# «Доктор Веб»:

## обзор вирусной активности для мобильных устройств в декабре 2023 года

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

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в декабре 2023 года наиболее активными вредоносными приложениями вновь стали рекламные троянские программы Android.HiddenAds. Однако пользователи сталкивались с ними на 53,89% реже по сравнению с месяцем ранее. Кроме того, снизилось число атак банковских троянских программ и шпионских приложений — на 0,88% и 10,83% соответственно.

В течение последнего месяца минувшего года вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play очередные вредоносные программы-подделки из семейства Android.FakeApp, применяемые в различных мошеннических схемах. Также наши специалисты выявили очередные сайты, через которые злоумышленники распространяли поддельные приложения криптокошельков.

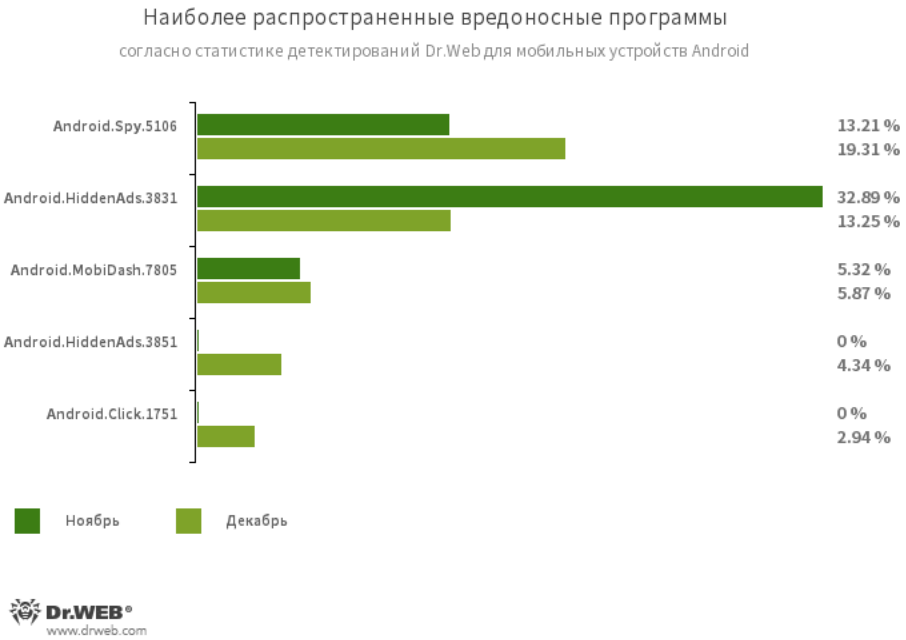


## Главные тенденции декабря

- На защищаемых устройствах чаще всего обнаруживались рекламные троянские программы из семейства Android.HiddenAds
- Снизилась активность банковских троянов и вредоносных приложений-шпионов
- В каталоге Google Play были выявлены новые вредоносные программы
- Продолжили выявляться сайты, распространяющие фальшивые приложения криптокошельков для устройств под управлением как ОС Android, так и iOS

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

## По данным антивирусных продуктов Dr.Web для Android




Android.Spy.5106

Детектирование 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.3831

Android.HiddenAds.3851

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.MobiDash.7805

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

Android.Click.1751

Троян, встраиваемый в модификации мессенджера WhatsApp и маскирующийся под классы библиотек от Google. Во время использования приложения-носителя Android.Click.1751 делает запросы к одному из управляющих серверов. В ответ троян получает две ссылки, одна из которых предназначена для русскоязычных пользователей, а другая — для всех остальных. Затем он демонстрирует диалоговое окно с полученным от сервера содержимым и после нажатия пользователем на кнопку подтверждения загружает соответствующую ссылку в браузере.

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

## По данным антивирусных продуктов Dr.Web для Android


### 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.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.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.

## По данным антивирусных продуктов Dr.Web для Android

Program.FakeMoney.7

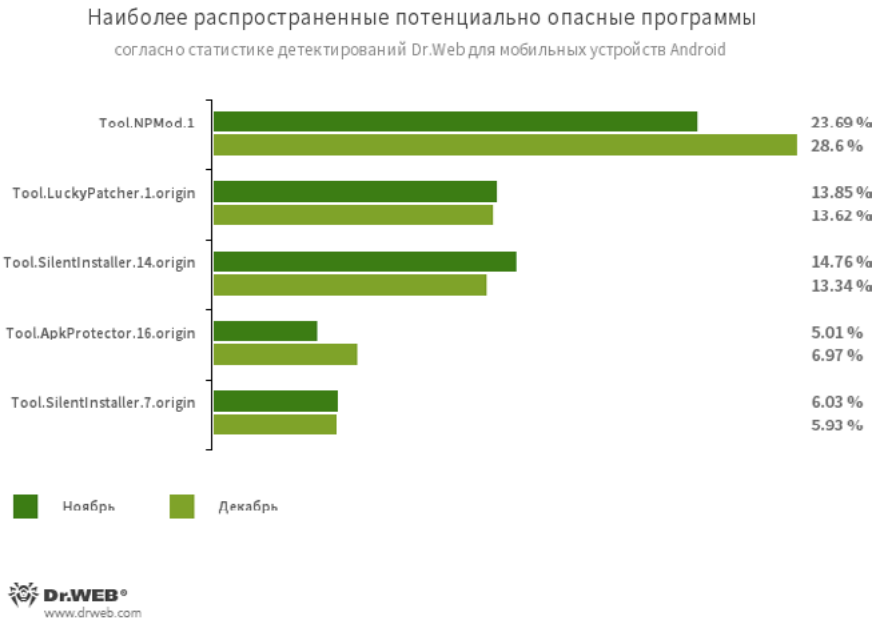
Детектирование приложений, якобы позволяющих зарабатывать на выполнении тех или иных действий или заданий. Эти программы имитируют начисление вознаграждений, причем для вывода «заработанных» денег требуется накопить определенную сумму. Даже когда пользователям это удается, получить выплаты они не могут.

Program.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 декабре 2023 года

## По данным антивирусных продуктов Dr.Web для Android




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.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.SilentInstaller.14.origin

Tool.SilentInstaller.7.origin

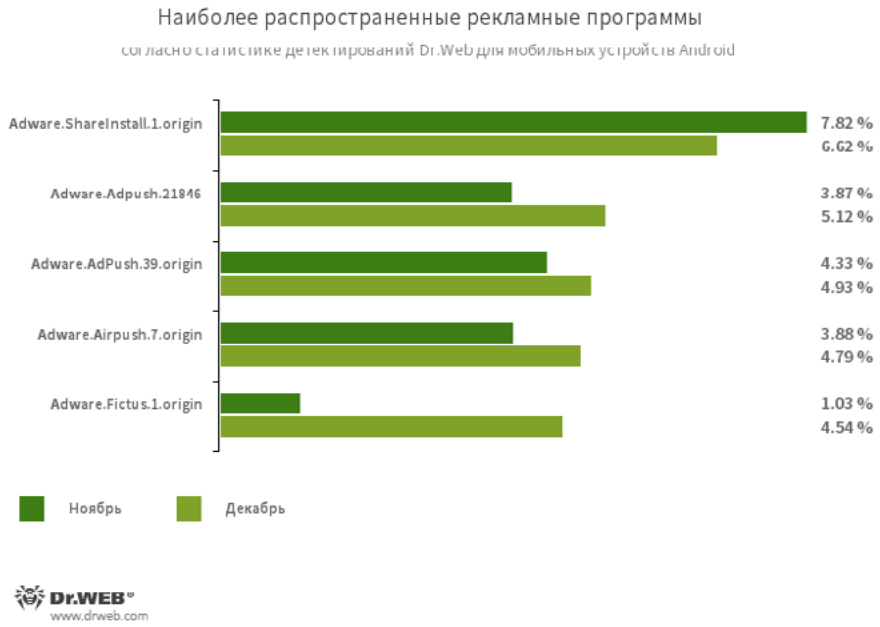
Потенциально опасные программные платформы, которые позволяют приложениям запускать APK-файлы без их установки. Эти платформы создают виртуальную среду исполнения в контексте приложений, в которые они встроены. Запускаемые с их помощью APK-файлы могут работать так, как будто являются частью таких программ, и автоматически получать те же разрешения.

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 декабре 2023 года

## По данным антивирусных продуктов Dr.Web для Android




### Adware.ShareInstall.1.origin

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

### Adware.Adpush.21846

### Adware.AdPush.39.origin

Рекламные модули, которые могут быть интегрированы в Android-программы. Они демонстрируют рекламные уведомления, вводящие пользователей в заблуждение. Например, такие уведомления могут напоминать сообщения от операционной системы. Кроме того, эти модули собирают ряд конфиденциальных данных, а также способны загружать другие приложения и инициировать их установку.

### Adware.Airpush.7.origin

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.

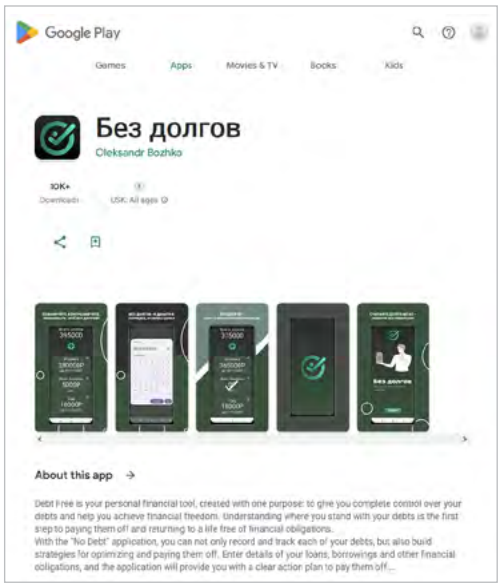
### Adware.Fictus.1.origin

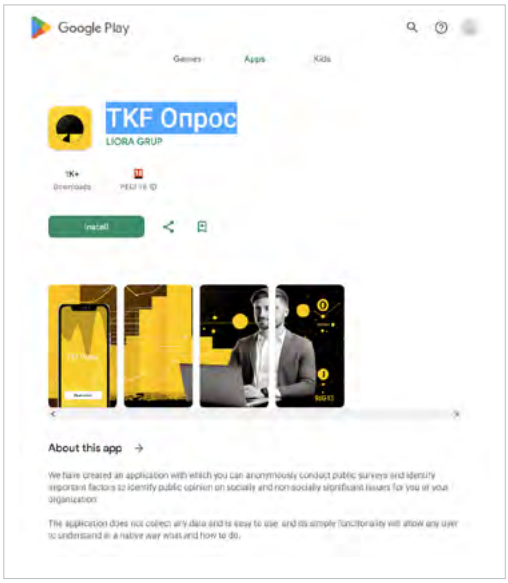
Рекламный модуль, который злоумышленники встраивают в версии-клоны популярных Android-игр и программ. Его интеграция в программы происходит при помощи специализированного упаковщика net2share. Созданные таким образом копии ПО распространяются через различные каталоги приложений и после установки демонстрируют нежелательную рекламу.

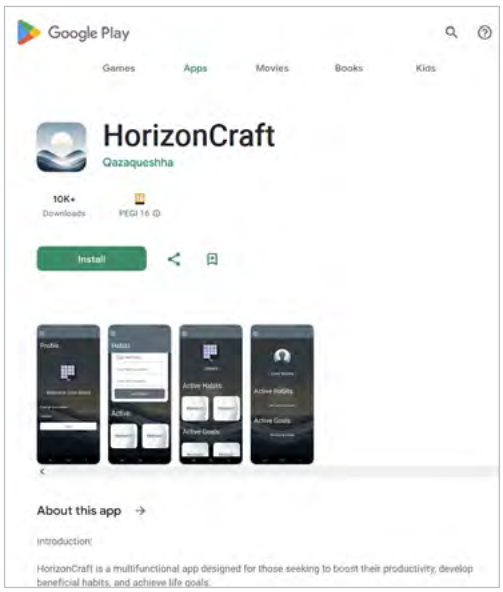
# «Доктор Веб»: обзор вирусной активности для мобильных устройств в декабре 2023 года

## Угрозы в Google Play

В декабре 2023 года специалисты компании «Доктор Веб» обнаружили в каталоге Google Play новые троянские программы из семейства Android.FakeApp. Например, Android.FakeApp.1564 злоумышленники распространяли под видом приложения, позволяющего вести учет долгов. Троян Android.FakeApp.1563 скрывался в программе для прохождения опросов.
А Android.FakeApp.1569 мошенники выдавали за инструмент, помогающий повысить продуктивность и выработать полезные привычки.



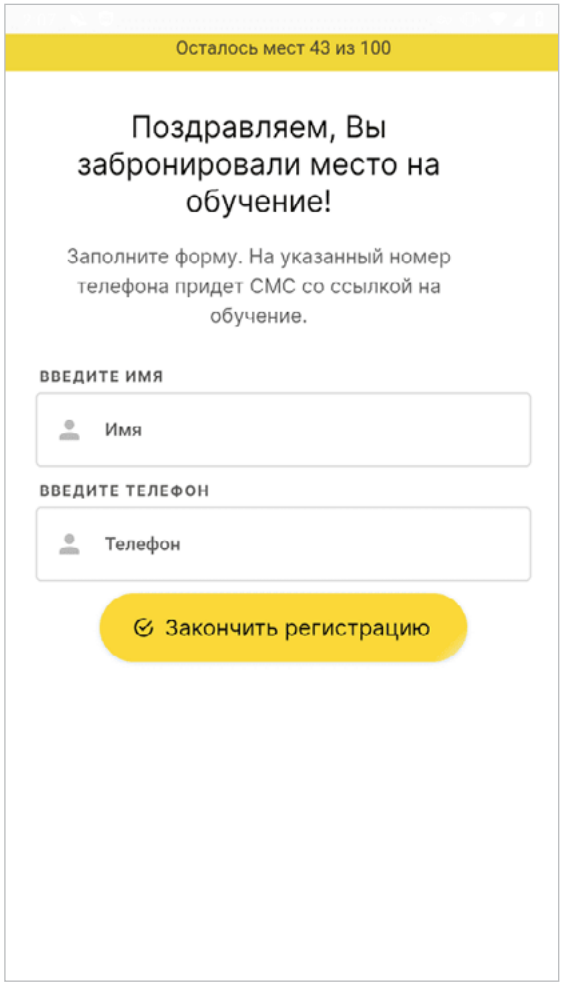



## Угрозы в Google Play

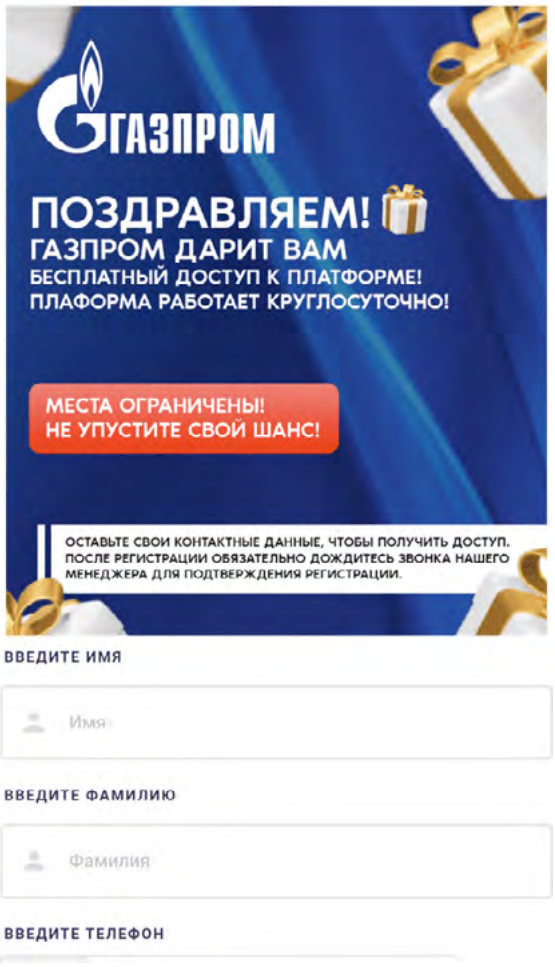
Все эти программы-подделки загружали мошеннические сайты финансовой тематики, которые копировали дизайн настоящих сайтов банков, новостных агентств и других известных организаций. Кроме того, в их оформлении использовались соответствующие названия и логотипы. На таких мошеннических интернет-ресурсах пользователям предлагалось стать инвесторами, пройти обучение финансовой грамотности, получить финансовую помощь и т. д. При этом требовалось указать персональные данные — якобы для регистрации учетной записи и получения доступа к соответствующим сервисам.

Примеры загружаемых троянами поддельных сайтов:

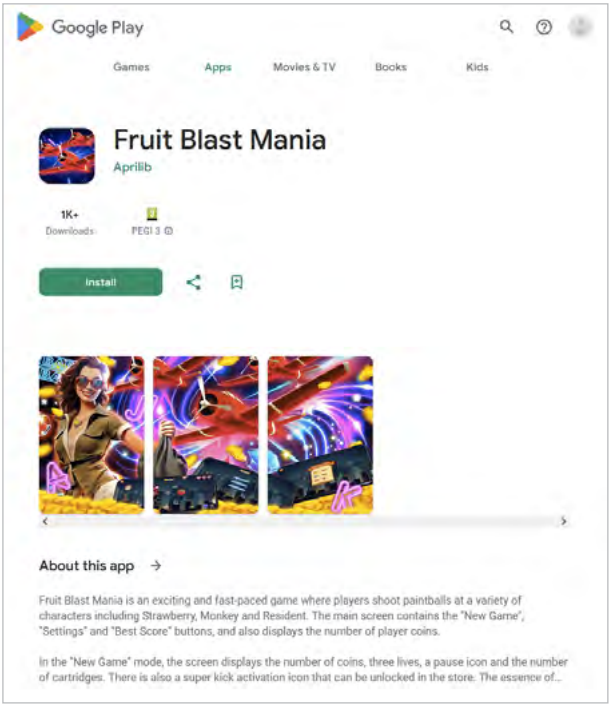

## Угрозы в Google Play

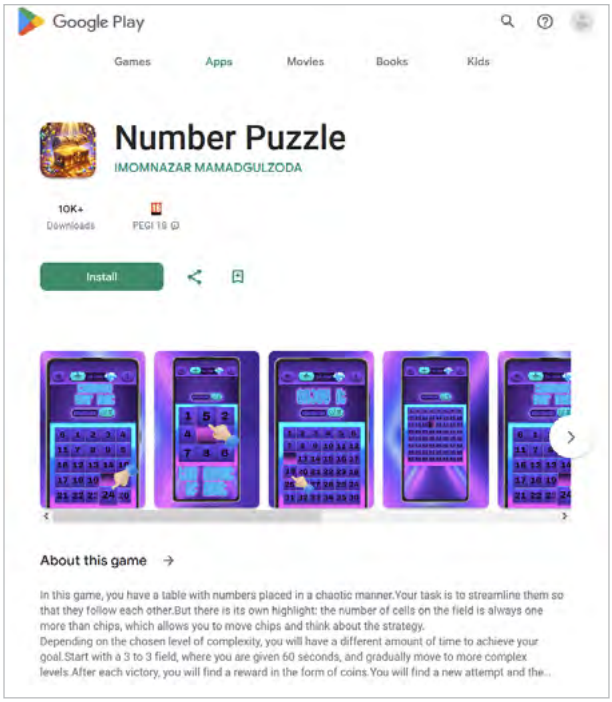


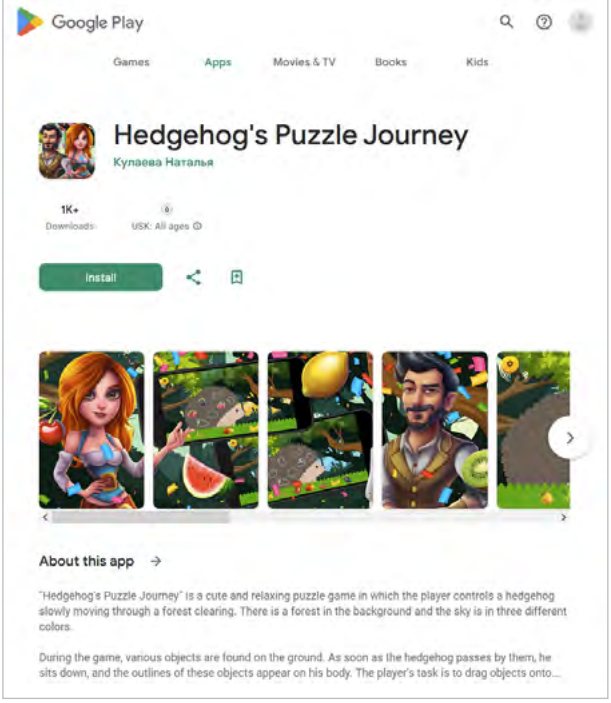

# «Доктор Веб»: обзор вирусной активности для мобильных устройств в декабре 2023 года

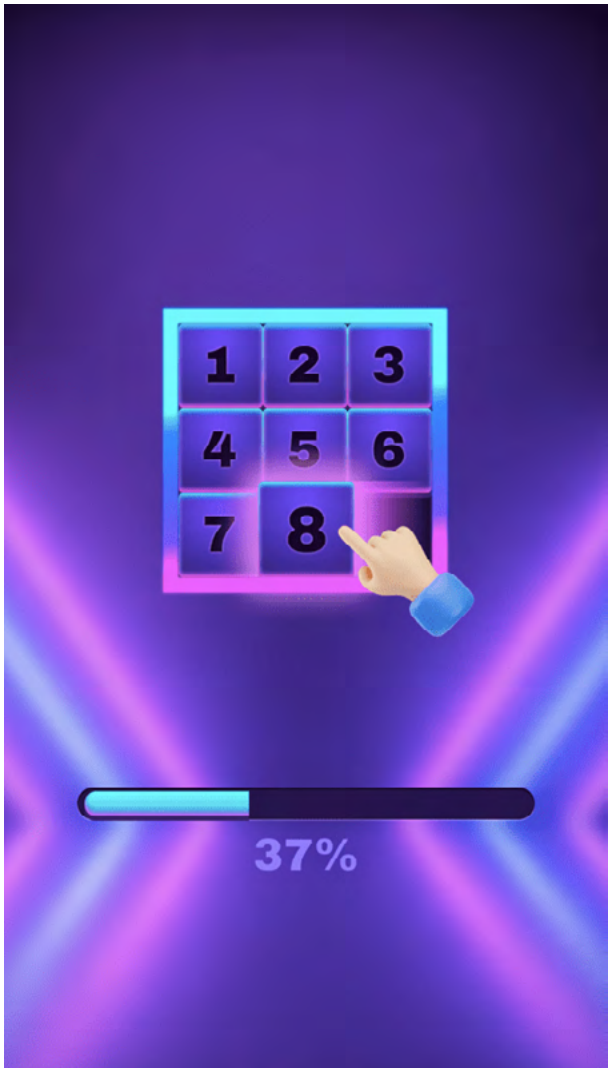
А вредоносные приложения Android.FakeApp.1566, Android.FakeApp.1567 и Android.FakeApp.1568 распространялись под видом игр:



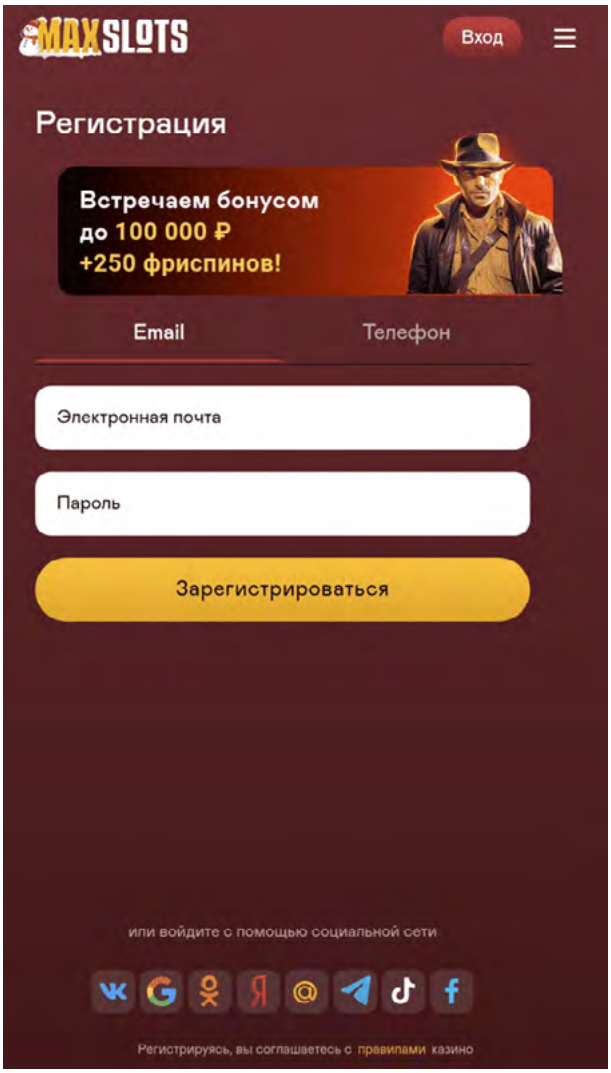



Вместо запуска игр они могли загружать сайты букмекеров и онлайн-казино, как показано на примере ниже.




Один из загруженных ей сайтов:


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 декабре 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