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

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

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в июне 2023 года активность рекламных троянских программ семейства Android.HiddenAds возросла на 10,93%. В то же время рекламные вредоносные приложения семейства Android.MobiDash обнаруживались на защищаемых устройствах реже на 15,94%. По сравнению с маем число атак шпионских троянских программ снизилось на 47,15%, а банковских троянов — на 12,23%. Вместе с тем пользователи на 46,30% чаще сталкивались с вредоносными программами-вымогателями семейства Android.Locker.

В июне в каталоге Google Play были выявлены очередные угрозы. Среди них — вредоносные программы-подделки из семейства Android.FakeApp, а также троянские приложения Android.Joker, подписывающие жертв на платные сервисы.

Главные тенденции июня

- Рост активности рекламных троянских программ Android.HiddenAds
- Снижение активности рекламных троянских программ Android.MobiDash
- Снижение активности шпионских вредоносных приложений и банковских троянов
- Новые угрозы в каталоге Google Play

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

По данным антивирусных продуктов Dr.Web для Android

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.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.Packed.57083

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

Android.MobiDash.7795

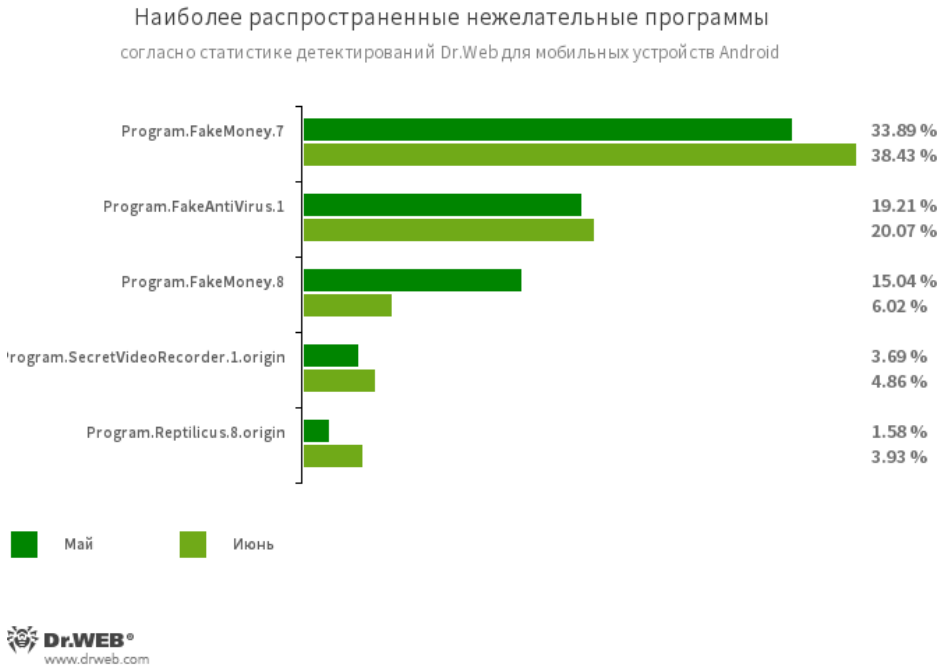
Троянская программа, показывающая надоедливую рекламу. Она представляет собой программный модуль, который разработчики ПО встраивают в приложения.

Android.Pandora.7

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.

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

По данным антивирусных продуктов Dr.Web для Android



Program.FakeMoney.7

Program.FakeMoney.8

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

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

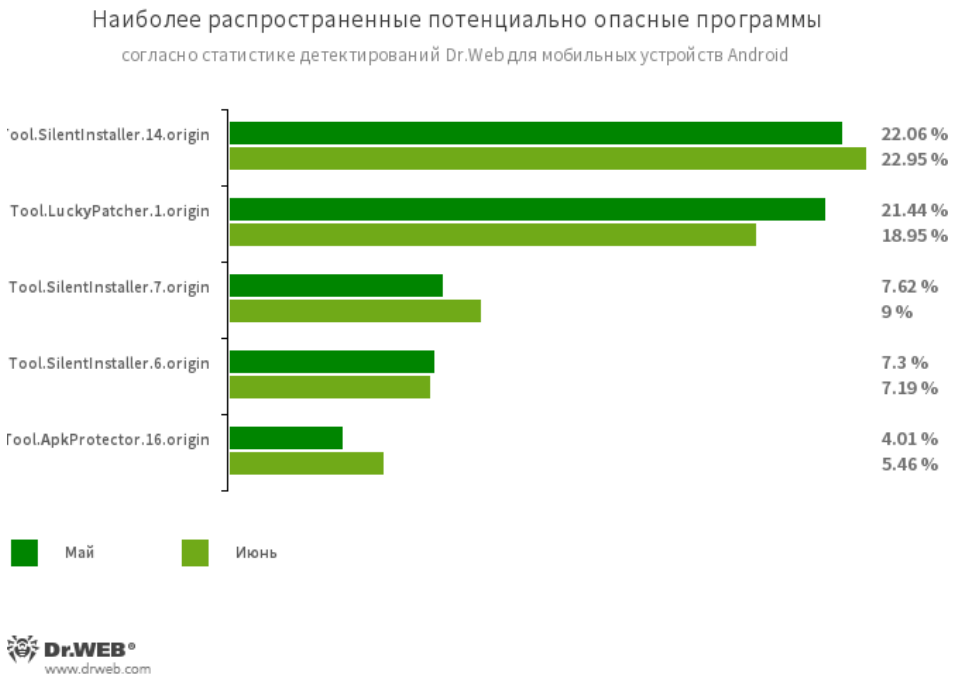
Детектирование различных версий приложения для фоновой фото- и видеосъемки через встроенные камеры Android-устройств. Эта программа может работать незаметно, позволяя отключить уведомления о записи, а также изменять значок и описание приложения на фальшивые. Такая функциональность делает ее потенциально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

Program.Reptilicus.8.origin

Приложение, позволяющее следить за владельцами Android-устройств. Оно способно контролировать местоположение устройства, собирать данные об СМС-переписке и беседах в социальных сетях, прослушивать телефонные звонки и окружение, создавать снимки экрана, отслеживать вводимую на клавиатуре информацию, копировать файлы с устройства и выполнять другие действия.

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

По данным антивирусных продуктов Dr.Web для Android



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. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

Tool.LuckyPatcher.1.origin

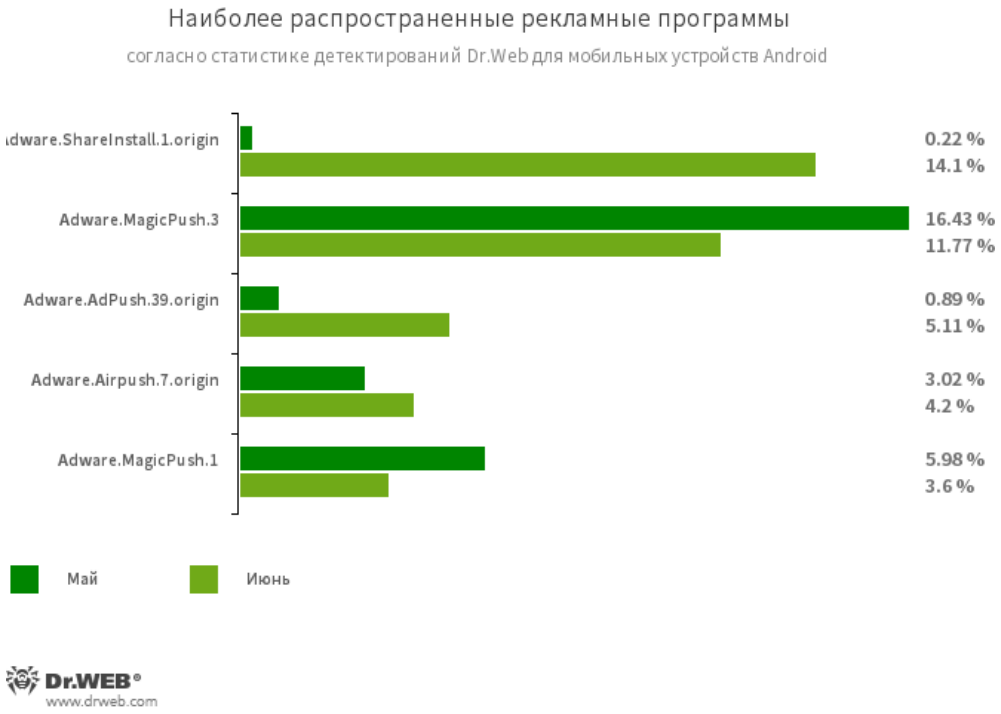
Утилита, позволяющая модифицировать установленные Android-приложения (создавать для них патчи) с целью изменения логики их работы или обхода тех или иных ограничений. Например, с ее помощью пользователи могут пытаться отключить проверку root-доступа в банковских программах или получить неограниченные 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.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 июне 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.MagicPush.3

Adware.MagicPush.1

Рекламные модули, встраиваемые в Android-приложения. Они демонстрируют 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 пользователь видит рекламу.

Adware.AdPush.39.origin

Рекламный модуль, который может быть интегрирован в Android-программы. Он демонстрирует рекламные уведомления, вводящие пользователей в заблуждение. Например, такие

уведомления могут быть похожи на сообщения от операционной системы. Кроме того, этот модуль собирает ряд конфиденциальных данных, а также способен загружать другие приложения и инициировать их установку.

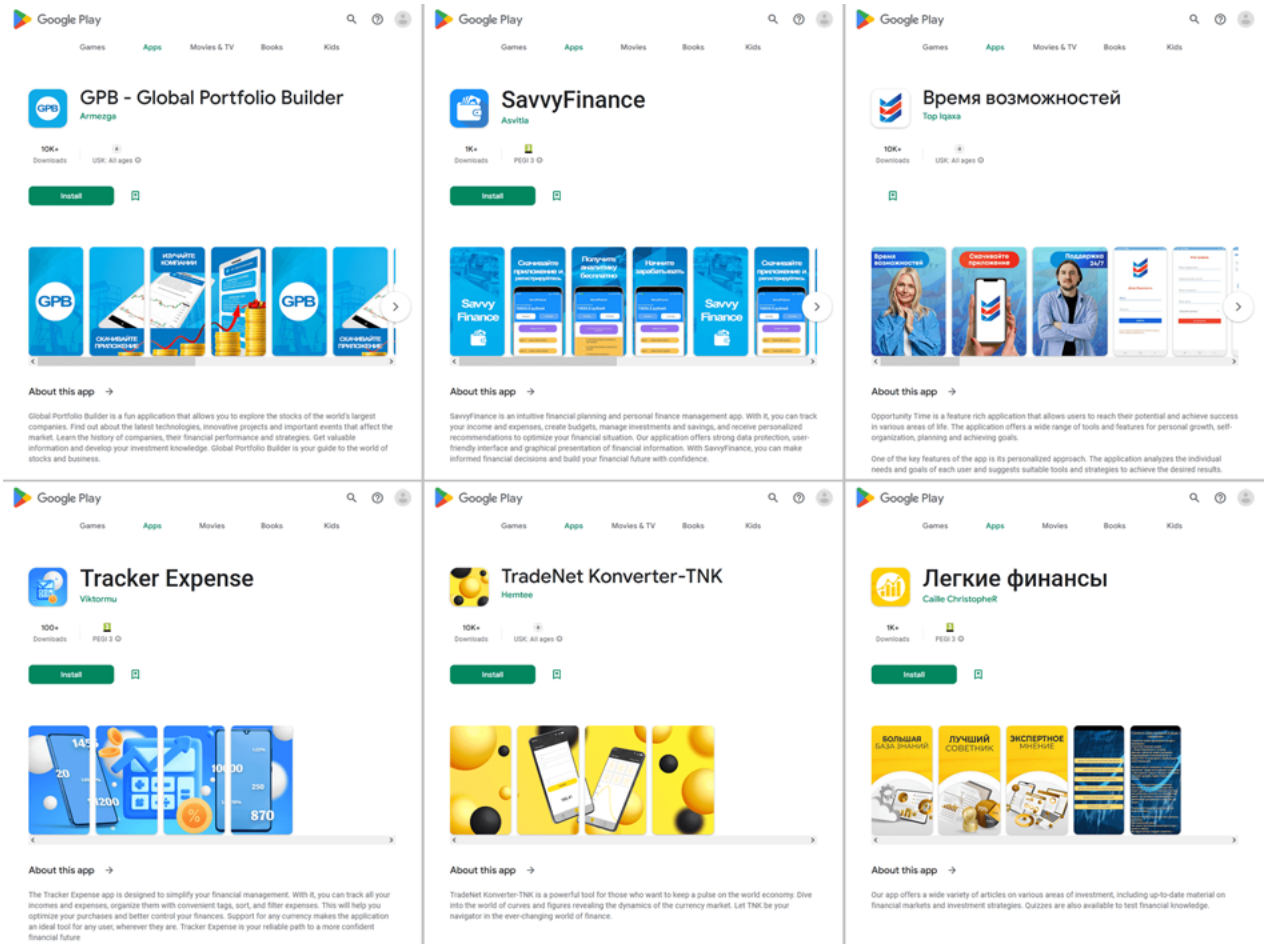
Adware.Airpush.7.origin

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 июне 2023 года

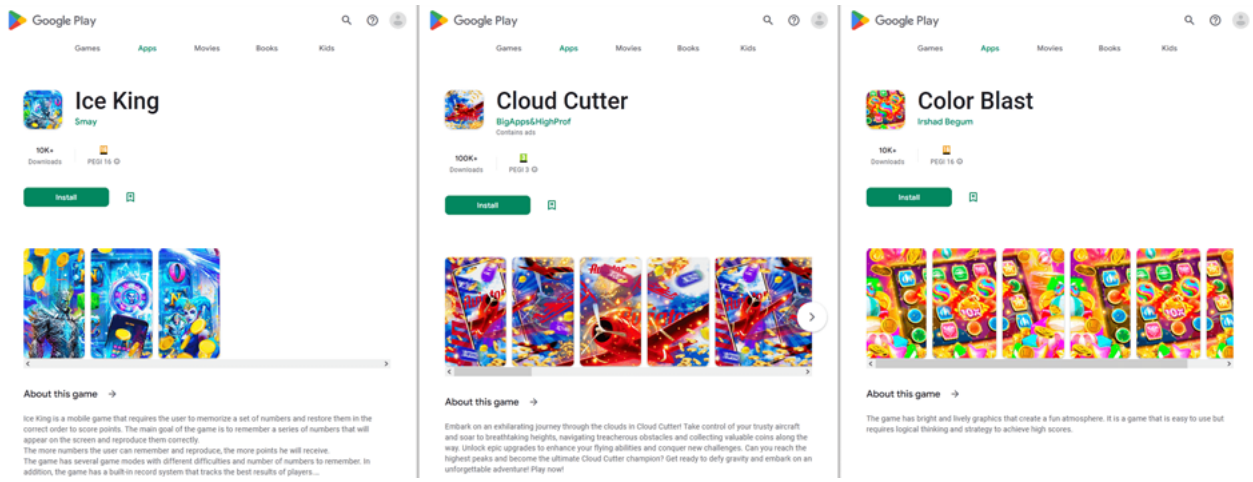
Угрозы в Google Play

В июне 2023 года специалисты компании «Доктор Веб» вновь обнаружили в каталоге Google Play троянские приложения семейства Android.FakeApp. Часть из них распространялась под видом программ финансовой тематики — справочников и пособий, домашней бухгалтерии, ПО для доступа к биржевой информации и т. д. Например, Android.FakeApp.1382, Android.FakeApp.1383, Android.FakeApp.1384, Android.FakeApp.1385, Android.FakeApp.1386, Android.FakeApp.1387 и другие. На самом деле их основной функцией была загрузка мошеннических сайтов, якобы имеющих отношение к инвестициям.

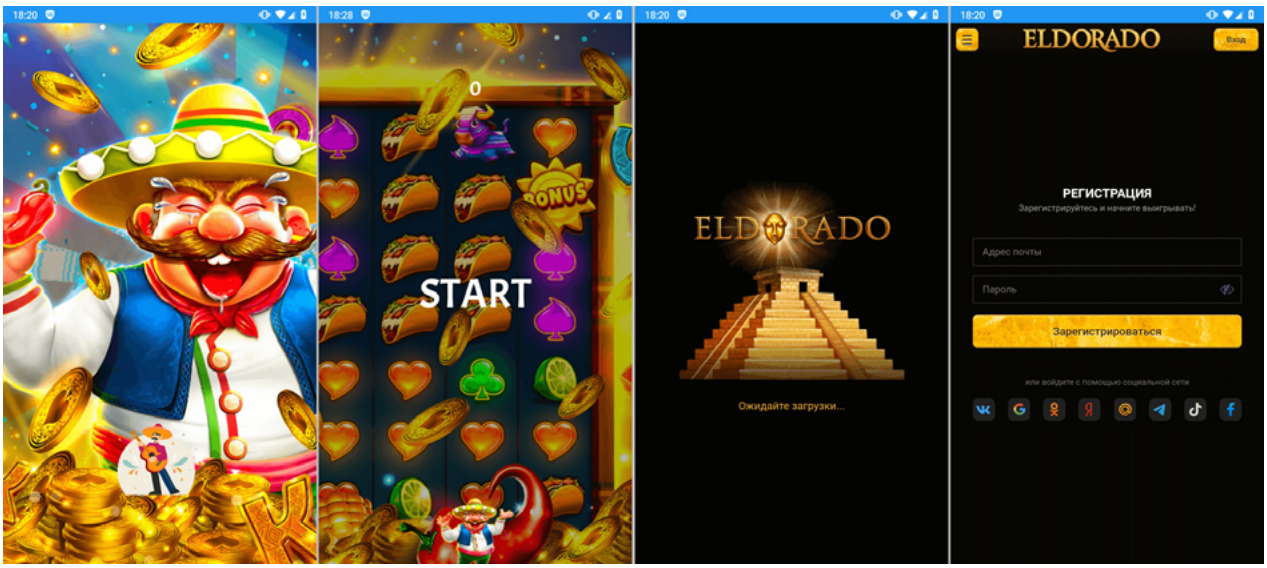


Другие такие программы распространялись под видом игр. Например, Android.FakeApp.1390, Android.FakeApp.1396, Android.FakeApp.1400 и Android.FakeApp.1401. При определенных условиях они могли загружать сайты онлайн-казино.

Угрозы в Google Play



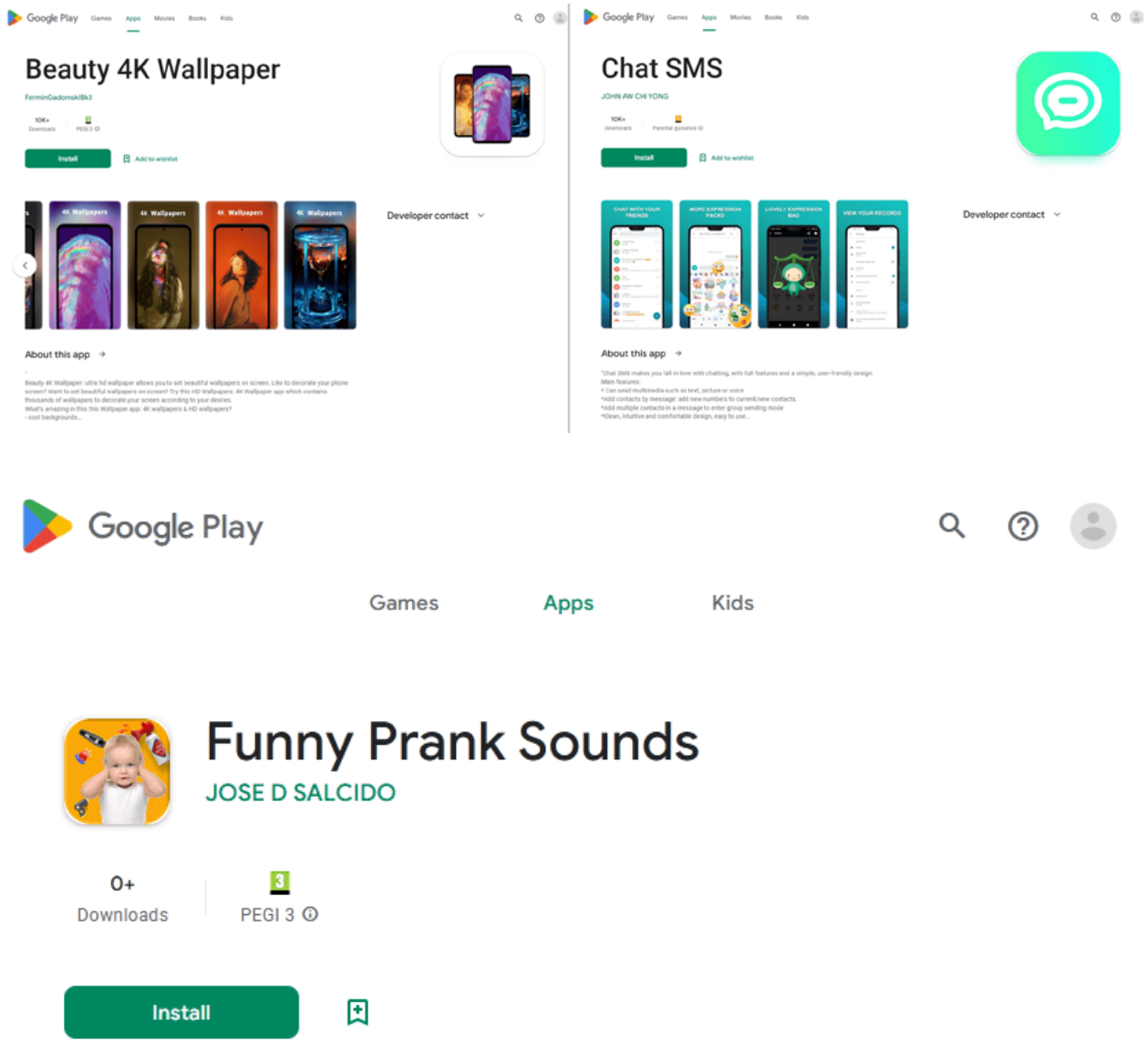
Ниже представлен пример работы одной из таких программ-подделок в качестве игры, а также загруженного ей сайта:



Кроме того, в июне были выявлены очередные троянские программы семейства Android.Joker. которые подписывали жертв на платные услуги. Они скрывались в приложениях Funny Prank Sounds, Beauty 4K Wallpaper и Chat SMS и по классификации антивируса Dr.Web получили имена Android.Joker.2143, Android.Joker.2152 и Android.Joker.2154 соответственно.

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

Угрозы в Google Play



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 июне 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