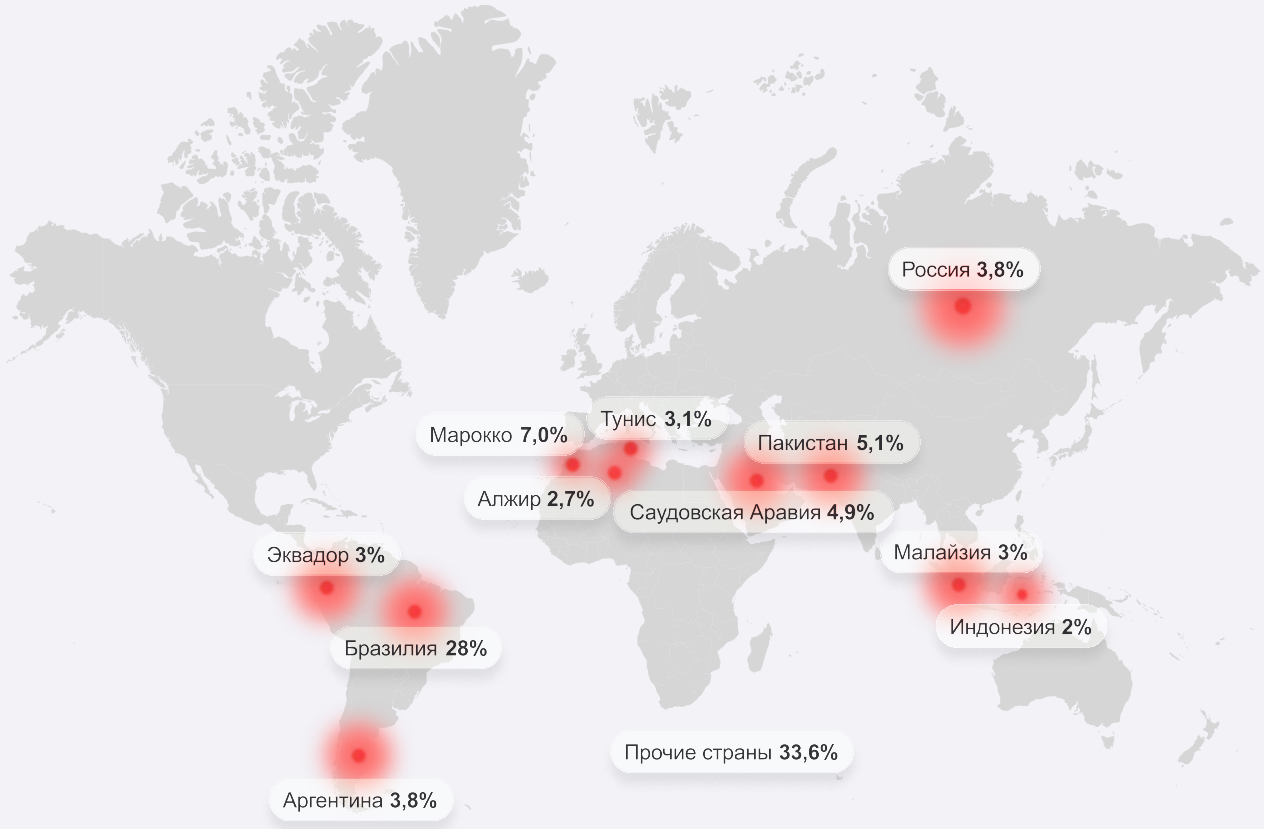
Dr.WEB

«Доктор Веб»: обзор вирусной активности для мобильных устройств в III квартале 2024 года

Главное

Согласно данным статистики детектирований Dr.Web Security Space для мобильных устройств, в III квартале 2024 года на защищаемых устройствах наиболее часто обнаруживались вредоносные приложения **Android.FakeApp**, которые злоумышленники используют в различных мошеннических схемах. На втором месте расположились рекламные трояны **Android.HiddenAds**. Третьими оказались представители семейства **Android.Siggen** — это программы, обладающие различной вредоносной функциональностью, которые сложно отнести к какому-либо конкретному семейству.

В августе специалисты «Доктор Веб» обнаружили бэкдор **Android.Vo1d**, который заразил почти 1 300 000 ТВ-приставок с ОС Android у пользователей из **197 стран**. Эта вредоносная программа помещает свои компоненты в системную область устройств и по команде злоумышленников способна незаметно загружать и устанавливать различные приложения.



Вместе с тем наши вирусные аналитики вновь выявили угрозы в каталоге Google Play. Среди них было множество новых программ-подделок, а также сразу несколько рекламных троянов.

Главные тенденции III квартала

Android.Vo1d

Бэкдор Android.Vo1d заразил более миллиона ТВ-приставок

Android.FakeApp

Высокая активность вредоносных программ **Android.FakeApp**, применяемых в мошеннических целях

Реклама

Высокая активность рекламных троянов **Android.HiddenAds**

Google Play

Появление новых вредоносных программ в каталоге Google Play

По данным Dr.Web Security Space для мобильных устройств

Android.FakeApp.1600

Троянская программа, которая загружает указанный в ее настройках веб-сайт. Известные модификации этого вредоносного приложения загружают сайт онлайн-казино.

Android.HiddenAds.3994

Троянская программа для показа навязчивой рекламы. Представители семейства Android.HiddenAds 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.7815

Android.MobiDash.7813

Троянские программы, показывающие надоедливую рекламу. Они представляют собой программные модули, которые 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.

Program.FakeMoney.11

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. Обычно в них имеется список популярных платежных систем и банков, через которые якобы возможно перевести награды. Но даже когда пользователям удается накопить достаточную для вывода сумму, обещанные выплаты им не поступают. Этой записью также детектируется другое нежелательное ПО, основанное на коде таких программ.

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 дистанционно 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.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.TrackView.1.origin

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.

Tool.Packer.1.origin

Специализированная утилита-упаковщик для защиты Android-приложений от модификации и обратного инжиниринга. Она не является вредоносной, но может использоваться для защиты как безобидных, так и троянских программ.

Tool.NPMod.1

Tool.NPMod.2

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.17.origin

Потенциально опасная программная платформа, которая позволяет приложениям запускать APK-файлы без их установки. Эта платформа создает 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.

Adware.ModAd.1

Детектирование некоторых модифицированных версий (модов) мессенджера WhatsApp, в функции которого внедрен код для загрузки заданных ссылок через веб-отображение во время работы с мессенджером. С этих интернет-адресов выполняется перенаправление на рекламируемые сайты — например, онлайн-казино и букмекеров, сайты для взрослых.

Adware.Basement.1

Приложения, демонстрирующие нежелательную рекламу, которая часто ведет на вредоносные и мошеннические сайты. Они имеют общую кодовую базу с нежелательными программами Program.FakeMoney.11.

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.

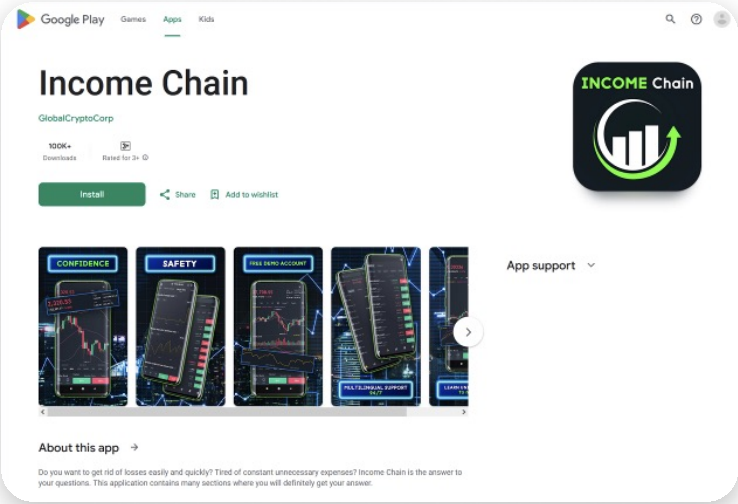
Adware.Adpush.21846

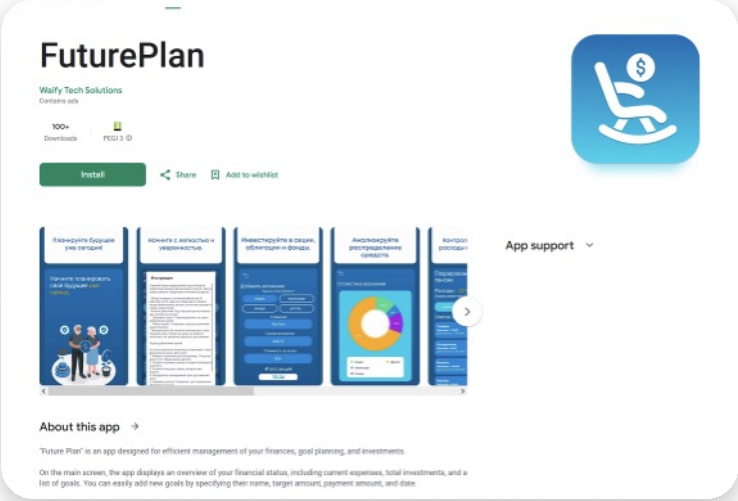
Adware.AdPush.39.origin

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.

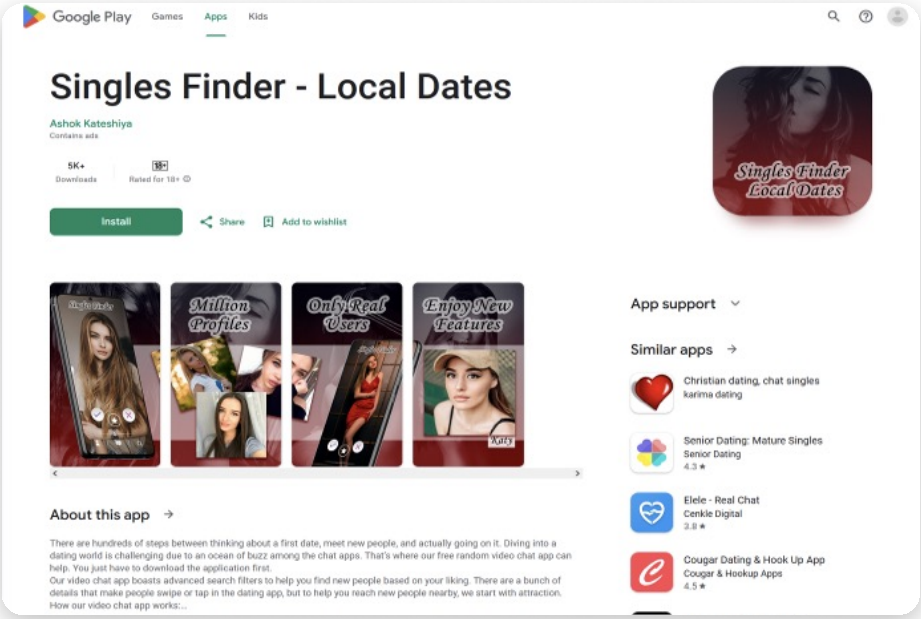
Угрозы в Google Play

В III квартале 2024 года вирусные аналитики «Доктор Веб» продолжили выявлять угрозы в каталоге Google Play. Среди них было множество новых вредоносных программ-подделок Android.FakeApp, которые распространялись под видом самого разнообразного ПО. Часть из них злоумышленники вновь выдавали за программы финансовой тематики — приложения для инвестирования, обучающие пособия по финансам, вариации домашних бухгалтерий и т. п. Некоторые из них действительно предоставляли заявленную функциональность, однако их основная задача — загрузить мошеннические сайты. На них потенциальным жертвам обещают легкий и быстрый заработок через инвестиции в акции, торговлю сырьевыми товарами, криптовалютой и т. п. Пользователям под видом доступа к «услуге» предлагается зарегистрировать учетную запись или оформить заявку для участия, указав персональные данные.

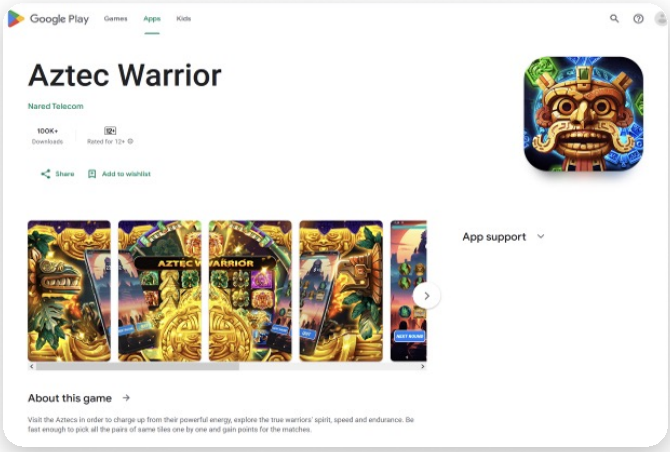


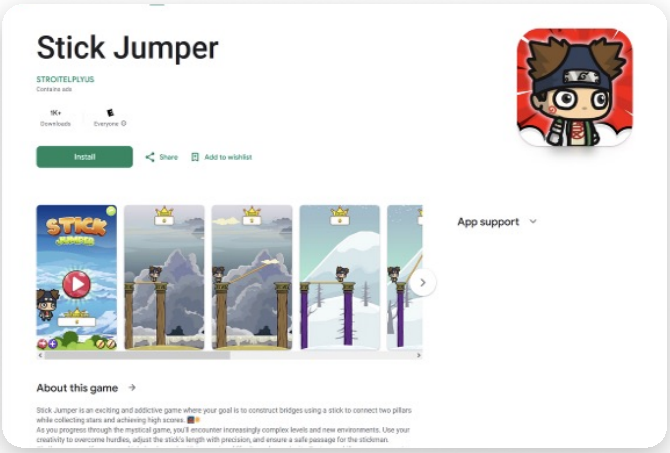


Примечательно, что один из троянов Android.FakeApp злоумышленники выдавали за программу для онлайн-знакомств и общения, однако он тоже загружал мошеннический сайт с «инвестициями».

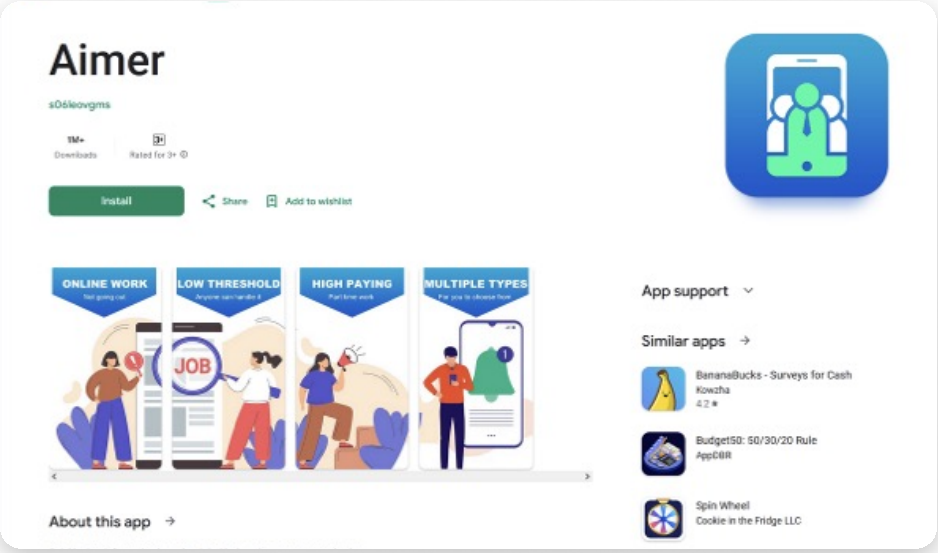


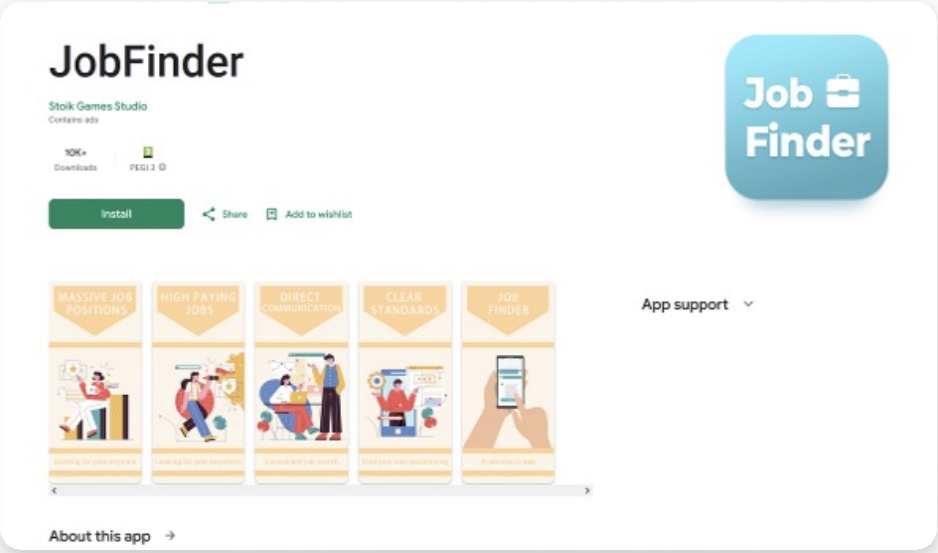
Другие трояны Android.FakeApp в очередной раз распространялись под видом игр. При определенных условиях они загружали сайты онлайн-казино и букмекеров.



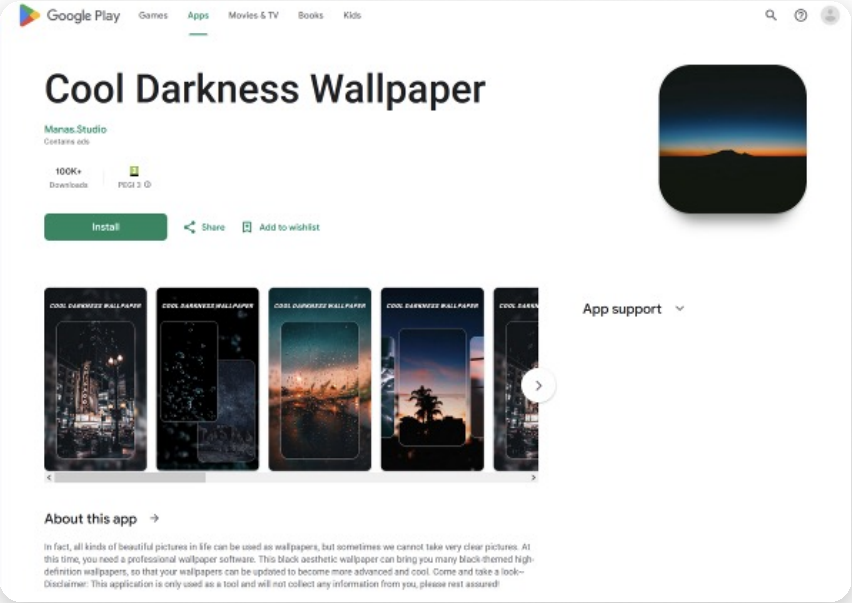


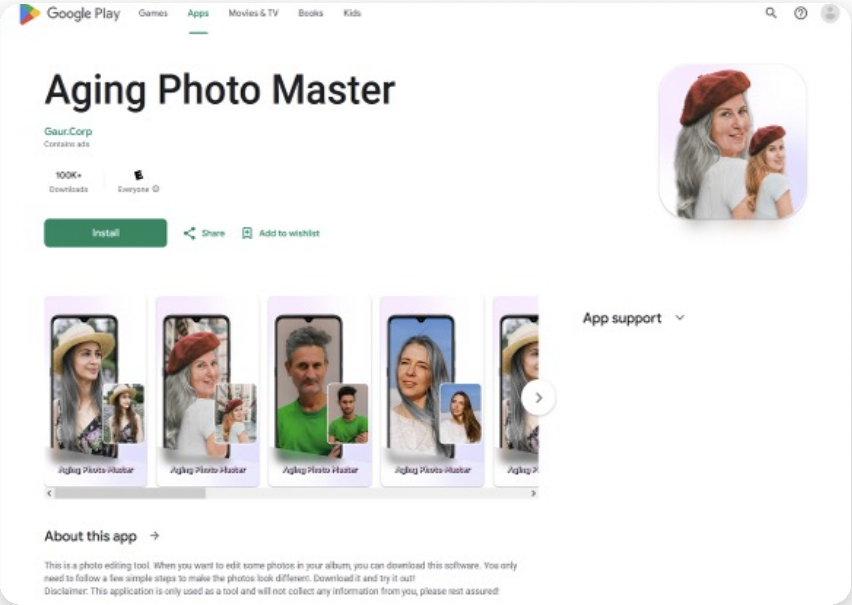
Среди программ-подделок наши специалисты выявили и новые варианты троянов, маскирующихся под инструменты для поиска работы. Такие вредоносные программы загружают поддельные списки вакансий и предлагают потенциальным жертвам через мессенджер связаться с «работодателем» (который на самом деле является мошенником) или составить «резюме», указав персональные данные.





Вирусные аналитики «Доктор Веб» также обнаружили в Google Play очередные трояны семейства Android.HiddenAds, которые скрывают свои значки в меню главного экрана и начинают показывать надоедливую рекламу. Они маскировались под приложения различных типов — сборники изображений, фоторедакторы, сканеры штрих-кодов.





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

Индикаторы компрометации

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
Антивирусная правда | Обучающие курсы | Просветительные проекты
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
«Доктор Веб» в других странах