«Доктор Веб»:

обзор вирусной активности для мобильных устройств в ноябре 2023 года

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

21 декабря 2023 года

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в ноябре 2023 года пользователи реже сталкивались с рекламными троянскими приложениями семейств Android.HiddenAds и Android.MobiDash. Активность первых снизилась на четверть (25,03%), вторых — более чем на треть (35,87%). Кроме того, на защищаемых устройствах реже обнаруживались банковские трояны и вредоносные программы-шпионы — на 3,53% и 17,10% соответственно.

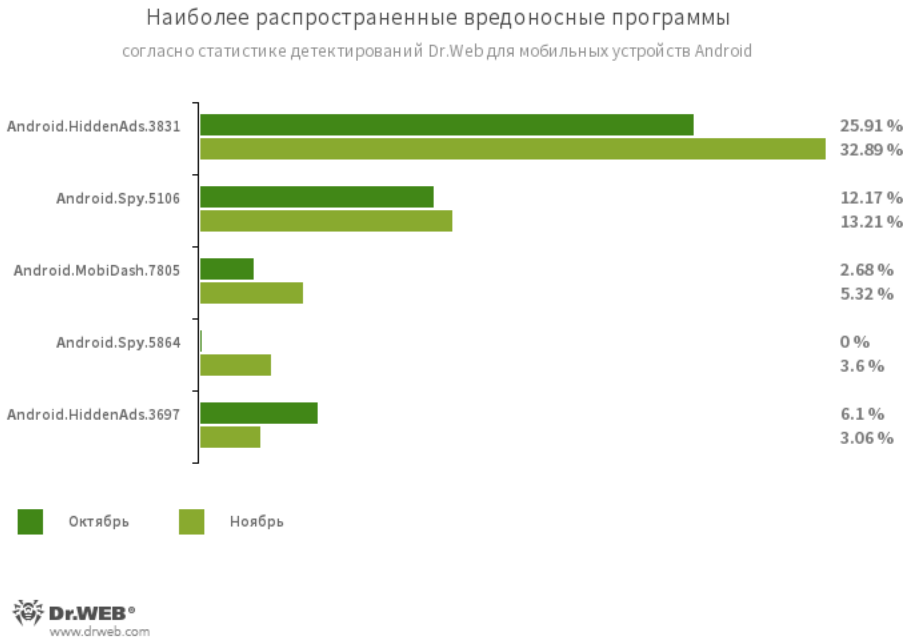
Вместе с тем злоумышленники вновь распространяли вредоносные программы через каталог Google Play. Наши специалисты выявили в нем более двух десятков троянских программ семейства Android.FakeApp, используемых в мошеннических целях, а также очередного трояна, подписывающего владельцев Android-устройств на платные услуги.

Главные тенденции в ноябре

- Снижение активности рекламных троянских программ
- Снижение активности банковских троянов и вредоносных приложений-шпионов
- Распространение новых вредоносных программ через каталог Google Play

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

По данным антивирусных продуктов Dr.Web для Android



Android.HiddenAds.3831

Android.HiddenAds.3697

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.Spy.5106

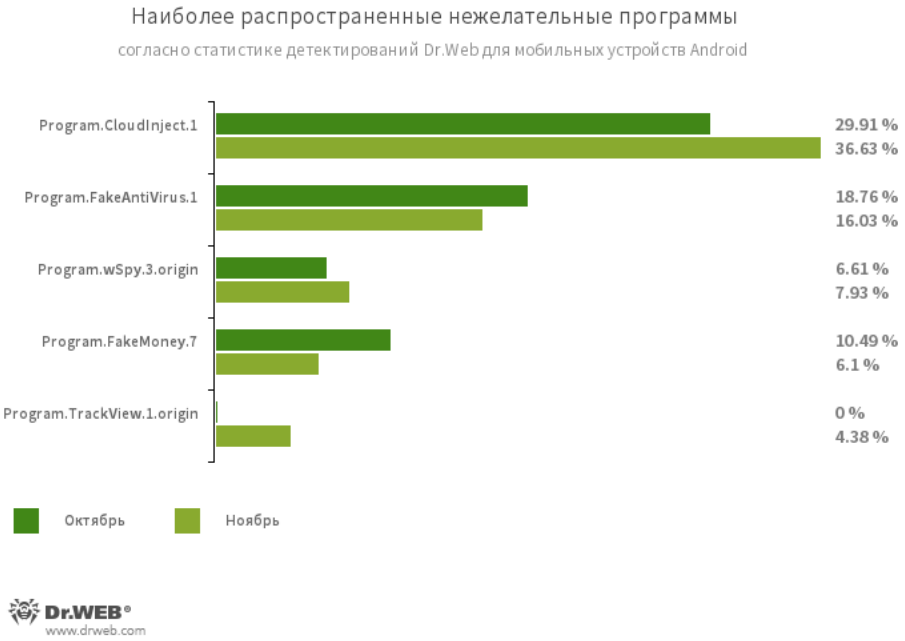
Детектирование троянской программы, представляющей собой видоизмененные версии неофициальных модификаций приложения WhatsApp. Она может похищать содержимое уведомлений, предлагать установку программ из неизвестных источников, а во время использования мессенджера — демонстрировать диалоговые окна с дистанционно настраиваемым содержимым.

Android.Spy.5864

С помощью этой вирусной записи антивирус Dr.Web обнаруживает троянскую программу, которая скрывается в ряде сторонних модификаций мессенджера WhatsApp. Злоумышленники используют эту вредоносную программу для слежки за пользователями. Например, они могут искать файлы на устройствах жертв и загружать их на удаленный сервер, собирать данные из телефонной книги, получать информацию о зараженном устройстве, выполнять аудиозапись окружения с целью прослушивания и т. д.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 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

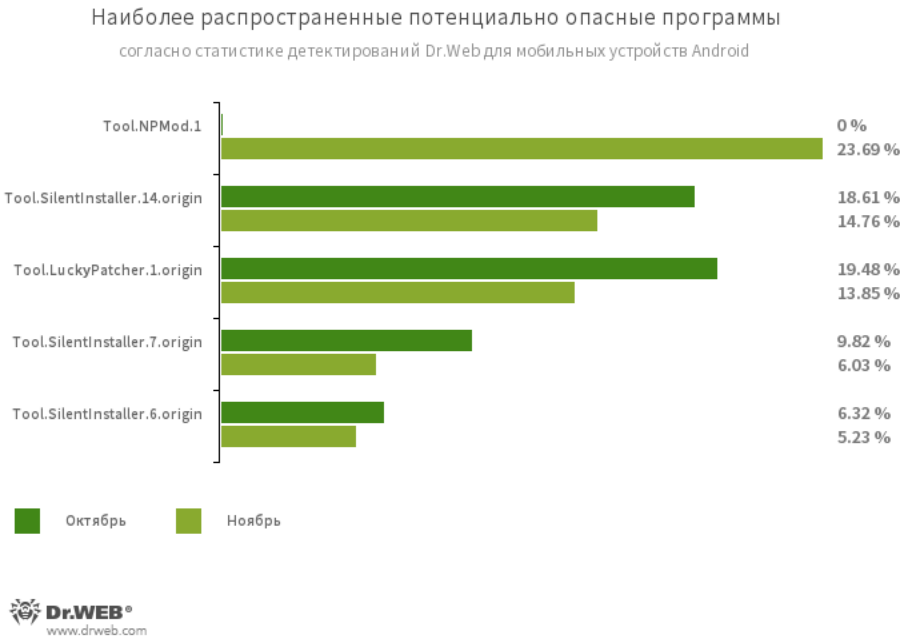
Детектирование приложений, якобы позволяющих зарабатывать на выполнении тех или иных действий или заданий. Эти программы имитируют начисление вознаграждений, причем для вывода «заработанных» денег требуется накопить определенную сумму. Даже когда пользователям это удается, получить выплаты они не могут.

Program.TrackView.1

Детектирование приложения, позволяющего вести наблюдение за пользователями через Android-устройства. С помощью этой программы злоумышленники могут определять местоположение целевых устройств, использовать камеру для записи видео и создания фотографий, выполнять прослушивание через микрофон, создавать аудиозаписи и т. д.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 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.SilentInstaller.14.origin

Tool.SilentInstaller.7.origin

Tool.SilentInstaller.6.origin

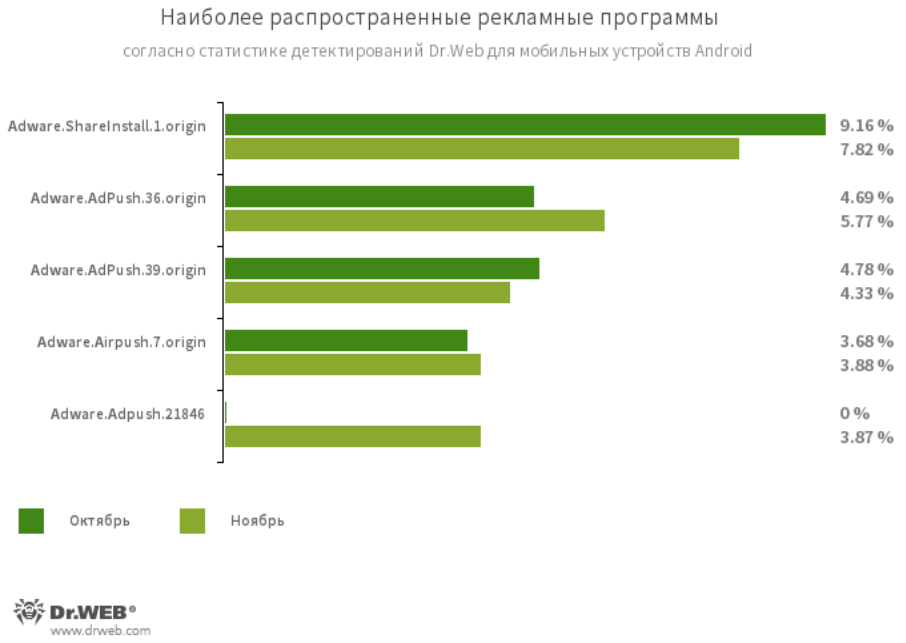
Потенциально опасные программные платформы, которые позволяют приложениям запускать APK-файлы без их установки. Эти платформы создают виртуальную среду исполнения в контексте приложений, в которые они встроены. Запускаемые с их помощью APK-файлы могут работать так, как будто являются частью таких программ,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

Tool.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.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 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.36.origin

Adware.AdPush.39.origin

Adware.Adpush.21846

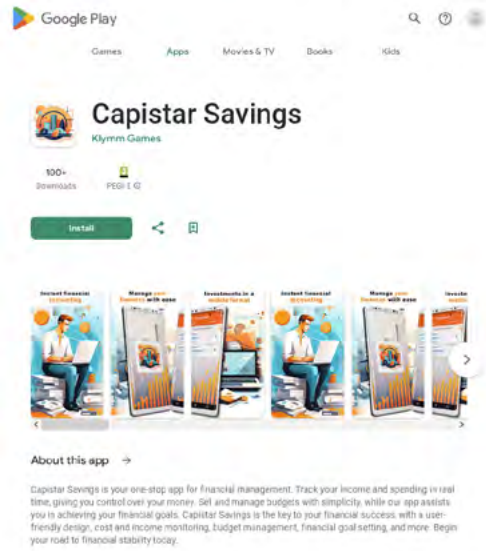
Рекламные модули, которые могут быть интегрированы в Android-программы. Они демонстрируют рекламные уведомления, вводящие пользователей в заблуждение. Например, такие уведомления могут быть похожи на сообщения от операционной системы. Кроме того, эти модули собирают ряд конфиденциальных данных, а также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

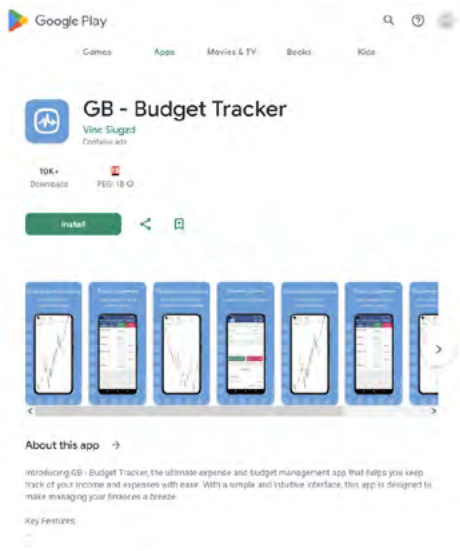
Adware.Airpush.7.origin

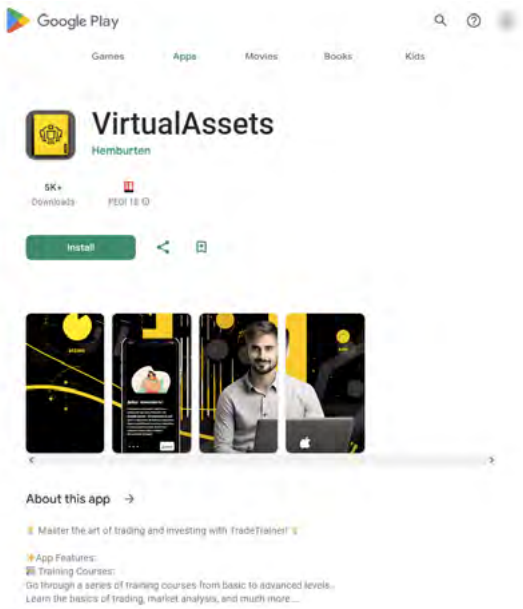
Представитель семейства рекламных модулей, встраиваемых в Android-приложения и демонстрирующих разнообразную рекламу. В зависимости от версии и модификации это могут быть рекламные уведомления, всплывающие окна или баннеры. С помощью данных модулей злоумышленники часто распространяют вредоносные программы,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

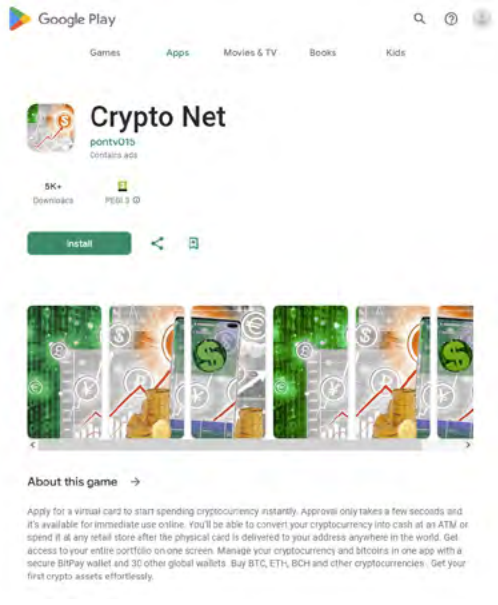
Угрозы в Google Play

В ноябре вирусная лаборатория компании «Доктор Веб» выявила в каталоге Google Play очередные вредоносные программы из семейства Android.FakeApp. Некоторые из них распространялись под видом программ финансовой тематики — обучающих и справочных приложений, домашних бухгалтерий, инструментов для доступа к инвестиционным сервисам и т. п. Среди них — Android.FakeApp.1497, Android.FakeApp.1498, Android.FakeApp.1499, Android.FakeApp.1526, Android.FakeApp.1527 и Android.FakeApp.1536. Их основной задачей является загрузка мошеннических сайтов, где пользователям предлагается стать инвесторами. Для этого те должны указать свои персональные данные.



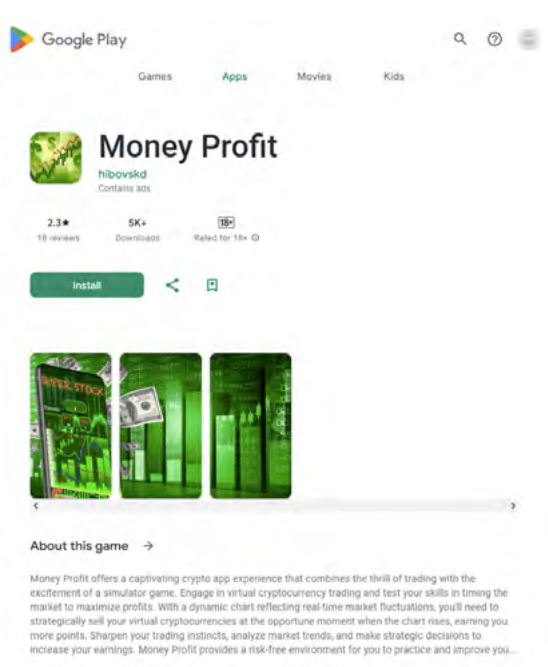


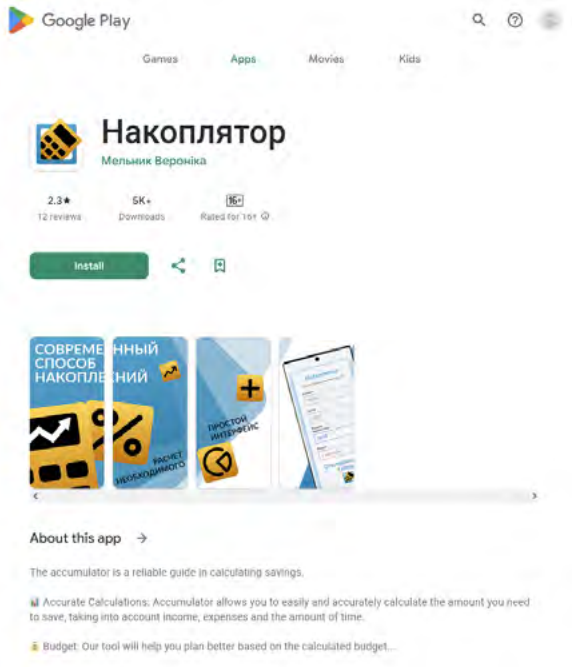




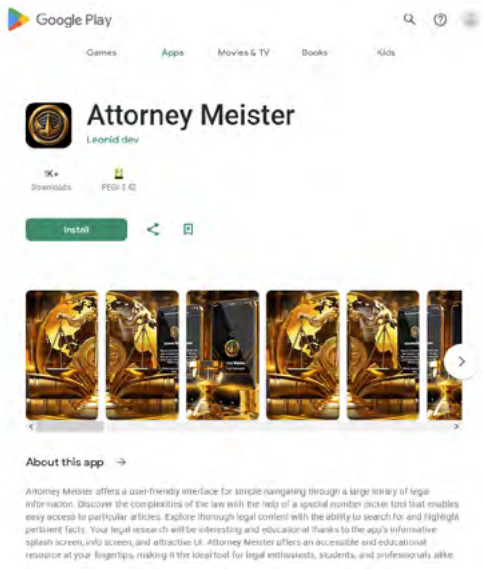
«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2023 года

Угрозы в Google Play



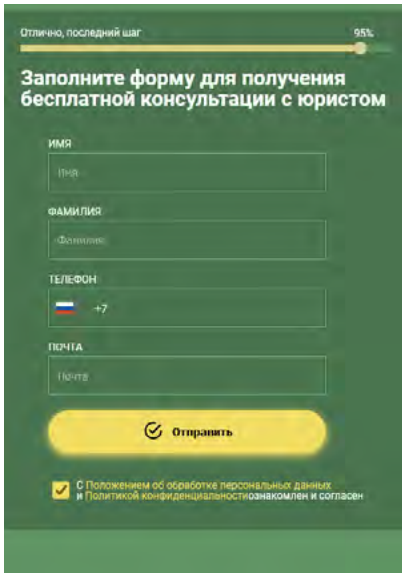


Еще одна программа-подделка, Android.FakeApp.1496, скрывалась в приложении-справочнике с доступом к правовой информации. Она могла загружать сайт, через который жертвы мошенников в сфере инвестиций якобы могли получить правовую помощь и вернуть утраченные деньги.

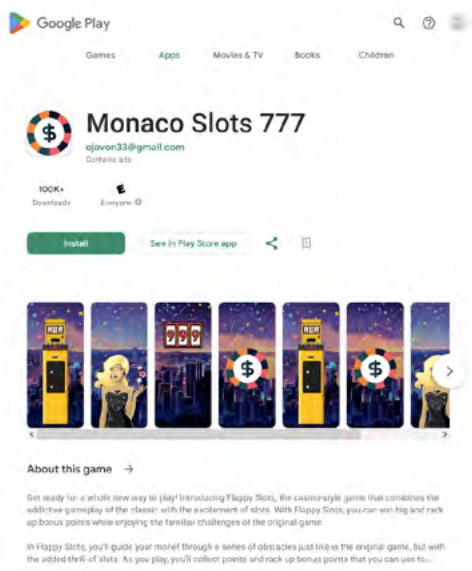


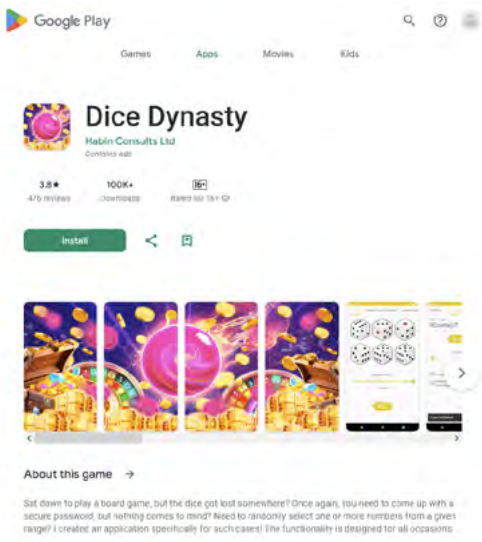
Угрозы в Google Play

Сайт, который загружала эта троянская программа, представлен ниже. Посетитель должен ответить на несколько вопросов, после чего заполнить форму для «получения бесплатной «консультации с юристом».

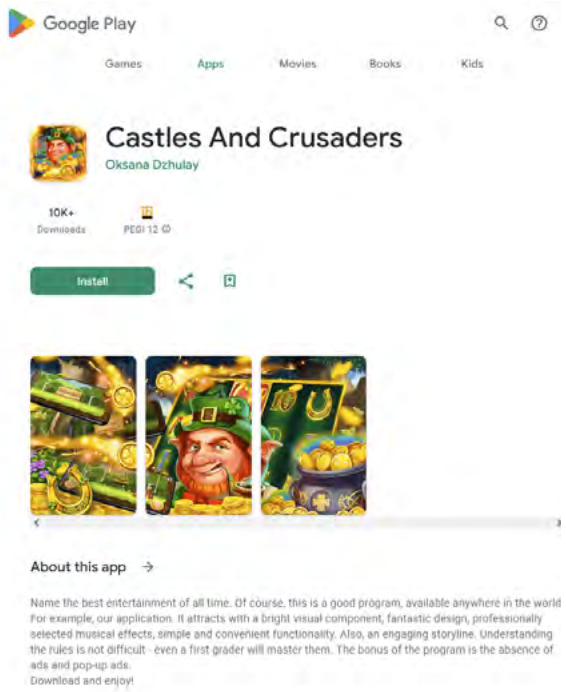


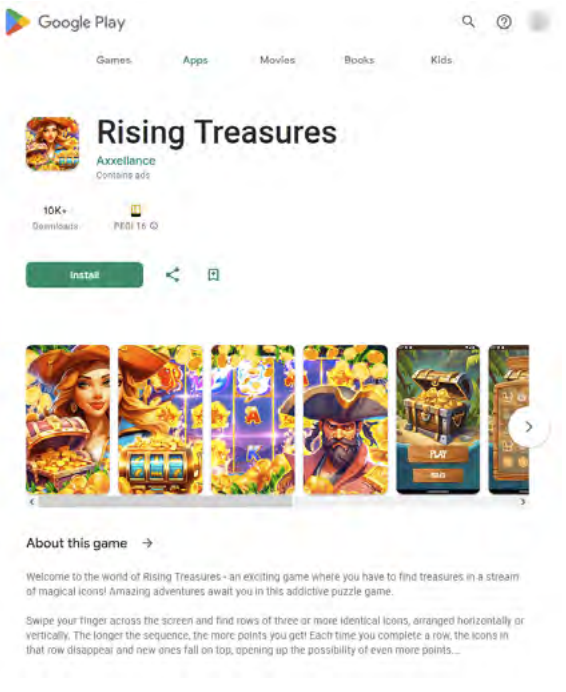
Другие программы-подделки злоумышленники вновь выдавали за игры. Например, Android.FakeApp.1494, Android.FakeApp.1503, Android.FakeApp.1504, Android.FakeApp.1533 и Android.FakeApp.1534. В ряде случаев они действительно работают как игры, однако их основная функция — загрузка сайтов онлайн-казино и букмекерских контор.

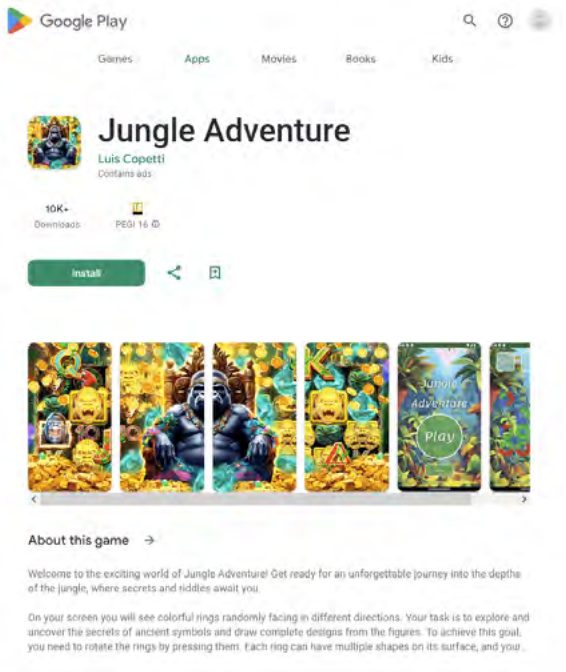


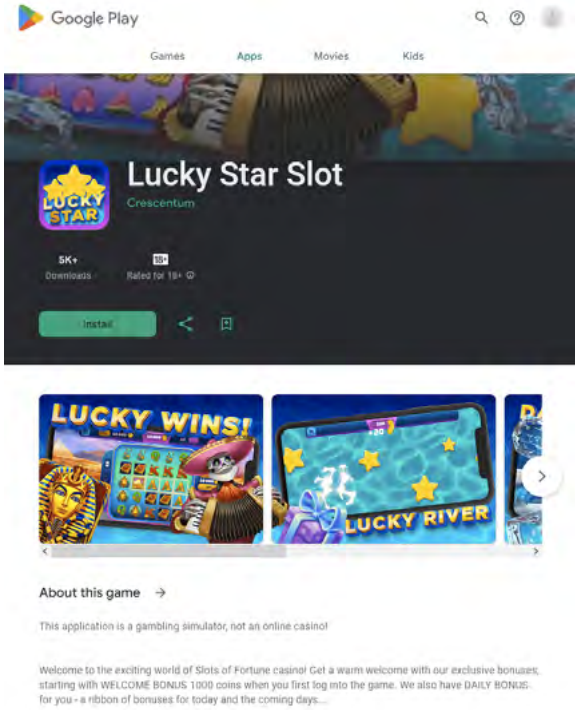


«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2023 года

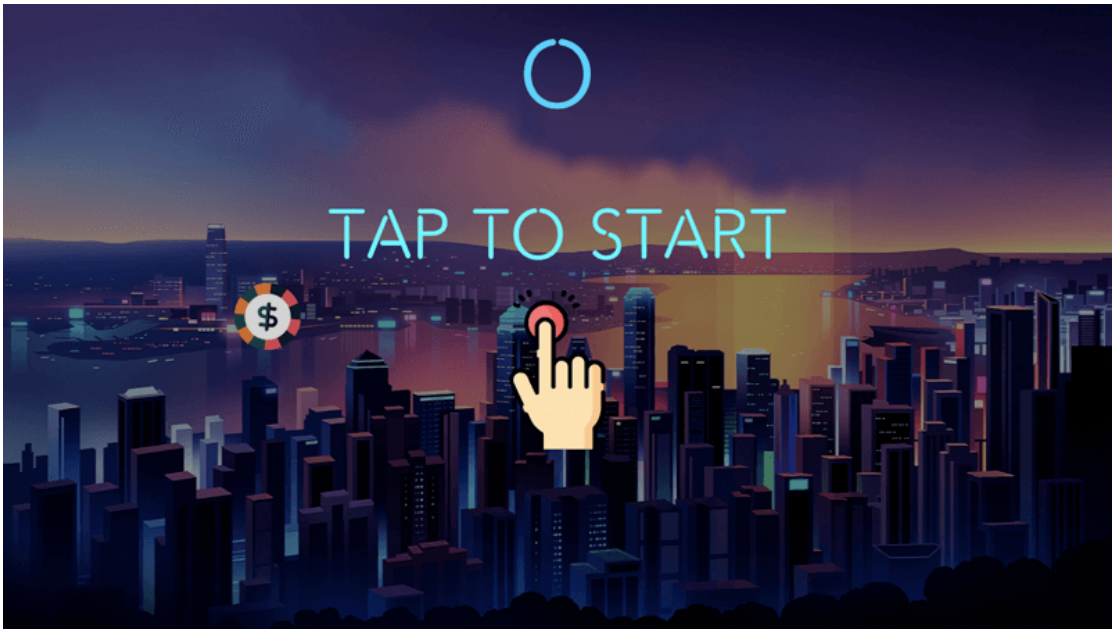


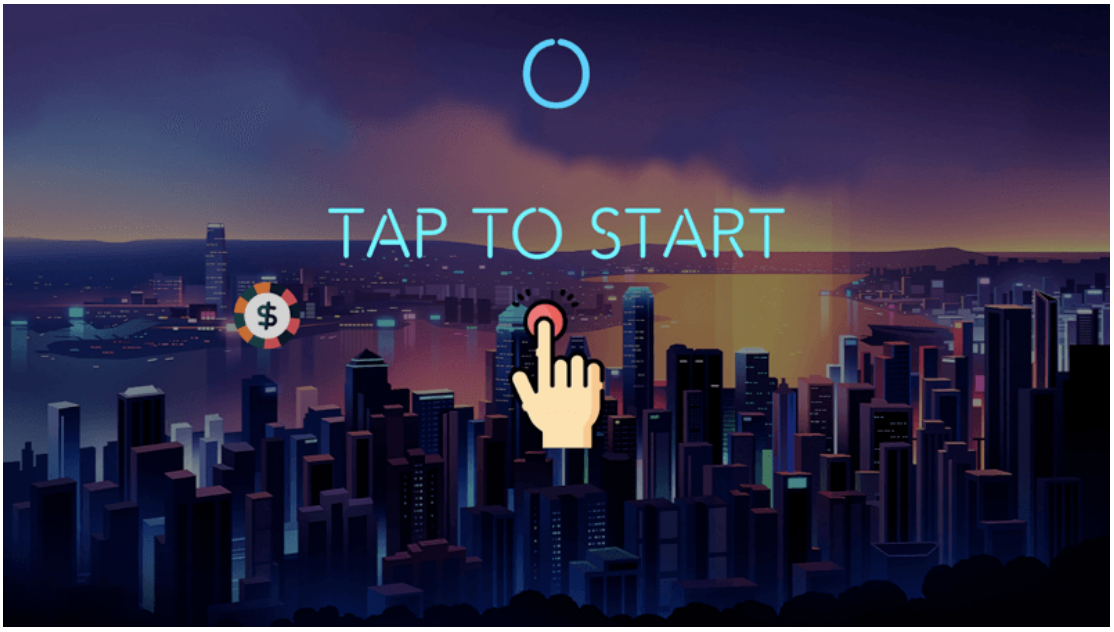






Примеры работы этих троянов в качестве игр:

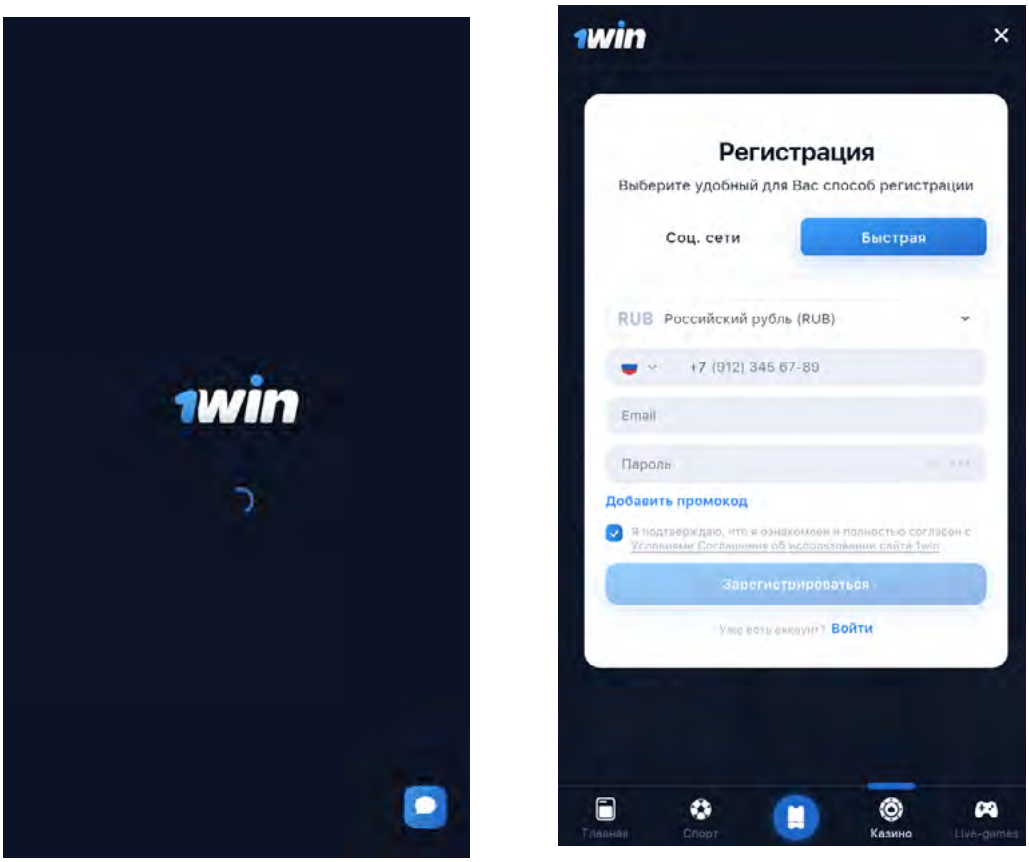




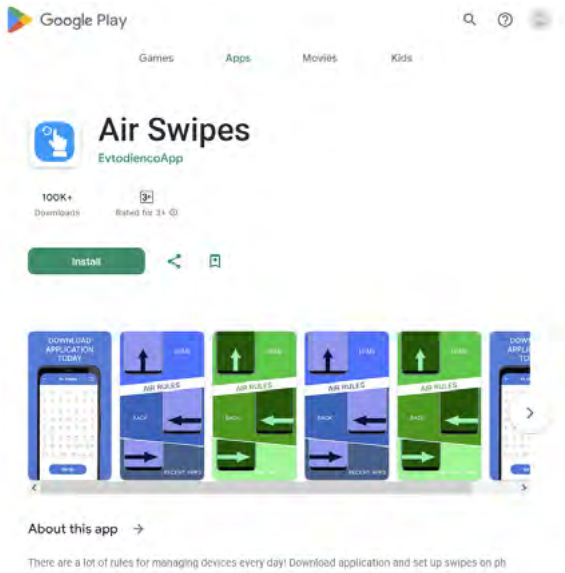

1 000
1
Fiesta
GOLDEN GOD


1 000
0
1
FREESPINS
0
10

Пример загруженного одним из них букмекерского сайта:

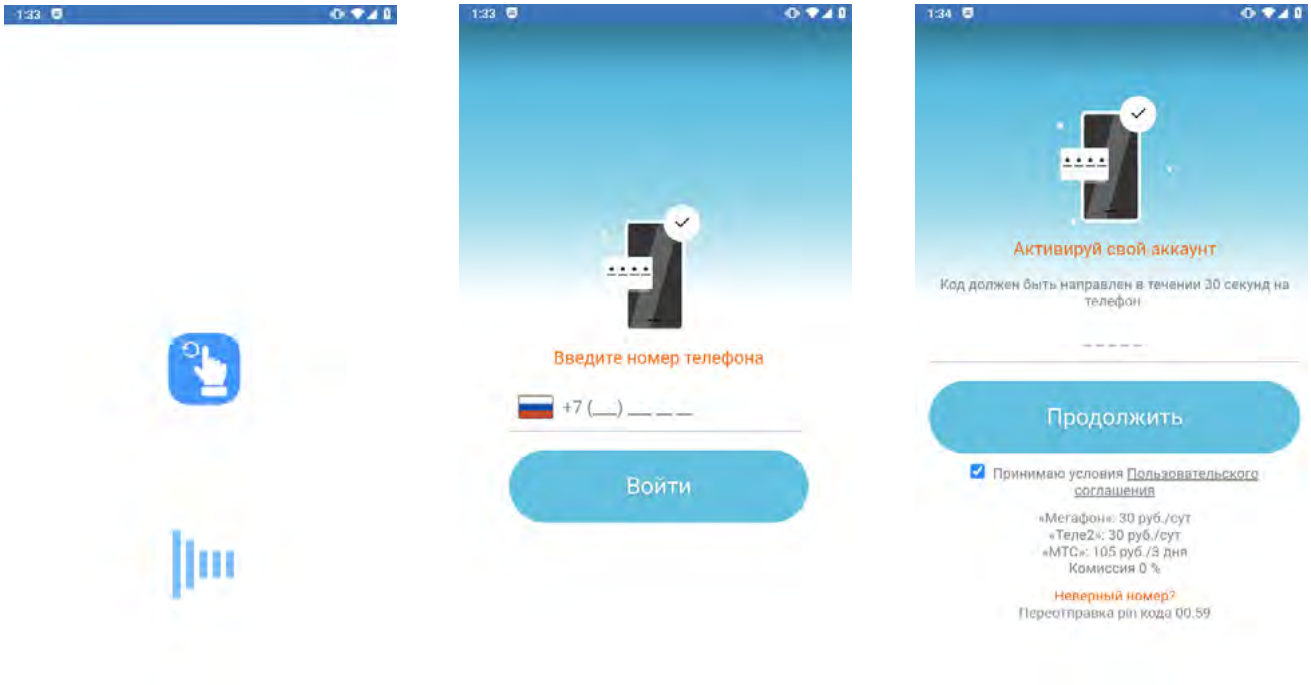


Также наши специалисты обнаружили очередную вредоносную программу, предназначенную для подключения пользователей к платным сервисам. Злоумышленники распространяли ее под видом приложения Air Swipes для управления Android-устройствами при помощи жестов.



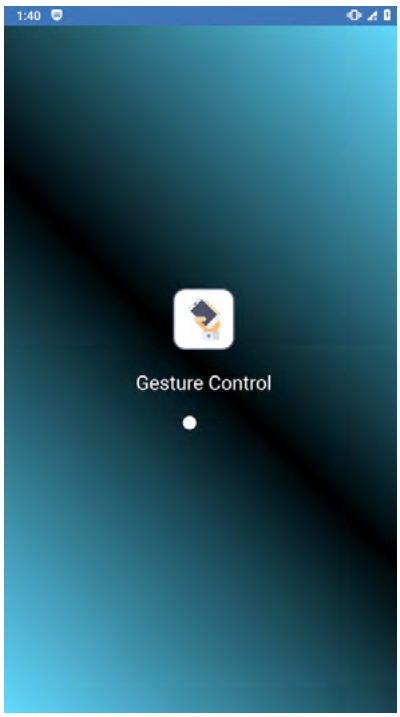
«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2023 года

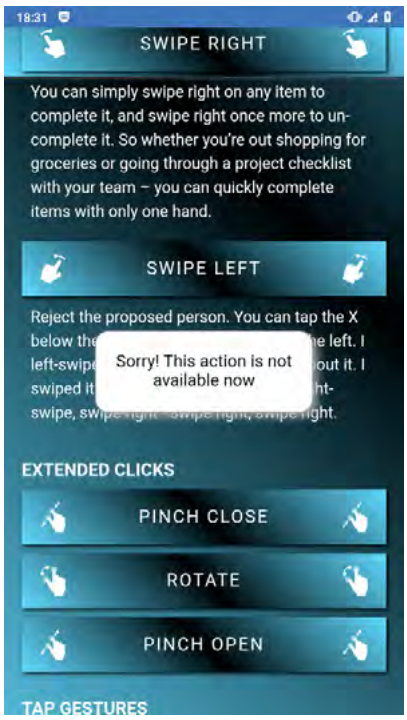
При запуске этот троян загружает сайт партнерского сервиса, через который оформляется подписка:



Если жертва запускает программу при отключенном доступе в интернет или если целевой сайт недоступен, программа выдает себя за обещанное приложение, но никакой полезной функциональности не предоставляет, сообщая об ошибке. Антивирус Dr.Web детектирует это троянское приложение как Android.Subscription.21.

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





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 ноябре 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