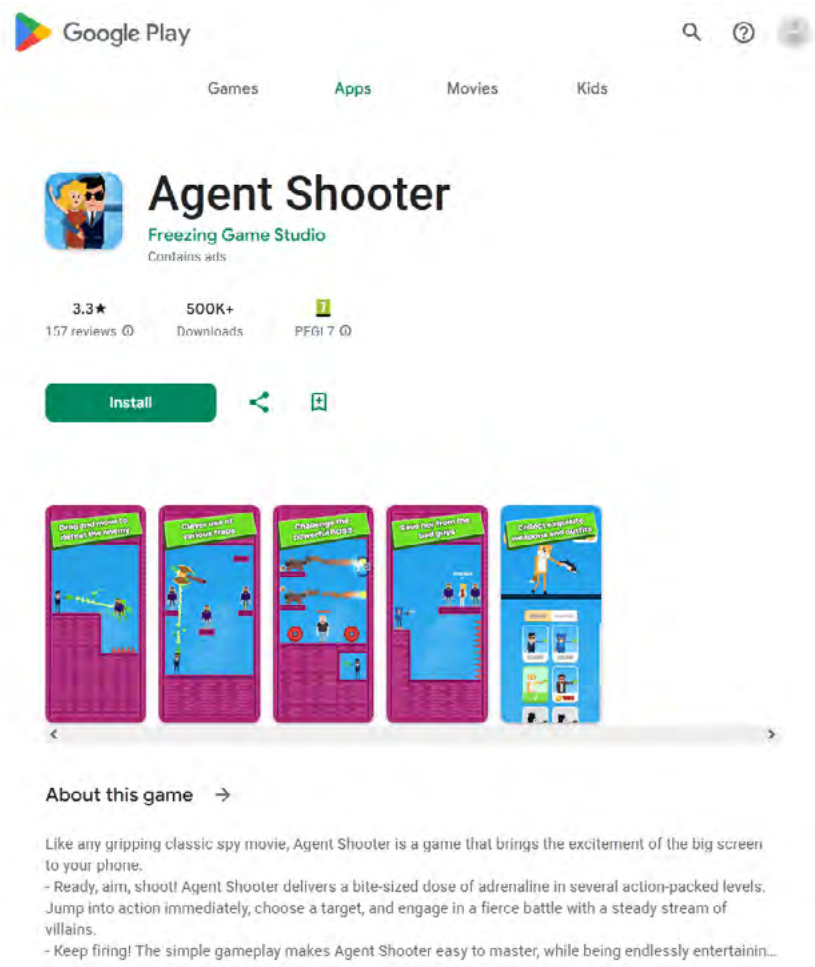
Adware.Airpush.7.origin

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.

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

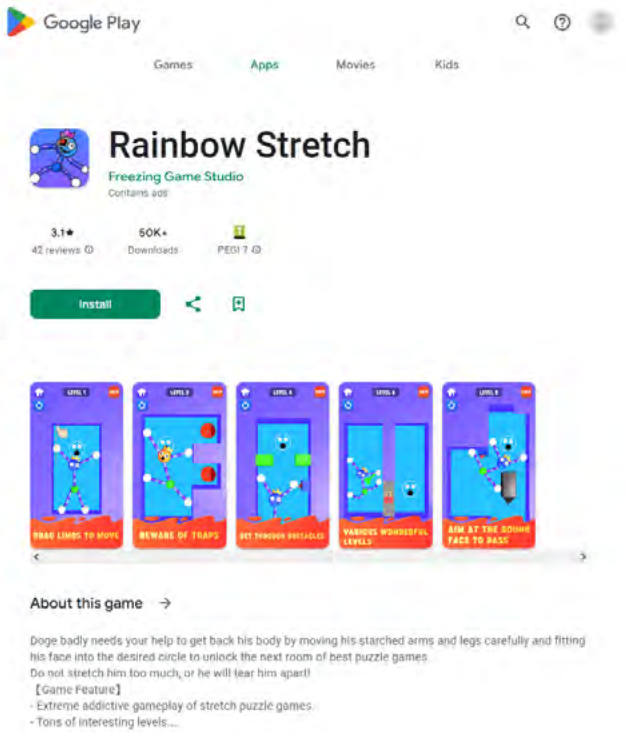
Угрозы в Google Play

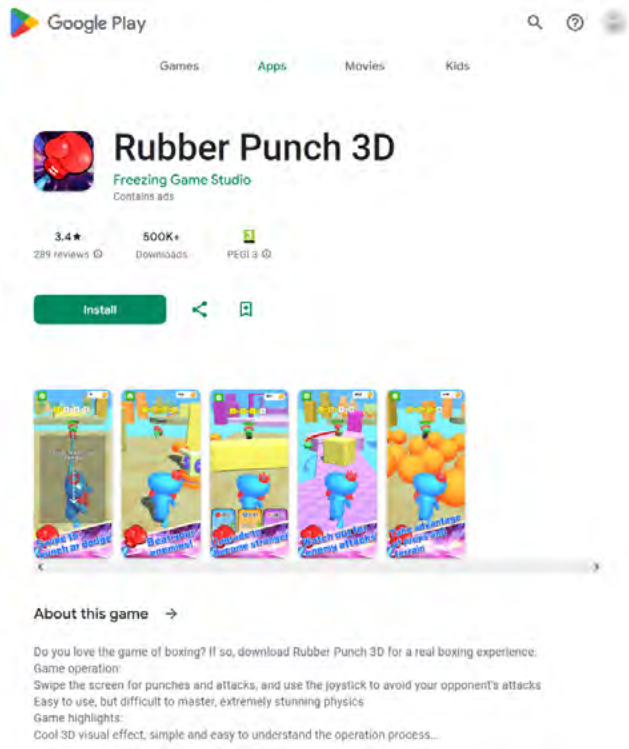
В сентябре 2023 года вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play множество новых вредоносных приложений. Среди них — троянские программы, демонстрировавшие навязчивую рекламу. Злоумышленники распространяли их под видом игр Agent Shooter (Android.HiddenAds.3781), Rainbow Stretch (Android.HiddenAds.3785), Rubber Punch 3D (Android.HiddenAds.3786) и Super Skibydi Killer (Android.HiddenAds.3787). После установки на Android-устройства эти трояны пытались скрыться от пользователей. Для этого они подменяли свои значки, расположенные на домашнем экране, прозрачной версией и заменяли их названия на пустые. Кроме того, они могли притвориться браузером Google Chrome, заменяя значки соответствующей копией. Когда пользователи нажимают на такой значок, троянские программы запускают браузер и сами продолжают работать в фоновом режиме. Это позволяет троянам стать менее заметными и снижает вероятность их преждевременного удаления. Кроме того, если работа вредоносных программ будет остановлена, пользователи перезапустят их, думая, что запускают браузер.

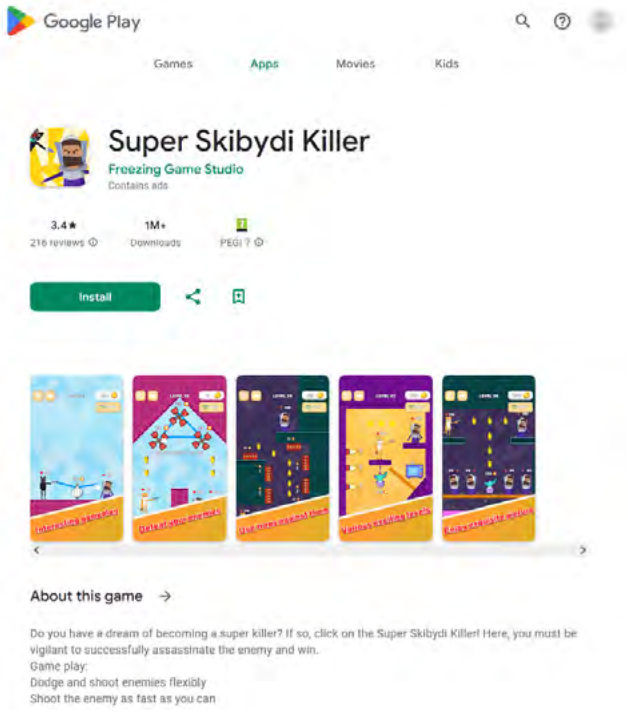


«Доктор Веб»: обзор вирусной активности для мобильных устройств в сентябре 2023 года

Угрозы в Google Play

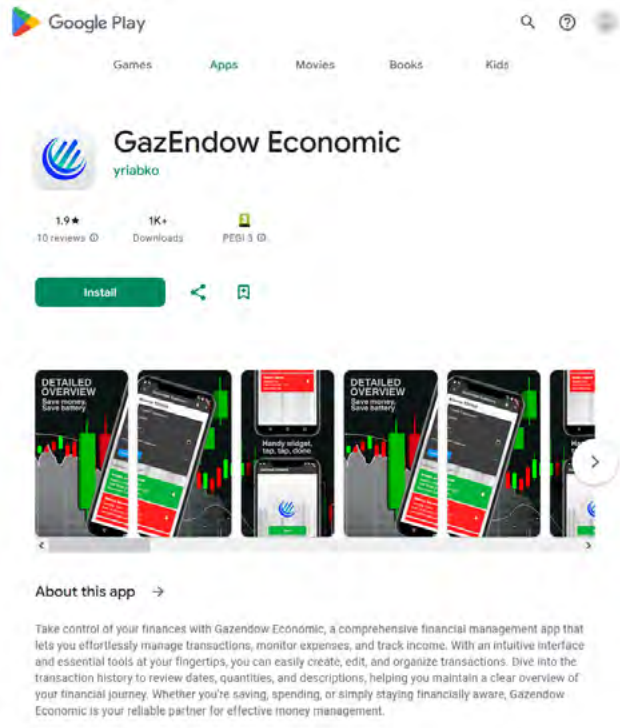


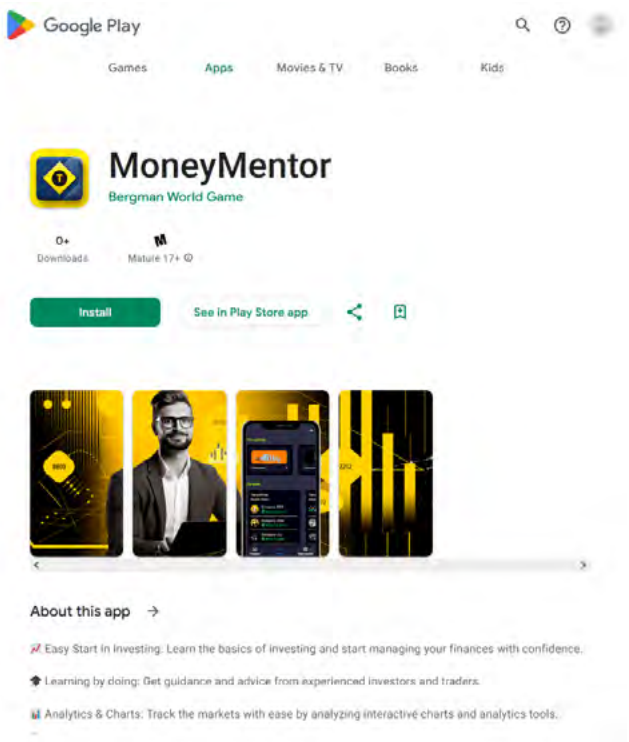




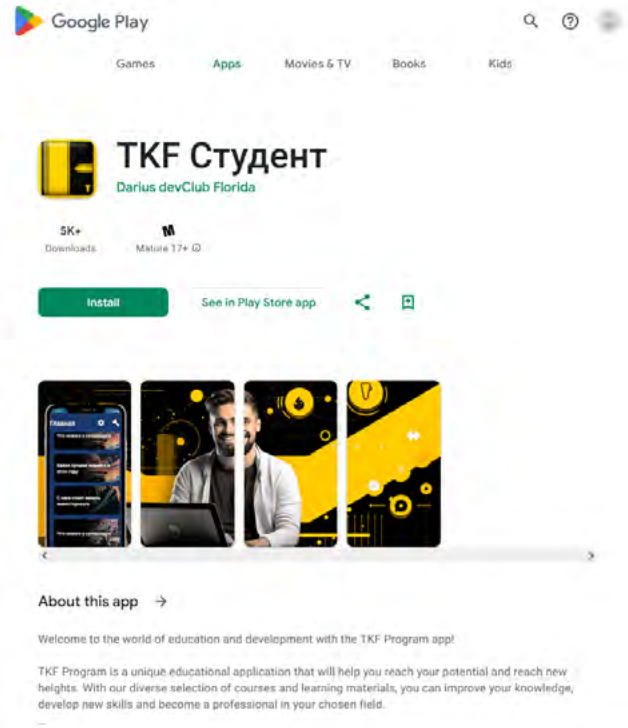
Угрозы в Google Play

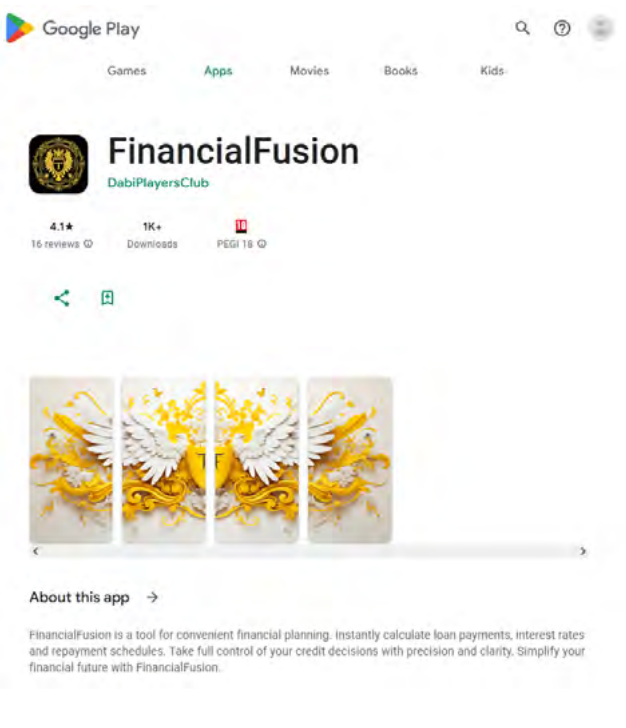
Также наши специалисты выявили очередные программы-подделки из семейства Android.FakeApp. Некоторые из них (Android.FakeApp.1429, Android.FakeApp.1430, Android.FakeApp.1432, Android.FakeApp.1434, Android.FakeApp.1435 и другие) распространялись под видом финансовых программ. Например, приложений для биржевой торговли, справочников и обучающих пособий по инвестированию, домашних бухгалтерий и других. На самом деле их основной задачей была загрузка мошеннических сайтов, на которых потенциальным жертвам предлагалось стать «инвесторами».

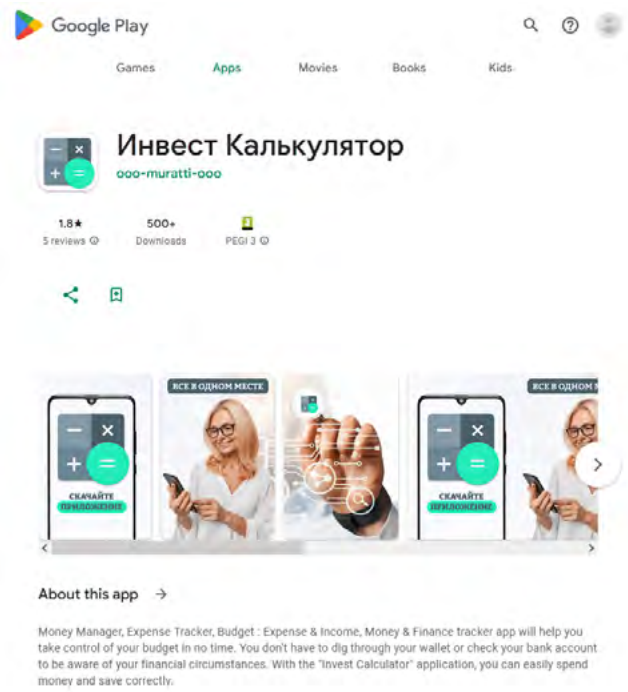


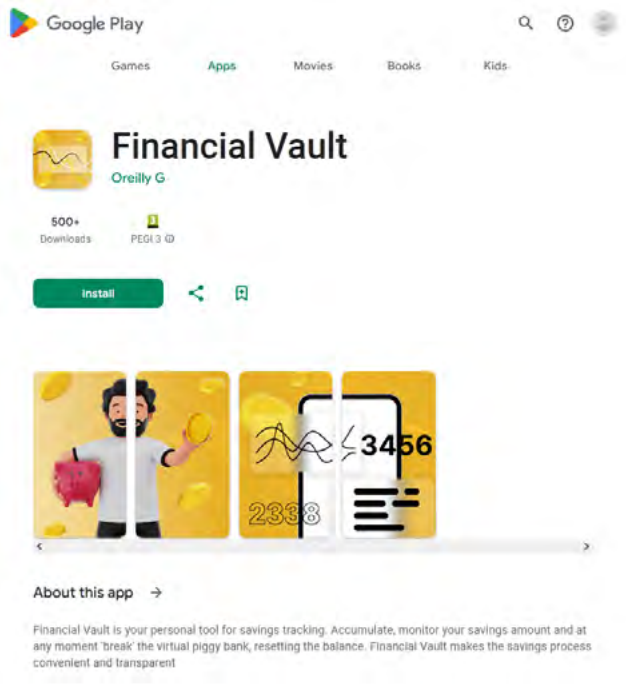


«Доктор Веб»: обзор вирусной активности для мобильных устройств в сентябре 2023 года



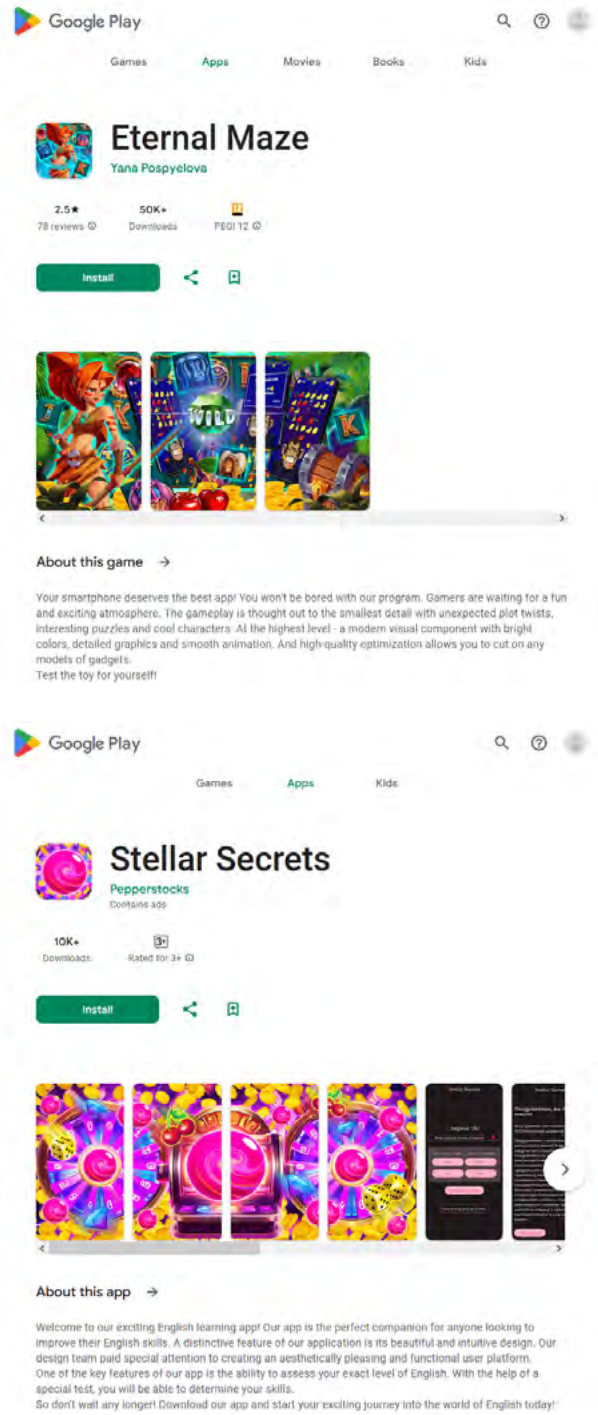


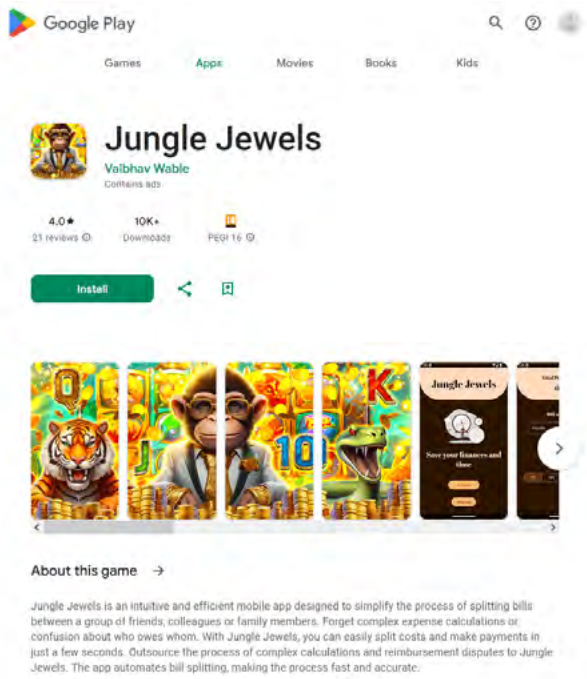


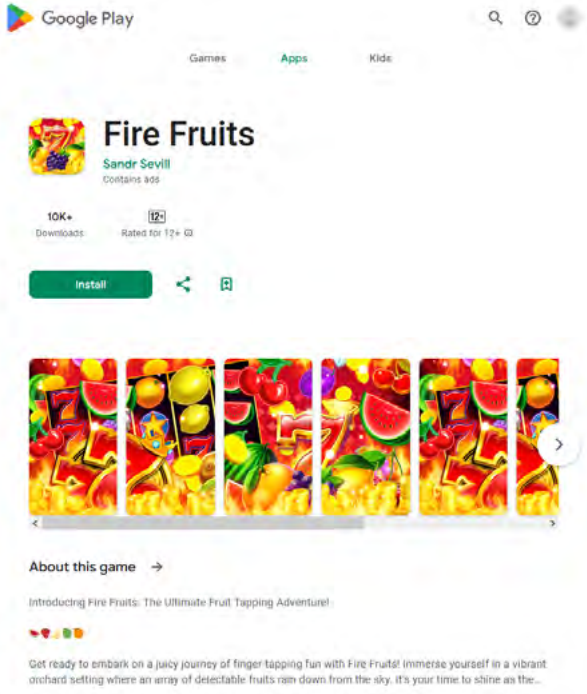


«Доктор Веб»: обзор вирусной активности для мобильных устройств в сентябре 2023 года

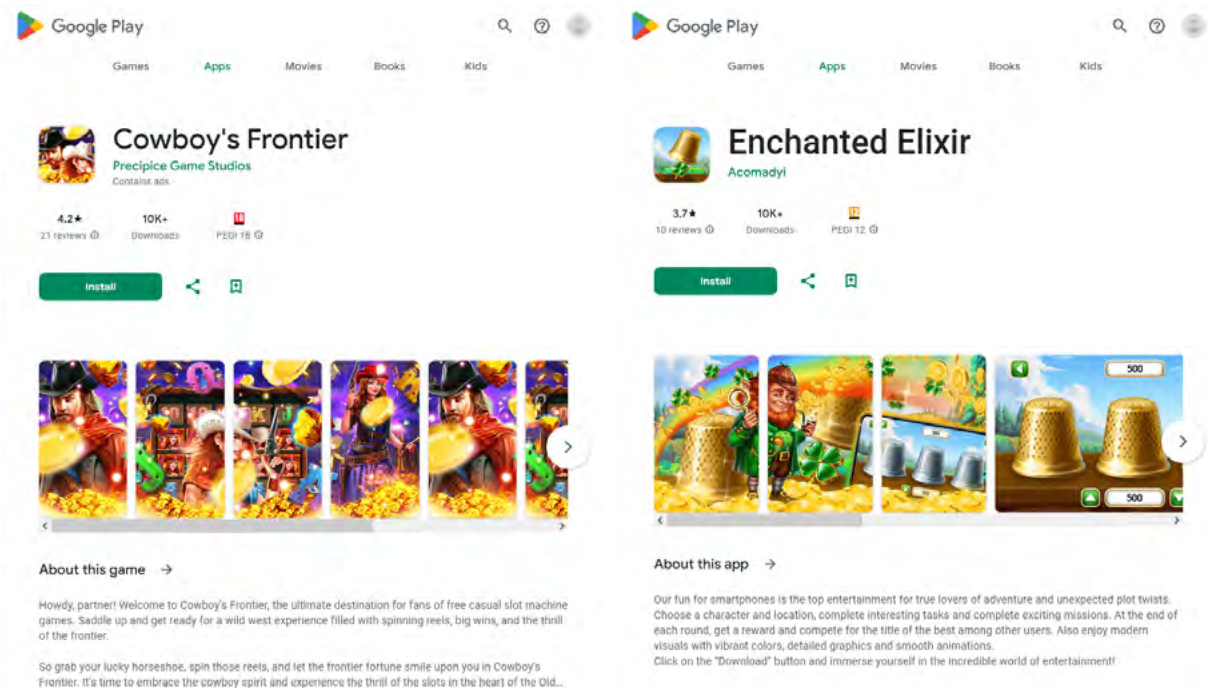
Другие программы-подделки (например, Android.FakeApp.1433, Android.FakeApp.1436, Android.FakeApp.1437, Android.FakeApp.1438, Android.FakeApp.1439 и Android.FakeApp.1440) злоумышленники выдавали за всевозможные игровые приложения. В ряде случаев те действительно могли работать как игры, но их главной функцией являлась загрузка сайтов онлайн-казино.



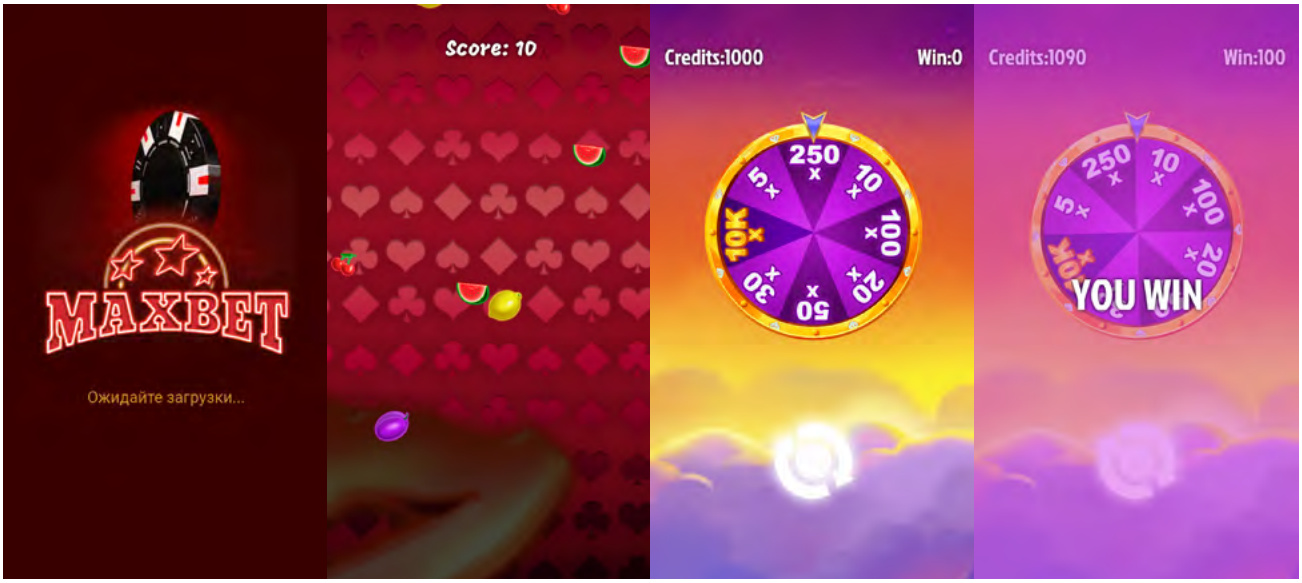




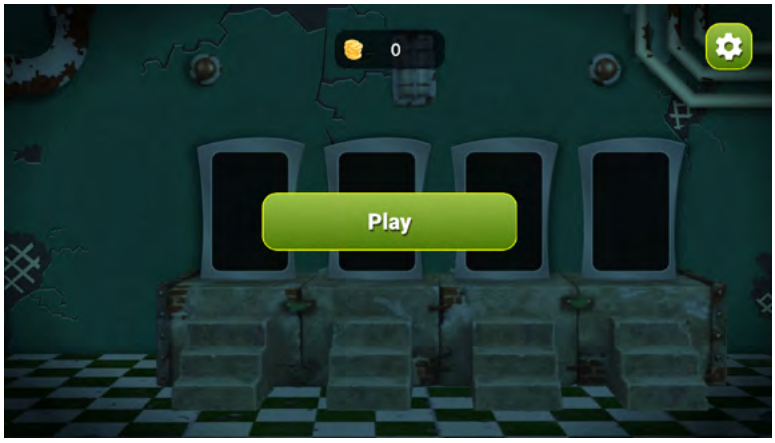
«Доктор Веб»: обзор вирусной активности для мобильных устройств в сентябре 2023 года

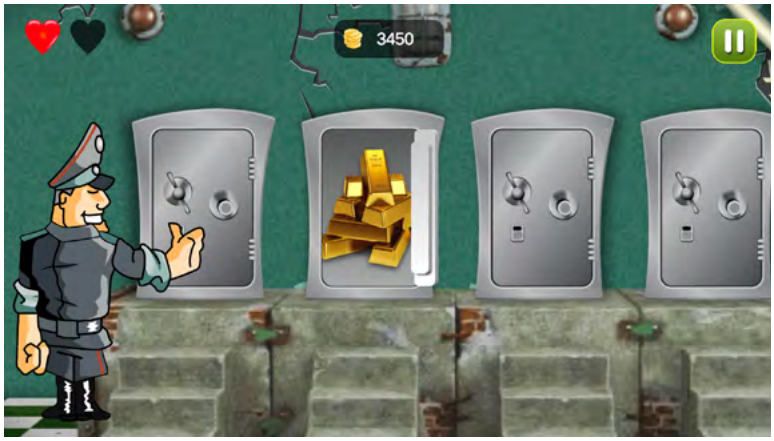


Примеры работы этих вредоносных программ в режиме игры:

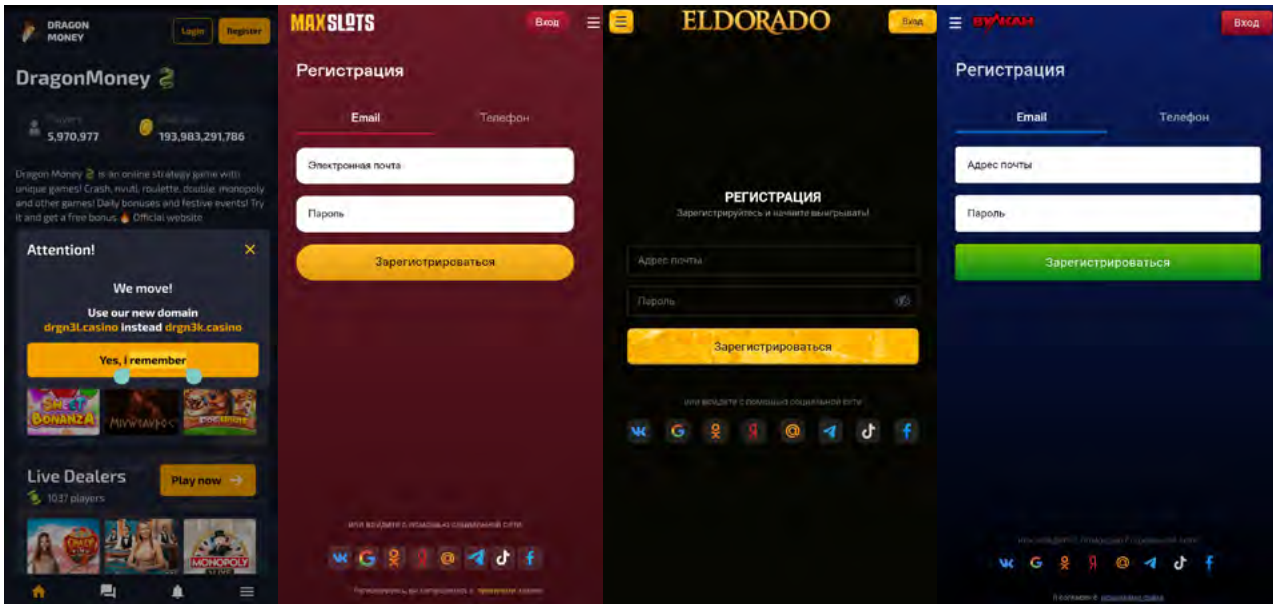


«Доктор Веб»: обзор вирусной активности для мобильных устройств в сентябре 2023 года



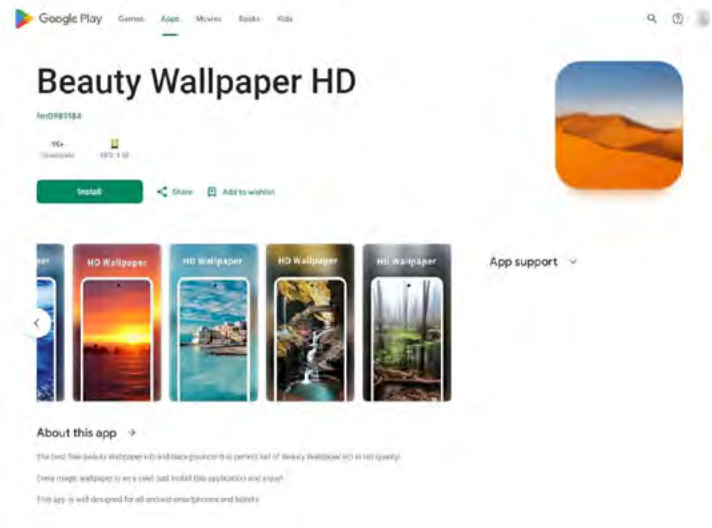


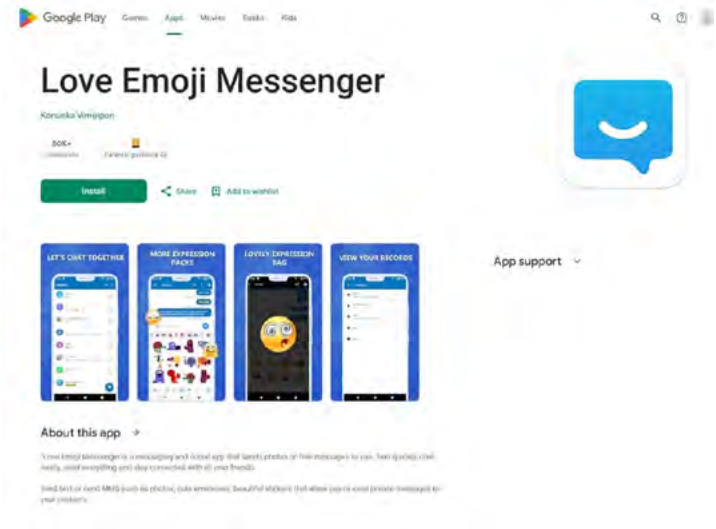
Примеры загружаемых ими сайтов онлайн-казино:



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

Вместе с тем в каталоге Google Play были обнаружены очередные троянские программы семейства Android.Joker, которые подписывали владельцев Android-устройств на платные услуги. Один из них скрывался в приложении с коллекцией изображений Beauty Wallpaper HD, по классификации компании «Доктор Веб» он получил имя Android.Joker.2216. Другой распространялся под видом онлайн-мессенджера Love Emoji Messenger и был добавлен в вирусную базу Dr.Web как Android.Joker.2217.





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 сентябре 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