Dr.WEB

«Доктор Веб»:

обзор вирусной активности для мобильных устройств в декабре 2022 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в декабре 2022 года

27 января 2023 года

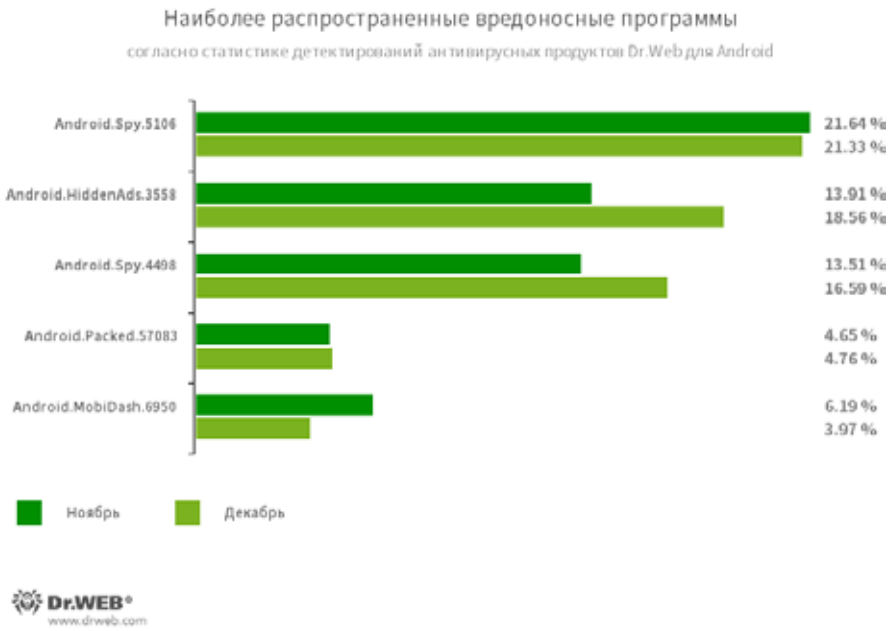
Согласно данным статистики детектирований антивируса Dr.Web для Android, в декабре 2022 года возросла активность рекламных троянских приложений, а также шпионских программ. В то же время в течение предыдущего месяца в каталоге Google Play было выявлено множество новых угроз, включая десятки программ-подделок, а также троянские приложения, подписывающие жертв на платные услуги.

ГЛАВНЫЕ ТЕНДЕНЦИИ ДЕКАБРЯ

- Рост активности вредоносных программ, демонстрирующих рекламу
- Рост активности шпионских приложений
- Обнаружение новых угроз в каталоге Google Play

«Доктор Веб»: обзор вирусной активности для мобильных устройств в декабре 2022 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, предназначенная 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.6950

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 декабре 2022 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.3

Program.FakeMoney.7

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

Program.SecretVideoRecorder.1.origin

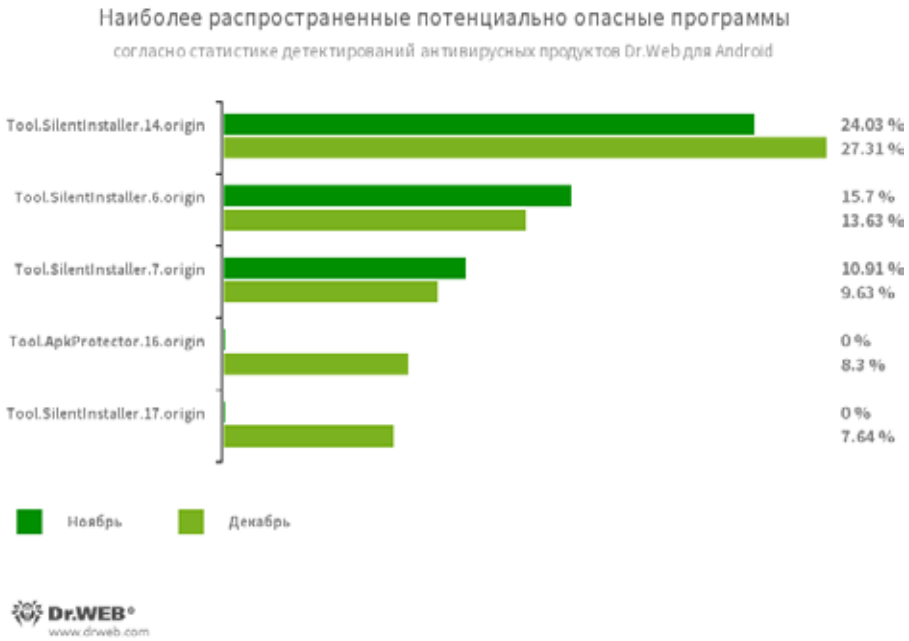
Детектирование различных версий приложения для фоновой фото- и видеосъемки через встроенные камеры Android-устройств. Эта программа может работать незаметно, позволяя отключить уведомления о записи, а также изменять значок и описание приложения на фальшивые. Такая функциональность делает ее потенциально опасной.

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.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в декабре 2022 года

По данным антивирусных продуктов Dr.Web для Android



Tool.SilentInstaller.14.origin

Tool.SilentInstaller.6.origin

Tool.SilentInstaller.7.origin

Tool.SilentInstaller.17.origin

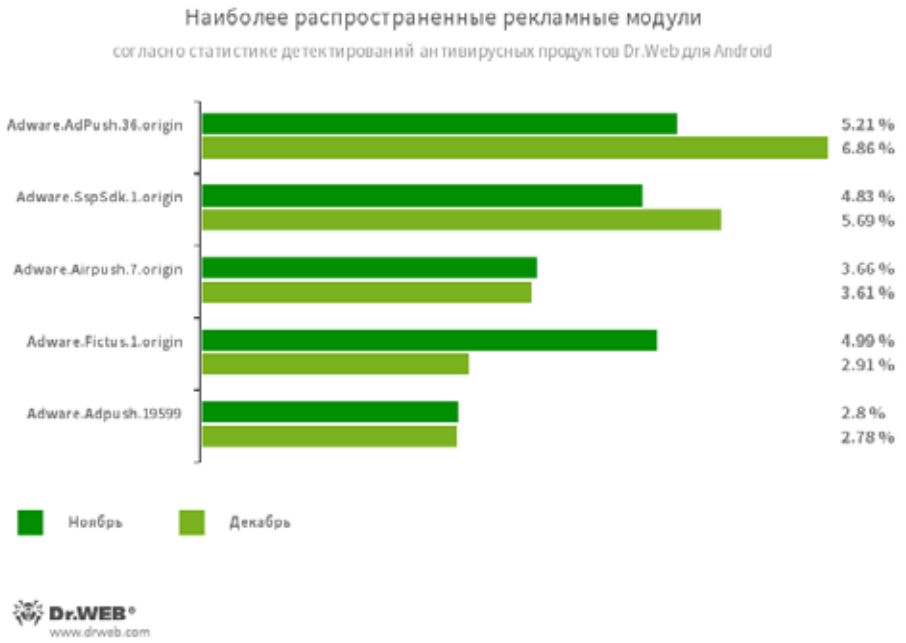
Потенциально опасные программные платформы, которые позволяют приложениям запускать APK-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

Tool.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 2022 года

По данным антивирусных продуктов Dr.Web для Android



Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать ярлыки и загружать веб-сайты.

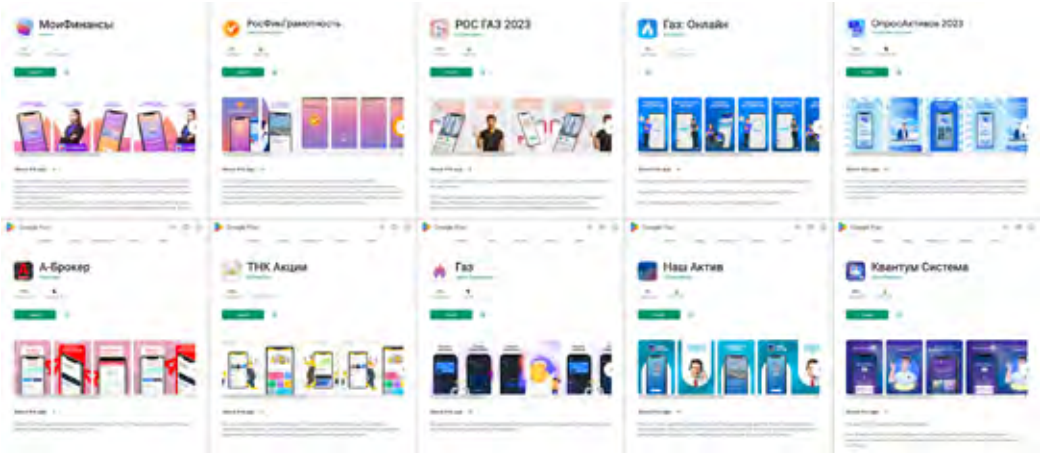
Adware.AdPush.36.origin
Adware.Adpush.19599
Adware.SspSdk.1.origin
Adware.Airpush.7.origin
Adware.Fictus.1.origin

«Доктор Веб»: обзор вирусной активности для мобильных устройств в декабре 2022 года

Угрозы в Google Play

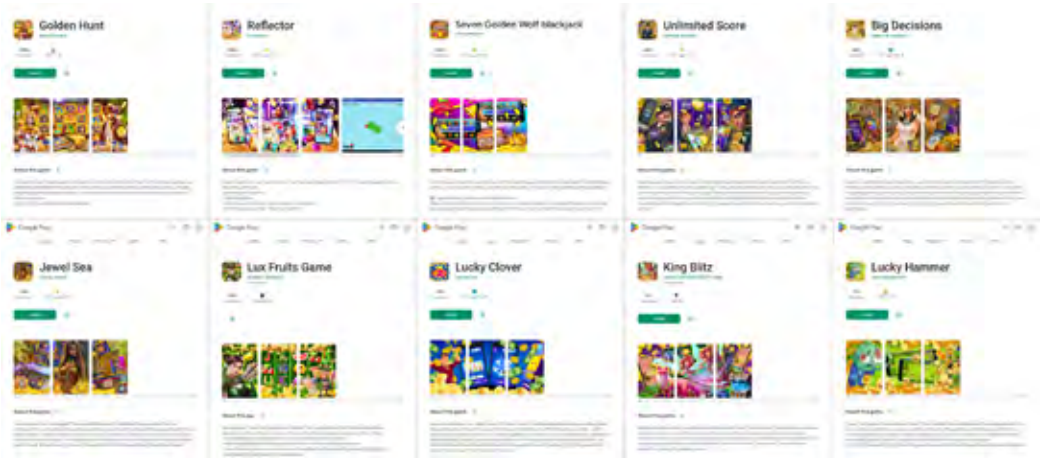
В декабре 2022 года специалисты компании «Доктор Веб» выявили множество новых угроз в каталоге Google Play. Среди них — десятки троянских программ из семейства Android.FakeApp. Они подключались к удаленному серверу и в соответствии с поступающими от него настройками вместо предоставления ожидаемых функций могли демонстрировать содержимое различных сайтов, в том числе фишинговых.

Некоторые из этих программ-подделок распространялись под видом инвестиционных приложений, справочников и опросников. С их помощью пользователи якобы могли повысить финансовую грамотность, вложить деньги в фондовый и криптовалютный рынки, напрямую торговать нефтью и газом и даже бесплатно получить акции крупных компаний. Вместо этого им предлагалось указать персональные данные для отправки «заявки» на регистрацию учетной записи или для связи со «специалистом».



Другие программы-подделки скрывались во множестве игр.

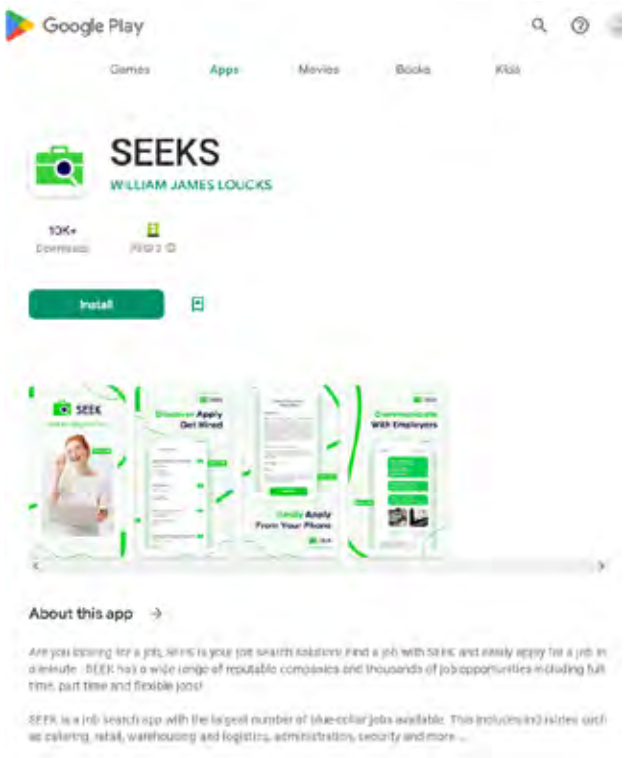
В зависимости от получаемой от управляющего сервера конфигурации они могли демонстрировать сайты различных онлайн-казино или безобидную игру, как показано на примерах ниже.



Угрозы в Google Play

В зависимости от получаемой от управляющего сервера конфигурации они могли демонстрировать сайты различных онлайн-казино или безобидную игру, как показано на примерах ниже.

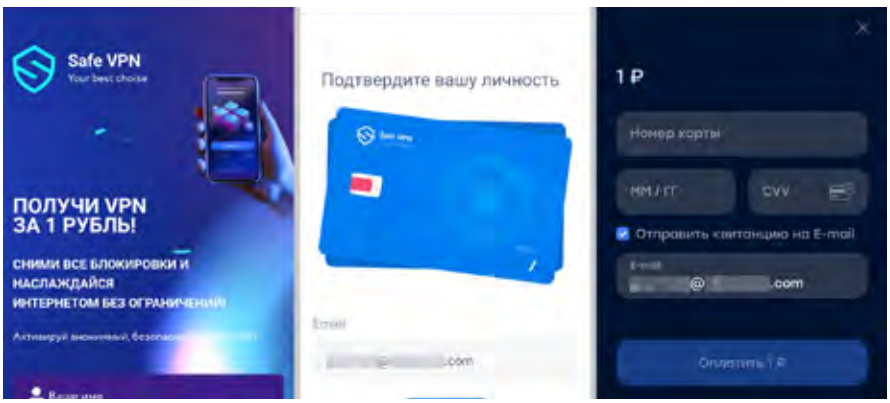
Также была выявлена очередная программа-подделка, которая распространялась под видом приложения для поиска работы под названием SEEKS. На самом деле она загружала веб-сайты с вымышленными вакансиями и заманивала потенциальных жертв в руки мошенников. Эта подделка была добавлена в вирусную базу Dr.Web как Android.FakeApp.1133.



Получившую имя Android.FakeApp.1141 вредоносную программу злоумышленники выдавали за VPN-клиент Safe VPN. На самом деле это было поддельное приложение.

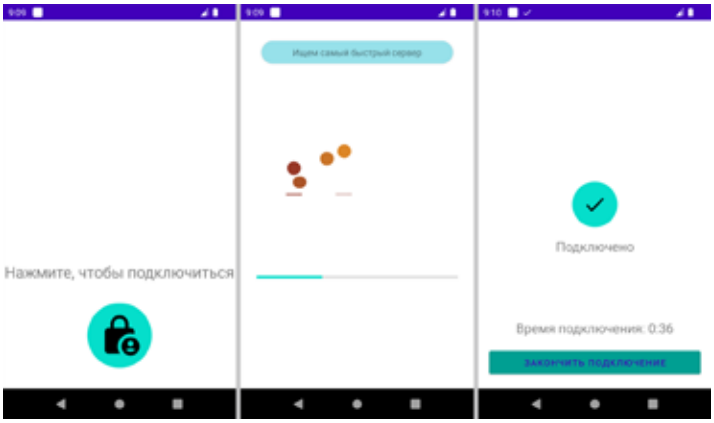
Угрозы в Google Play

Программа при запуске демонстрировала содержимое сайта, на котором потенциальным жертвам предлагалось всего за 1 рубль получить доступ к VPN-сервису. Для этого от них требовалось создать учетную запись и произвести оплату банковской картой. В действительности они приобретали пробную трехдневную версию услуги, и по истечении пробного периода с их счета ежедневно должна была списываться сумма в 140 рублей. Информация об этих условиях присутствовала на сайте, однако располагалась таким образом, что большинство жертв этой схемы обмана могло ее не заметить.

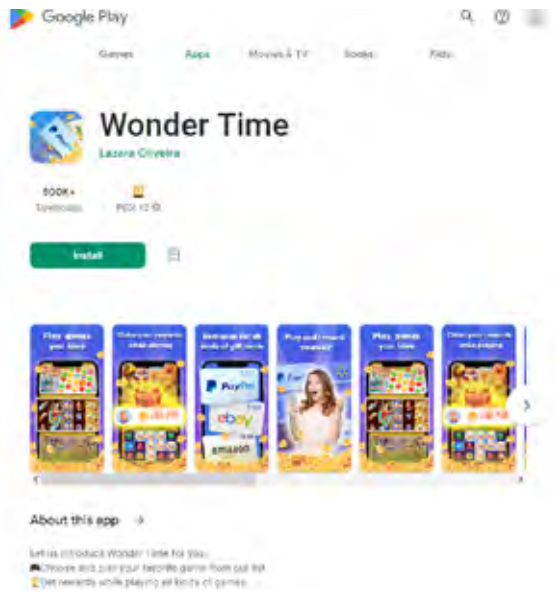


При этом данное приложение имитировало возможность подключения к защищенной сети, уведомляя пользователей об успешном соединении. На самом деле это был обман — заявленная функциональность в программе отсутствовала.

Угрозы в Google Play



Были обнаружены и очередные мошеннические программы, которые якобы позволяли зарабатывать на выполнении тех или иных заданий. Так, приложение Wonder Time предлагало устанавливать, запускать и использовать другие программы и игры. За это пользователи получали виртуальное вознаграждение — токены, которые якобы можно было обменять на настоящие деньги. Однако, чтобы вывести «заработанное», требовалось накопить миллионы наград, в то время как за выполнение заданий начислялись лишь небольшое количество токенов. Таким образом, даже если пользователи могли собрать требуемую сумму, они затратили бы на это намного больше времени, сил и других ресурсов по сравнению с ожидаемой выгодой. В зависимости от версии это приложение детектируется Dr.Web как Program.FakeMoney.4, Program.FakeMoney.5 и Program.FakeMoney.6.

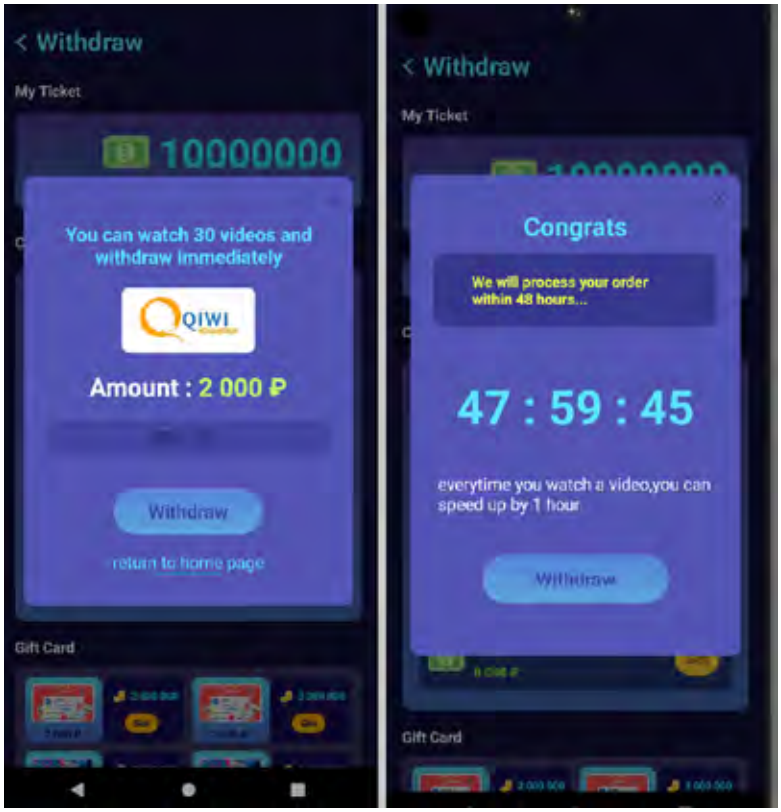


Угрозы в Google Play

Несколько программ с аналогичным принципом работы были внесены в вирусную базу Dr.Web как Program.FakeMoney.7. Например, этой записью детектируются приложения Lucky Habit: health tracker, WalkingJoy и некоторые версии Lucky Step-Walking Tracker. Первая распространялась в качестве программы для выработки полезных привычек, другие — как шагомеры. Они начисляли виртуальное вознаграждение («тикеты» или «монеты») за различные достижения — пройденное пользователями расстояние, соблюдение распорядка дня и т. д., а также позволяли получать дополнительные начисления за просмотр рекламы.

Как и в предыдущем случае, для начала процесса вывода заработанных наград было необходимо накопить их существенный объем. Если собрать необходимую сумму пользователю удавалось, программы дополнительно требовали просмотреть несколько десятков рекламных роликов. Затем они предлагали просмотреть еще несколько десятков объявлений, чтобы «ускорить» процесс вывода. При этом проверка корректности указываемых пользователем платежных данных не проводилась, поэтому вероятность получения им каких-либо выплат от этих программ крайне мала.

Угрозы в Google Play

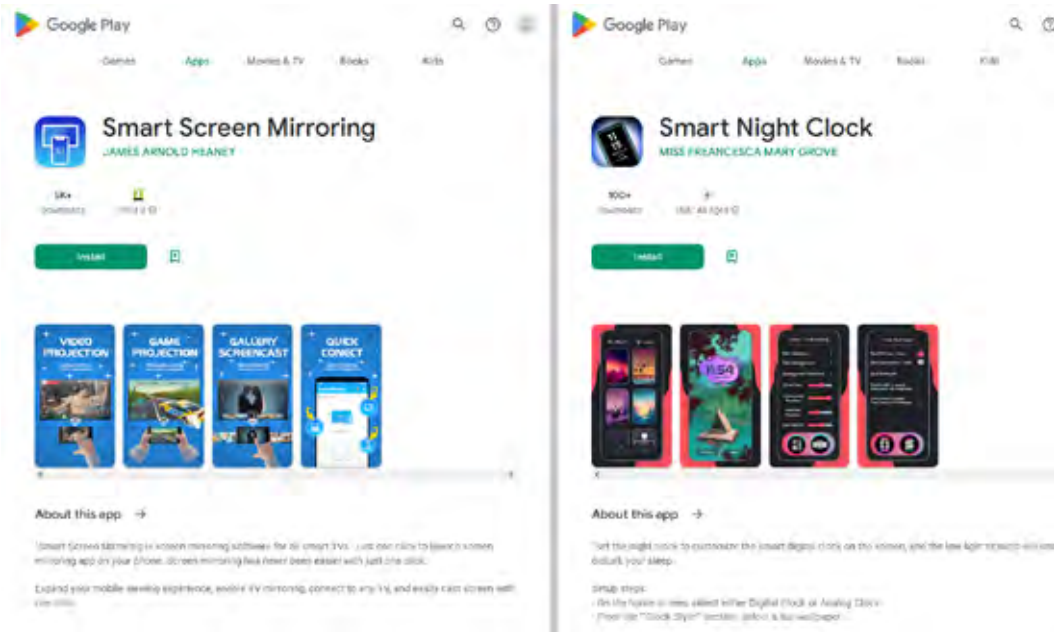


Более того, ранние версии Lucky Step-Walking Tracker, которые детектирует антивирус Dr.Web, предлагали конвертировать награду в подарочные карты интернет-магазинов. Однако с выходом обновления приложения разработчики убрали возможность обмена наград на настоящие деньги, избавившись от соответствующих элементов интерфейса. В результате все ранее накопленные начисления фактически стали бесполезными цифрами. При этом и Lucky Habit: health tracker, и Lucky Step-Walking Tracker, и WalkingJoy имеют общий управляющий сервер [string]richox[.]net[/string]. Это может говорить о том, что они связаны друг с другом, и что пользователи Lucky Habit: health tracker и WalkingJoy в любой момент также могут лишиться всех надежд на получение выплат.

Среди обнаруженных угроз также оказались и новые троянские приложения из семейства Android.Joker, которые подписывают жертв на платные услуги. Они скрывались в таких программах как Document PDF Scanner (Android.Joker.1941), Smart Screen Mirroring (Android.Joker.1942) и Smart Night Clock (Android.Joker.1949).

«Доктор Веб»: обзор вирусной активности для мобильных устройств в декабре 2022 года

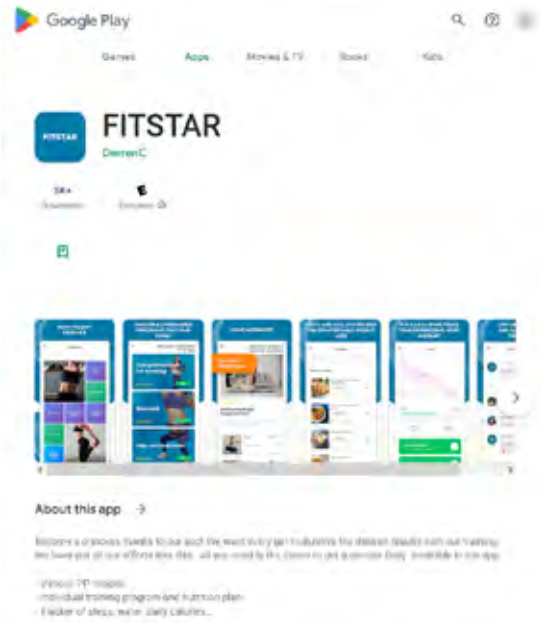
Угрозы в Google Play



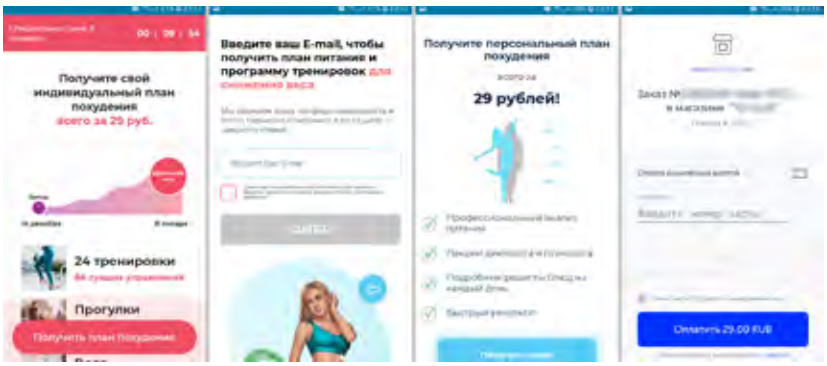
Кроме того, в каталоге Google Play распространялась программа FITSTAR, позиционируемая как фитнес-приложение.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в декабре 2022 года

Угрозы в Google Play



При запуске она загружала веб-сайты, где пользователям за относительно небольшие деньги — 29 рублей — предлагалось приобрести индивидуальные планы похудения. При этом в действительности указанная цена не была окончательной. За эти деньги они лишь приобретали пробный доступ к сервису на 1 день. По окончании пробного периода выполнялось автоматическое продление подписки на 4 дня — уже за 980 рублей. Стоимость же полного доступа к сервису могла достигать 7000 рублей, при этом предполагалось дальнейшее автоматическое продление имеющейся подписки.
Таким образом, установившие данную программу владельцы Android-устройств по неосторожности могли лишиться существенной суммы денег. Это приложение было добавлено в вирусную базу Dr.Web как Program.Subscription.1.



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

«Доктор Веб»: обзор вирусной активности для мобильных устройств в декабре 2022 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