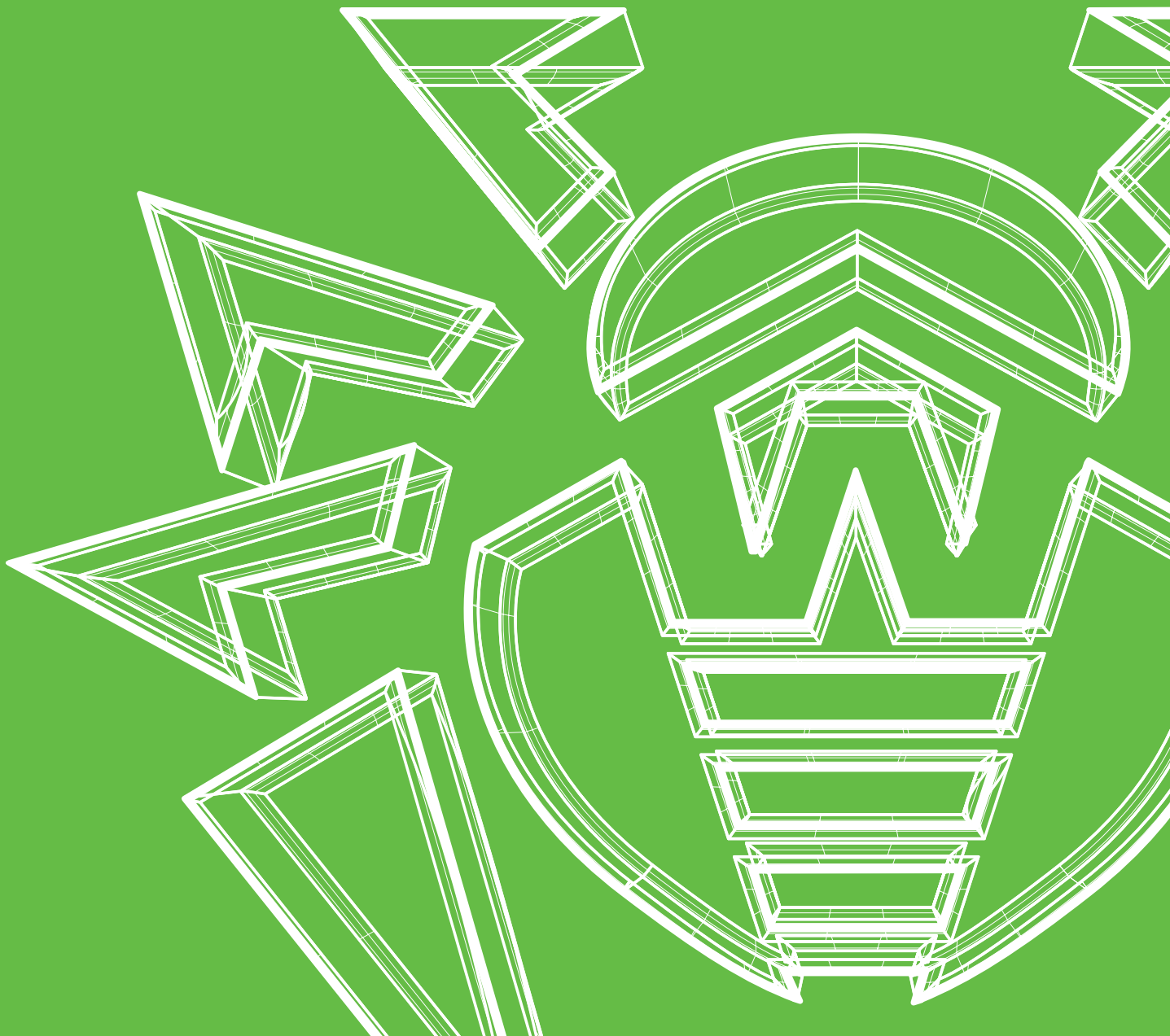
«Доктор Веб»: обзор вирусной активности для мобильных устройств в июне 2022 года



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

26 июля 2022 года

В июне продолжилось снижение активности трояна Android.Spy.4498, похищающего информацию из уведомлений от других приложений. По сравнению с маем он встречался на Android-устройствах на 20,56% реже. Активность рекламных троянов семейства Android.HiddenAds также снизилась, хоть и менее значительно — на 8%. Вместе с тем эти вредоносные приложения остаются одними из наиболее распространенных Android-угроз.

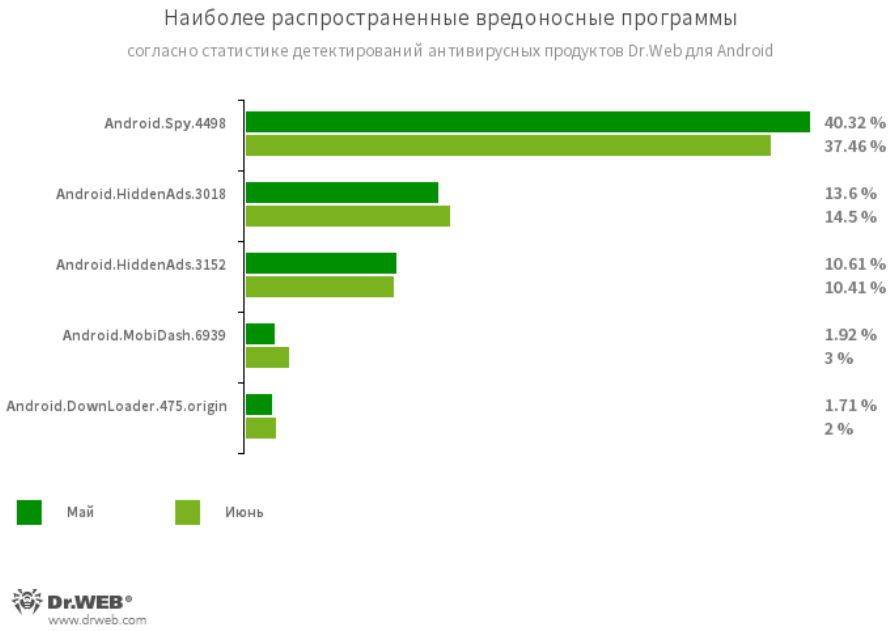
В течение месяца вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play десятки вредоносных программ. Среди них — рекламные трояны, программы-подделки, применяемые мошенниками, похитители конфиденциальной информации и другие.

ГЛАВНЫЕ ТЕНДЕНЦИИ ИЮНЯ

- Снижение активности трояна Android.Spy.4498
- Снижение активности рекламных троянов
- Обнаружение большого числа вредоносных программ в каталоге Google Play

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

По данным антивирусных продуктов Dr.Web для Android



Android.Spy.4498

Троян, крадущий содержимое уведомлений от других приложений. Кроме того, он загружает и предлагает пользователям установить другие программы, а также может демонстрировать различные диалоговые окна.

Android.HiddenAds.3018

Android.HiddenAds.3152

Трояны, предназначенные 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.MobiDash.6939

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

Android.DownLoader.475.origin

Троян, загружающий другие вредоносные программы и ненужное ПО. Он может скрываться во внешне безобидных приложениях, которые распространяются через каталог Google Play или вредоносные сайты.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в июне 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.SecretVideoRecorder.1.origin

Program.SecretVideoRecorder.2.origin

Детектирование различных версий приложения, предназначенного 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

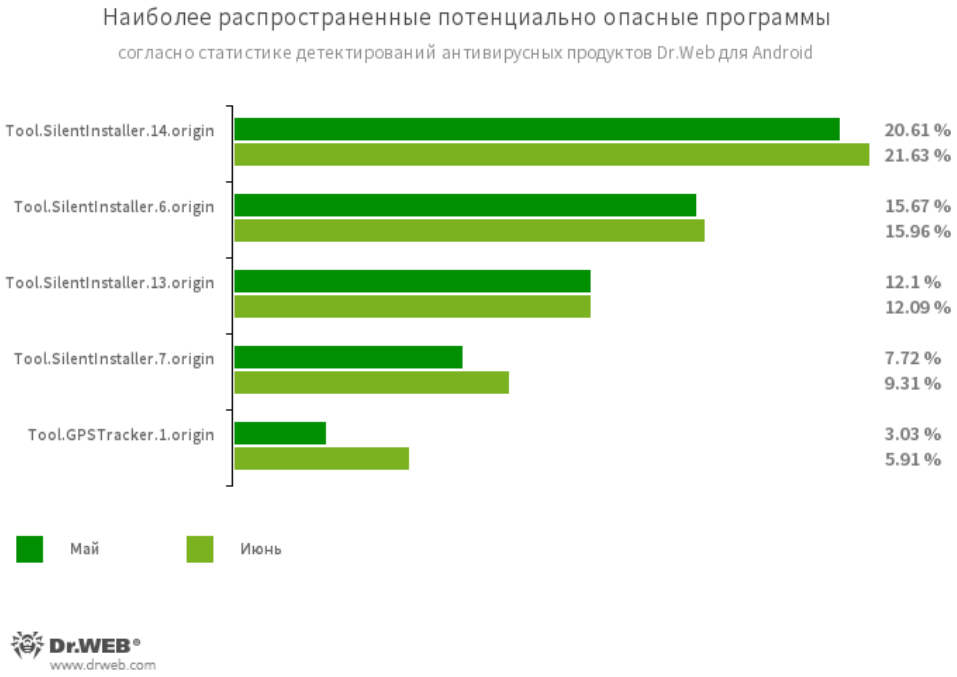
Коммерческая программа-шпион, предназначенная для скрытого наблюдения за владельцами Android-устройств. Она позволяет читать переписку пользователя (сообщения в популярных мессенджерах и СМС), прослушивать окружение, отслеживать местоположение устройства, следить за историей веб-браузера, получать доступ к телефонной книге и контактам, фотографиям и видео, делать скриншоты экрана и фотографии через камеру устройства, а также имеет функцию кейлоггера.

Program.WapSniff.1.origin

Программа для перехвата сообщений в мессенджере WhatsApp.

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

По данным антивирусных продуктов Dr.Web для Android



Tool.SilentInstaller.14.origin

Tool.SilentInstaller.6.origin

Tool.SilentInstaller.13.origin

Tool.SilentInstaller.7.origin

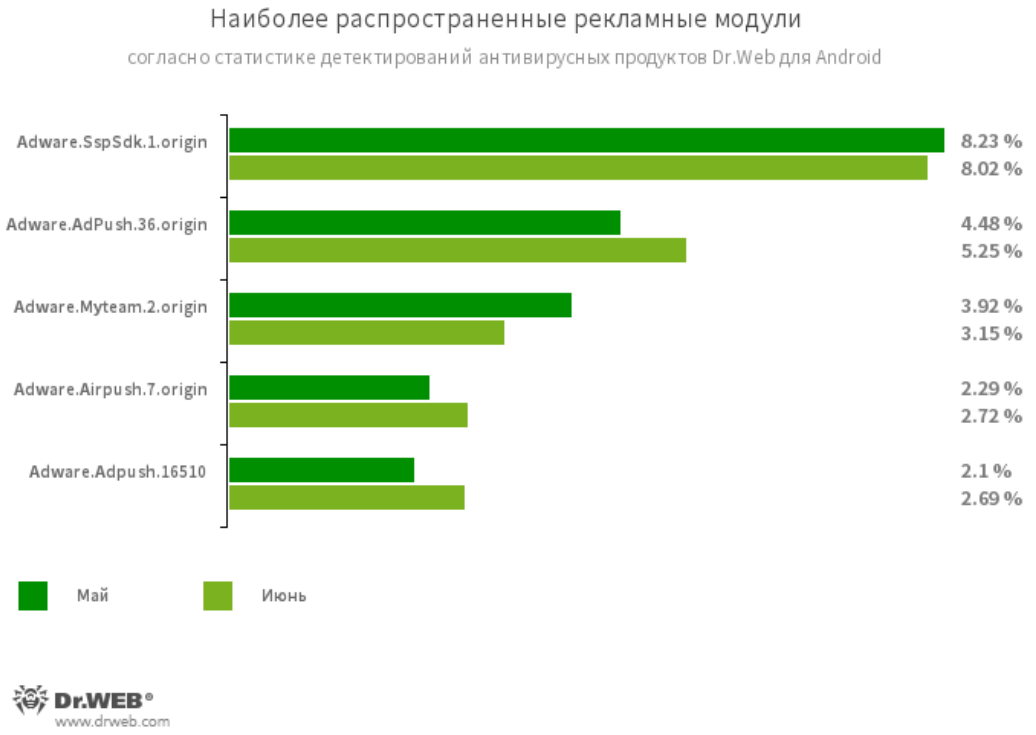
Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

Tool.GPSTracker.1.origin

Специализированная программная платформа, предназначенная для скрытого слежения за местоположением и перемещением пользователей. Она может быть встроена в различные приложения и игры.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в июне 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.SspSdk.1.origin

Adware.AdPush.36.origin

Adware.Adpush.16510

Adware.Myteam.2.origin

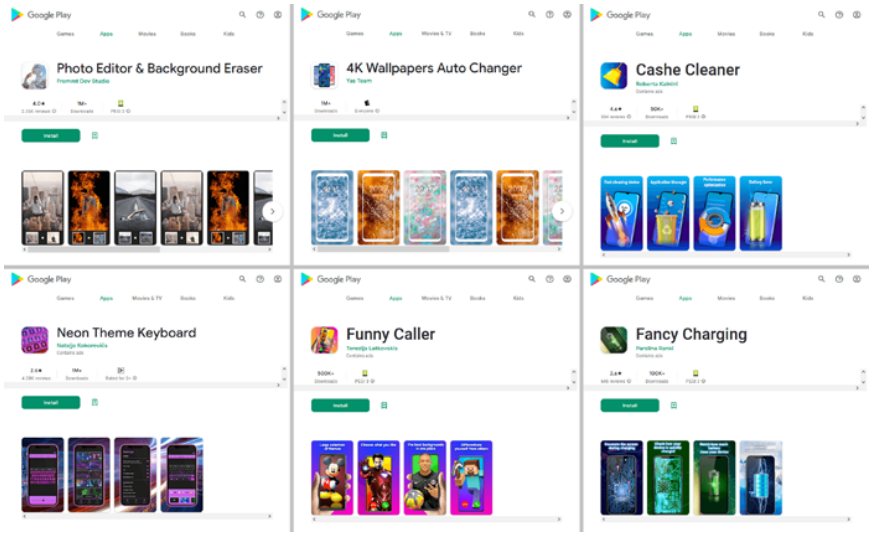
Adware.Airpush.7.origin

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

Угрозы в Google Play

В июне вирусная лаборатория компании «Доктор Веб» выявила в каталоге Google Play около 30 рекламных троянов Android.HiddenAds, общее число загрузок которых превысило 9 890 000. Среди них были как новые представители семейства (Android.HiddenAds.3168, Android.HiddenAds.3169, Android.HiddenAds.3171, Android.HiddenAds.3172 и Android.HiddenAds.3207), так и новые модификации уже известного трояна Android.HiddenAds.3158, о котором мы сообщали в майском обзоре.

Все они были встроены в разнообразные программы — редакторы изображений, экранные клавиатуры, системные утилиты, приложения для звонков, программы для замены фонового изображения домашнего экрана и другие.



Ниже представлен список с названиями программ, в которых скрывались эти трояны:

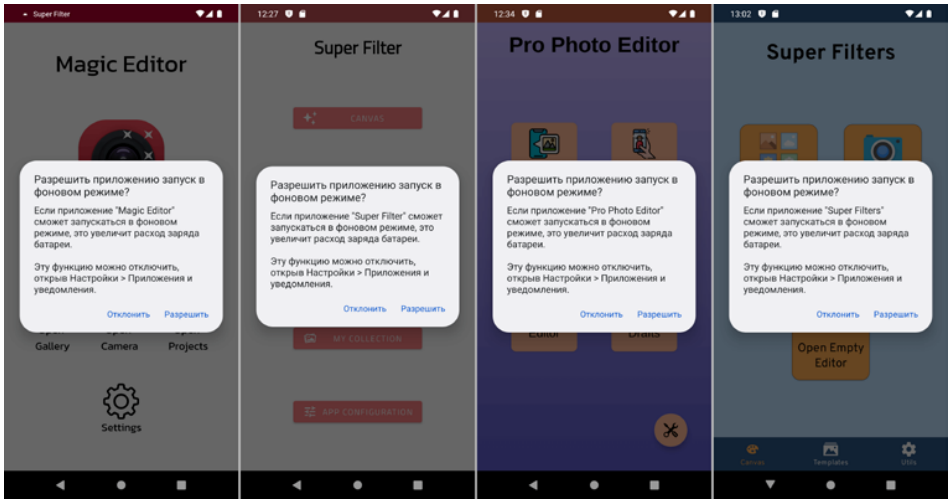
- Photo Editor: Beauty Filter (gb.artfilter.tenvarnist)
- Photo Editor: Retouch & Cutout (de.nineergysh.quickarttwo)
- Photo Editor: Art Filters (gb.painnt.moonlightingnine)
- Photo Editor - Design Maker (gb.twentynine.redaktoridea)
- Photo Editor & Background Eraser (de.photoground.twentysixshot)
- Photo & Exif Editor (de.xnano.photoexifeditornine)
- Photo Editor - Filters Effects (de.hitopgop.sixtyeightgx)
- Photo Filters & Effects (de.sixtyonecollice.cameraroll)
- Photo Editor : Blur Image (de.instgang.fiftyggfife)
- Photo Editor : Cut, Paste (de.fiftyninecamera.rollredactor)
- Emoji Keyboard: Stickers & GIF (gb.crazykey.sevenboard)
- Neon Theme Keyboard (com.neonthemekeyboard.app)

Угрозы в Google Play

- Neon Theme - Android Keyboard (com.androidneonkeyboard.app)
- Cashe Cleaner (com.cachecleanereasytool.app)
- Fancy Charging (com.fancyanimatedbattery.app)
- FastCleaner: Cashe Cleaner (com.fastcleanercashecleaner.app)
- Call Skins - Caller Themes (com.rockskinthemes.app)
- Funny Caller (com.funnycallercustomtheme.app)
- CallMe Phone Themes (com.callercallwallpaper.app)
- InCall: Contact Background (com.mycallcustomcallscrean.app)
- MyCall - Call Personalization (com.mycallcallpersonalization.app)
- Caller Theme (com.caller.theme.slow)
- Caller Theme (com.callertheme.firstref)
- Funny Wallpapers - Live Screen (com.funnywallpapaerslive.app)
- 4K Wallpapers Auto Changer (de.andromo.ssfiftylivesixcc)
- NewScrean: 4D Wallpapers (com.newscrean4dwallpapers.app)
- Stock Wallpapers & Backgrounds (de.stockeighty.onewallpapers)
- Notes - reminders and lists (com.notesreminderslists.app)

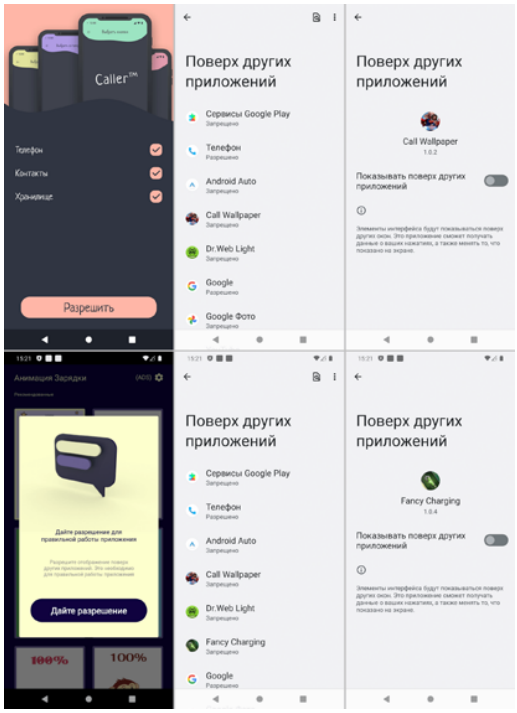
Для показа рекламы часть из них пытается получить разрешение на демонстрацию окон поверх других программ, остальные — попасть в список исключений функции экономии заряда аккумулятора. А чтобы в дальнейшем пользователям было сложнее обнаружить «нарушителей», трояны скрывают свои значки в списке установленных приложений главного экрана или заменяют их менее приметными. Например, значком с названием «SIM Toolkit», при выборе которого вместо исходного приложения запускается одноименное системное ПО для работы с SIM-картой.

Примеры того, как эти трояны пытаются получить доступ к необходимым функциям:

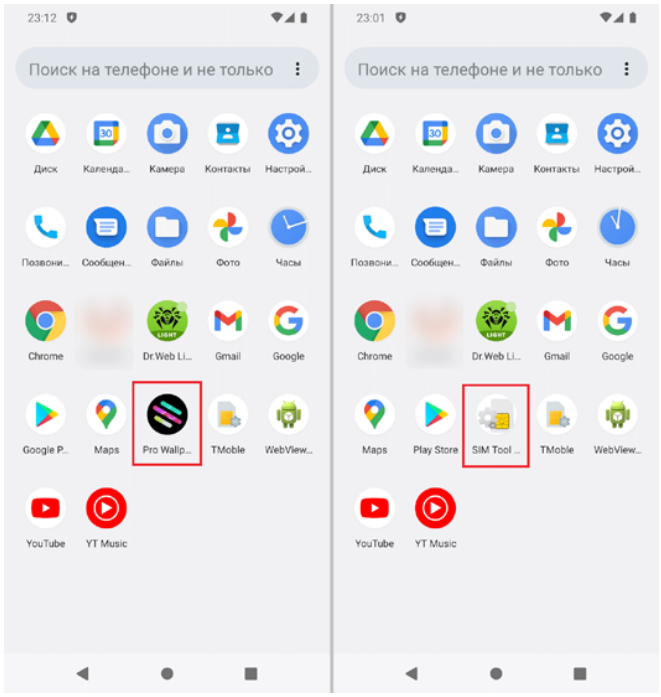


«Доктор Веб»: обзор вирусной активности для мобильных устройств в июне 2022 года

Угрозы в Google Play



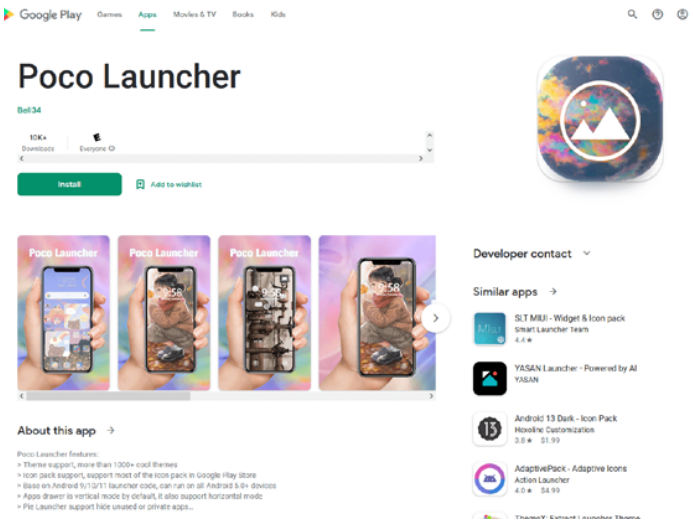
Пример изменения значка одного из вредоносных приложений:

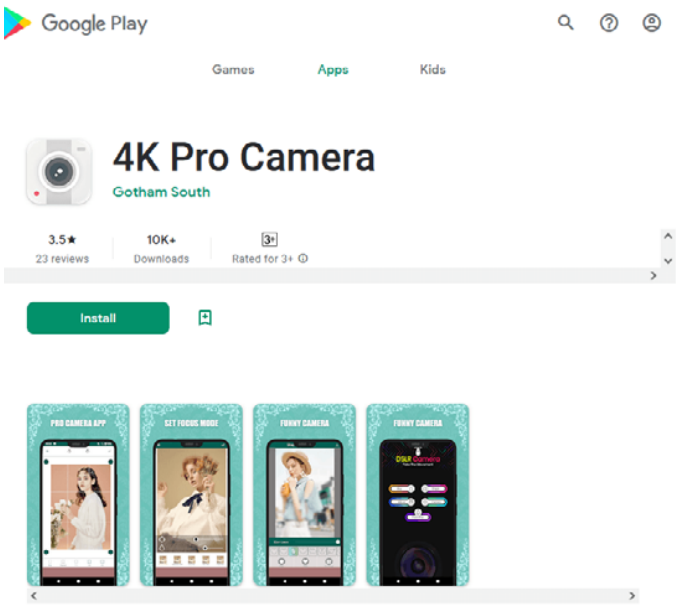


«Доктор Веб»: обзор вирусной активности для мобильных устройств в июне 2022 года

Угрозы в Google Play

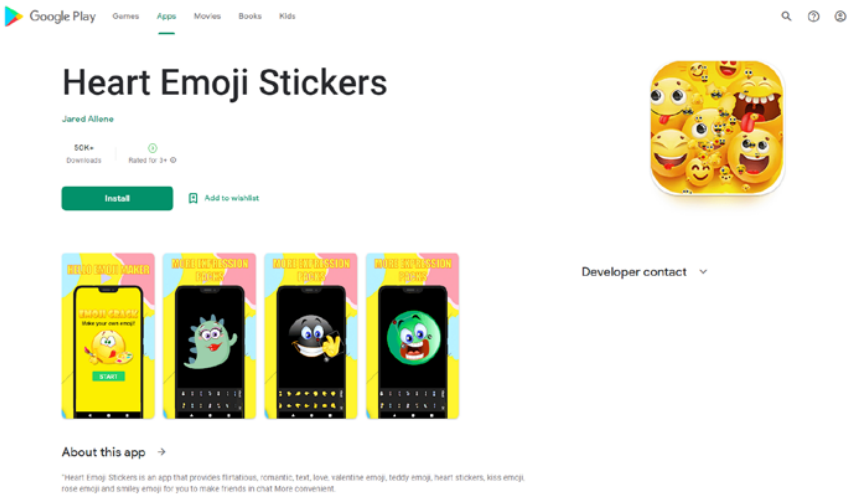
Кроме того, наши специалисты обнаружили очередных троянов семейства Android.Joker, которые способны загружать и выполнять произвольный код, а также подписывать пользователей на платные мобильные услуги без их ведома. Один из них скрывался в лончере Poco Launcher, другой — в приложении-камере 4K Pro Camera; третий — в сборнике стикеров Heart Emoji Stickers. Они были добавлены в вирусную базу Dr.Web как Android.Joker.1435, Android.Joker.1461 и Android.Joker.1466 соответственно.





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

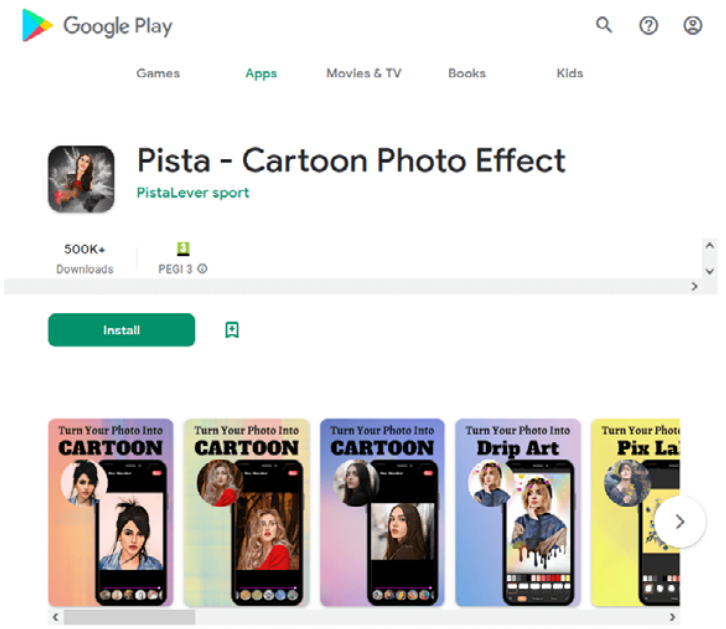
Угрозы в Google Play



Среди выявленных угроз также были новые вредоносные приложения семейства Android.PWS.Facebook, получившие имена Android.PWS.Facebook.149 и Android.PWS.Facebook.151. Они похищали данные, необходимые для взлома учетных записей Facebook (деятельность социальной сети Facebook запрещена на территории России). Оба трояна распространялись под видом редакторов изображений. Первый — программы под названием YouToon - AI Cartoon Effect, второй — Pista - Cartoon Photo Effect.

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

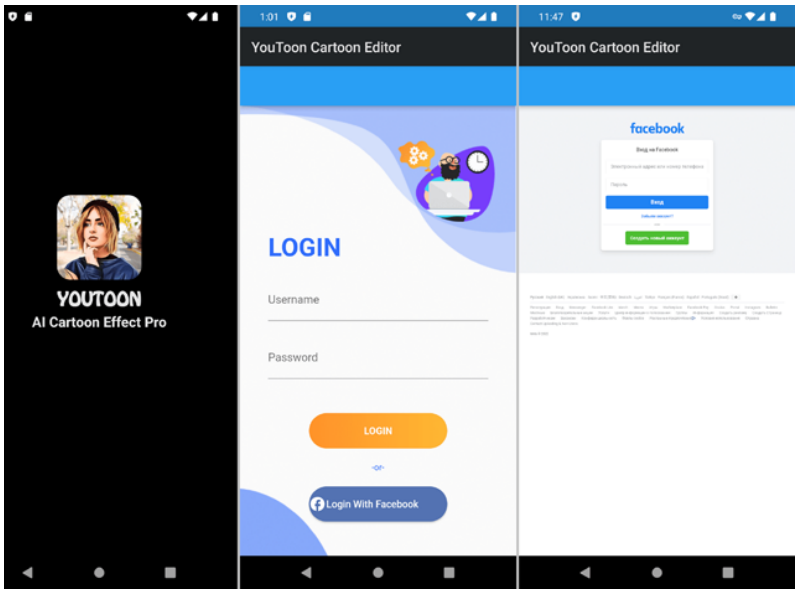
Угрозы в Google Play

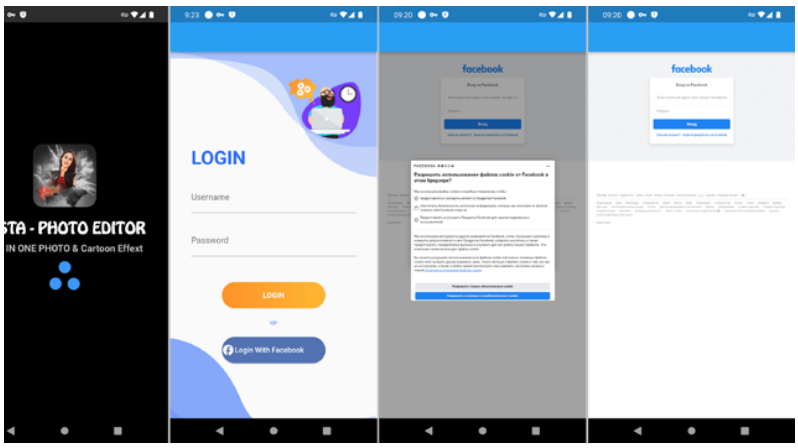


После запуска они предлагали потенциальным жертвам войти в свою учетную запись, после чего загружали стандартную страницу авторизации Facebook. Затем они перехватывали данные аутентификации и передавали их злоумышленникам.

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

Угрозы в Google Play

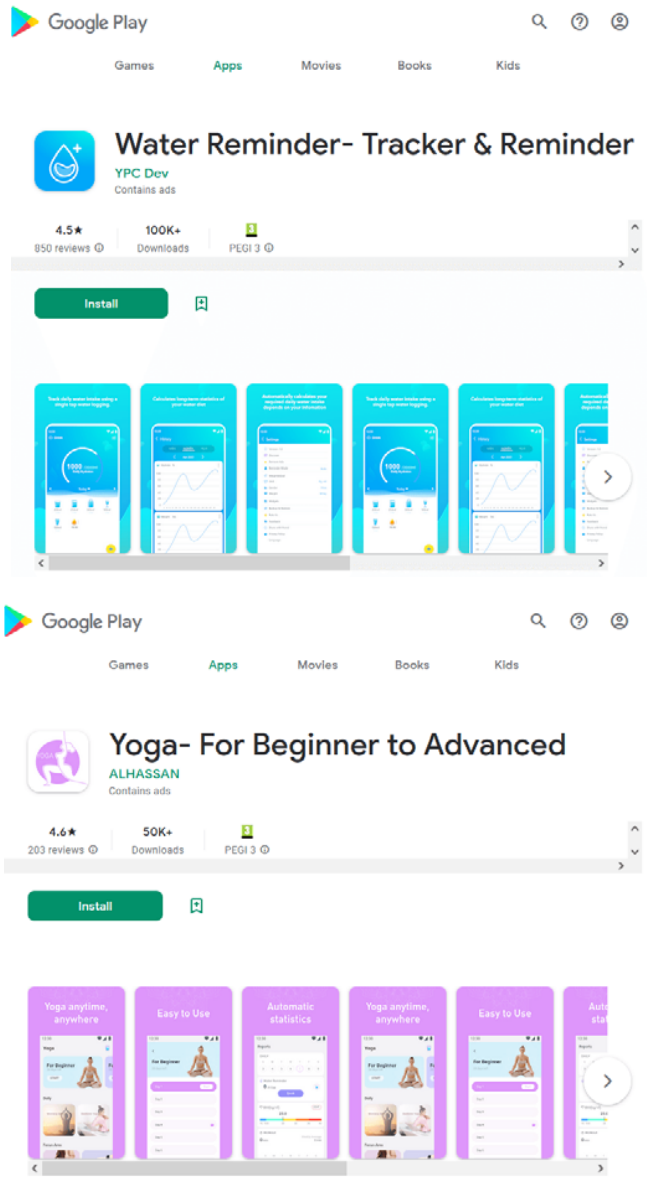




Также специалисты «Доктор Веб» обнаружили трояна Android.Click.401.origin. Он скрывался в программе Water Reminder- Tracker & Reminder, напоминающей о необходимости пить достаточно жидкости, и в обучающей программе по йоге Yoga- For Beginner to Advanced. Обе были полностью работоспособными, поэтому у пользователей не было причин заподозрить в них угрозу.

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

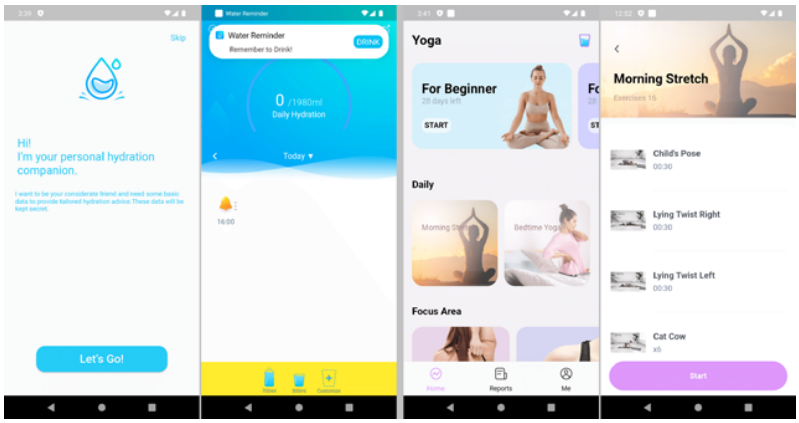
Угрозы в Google Play



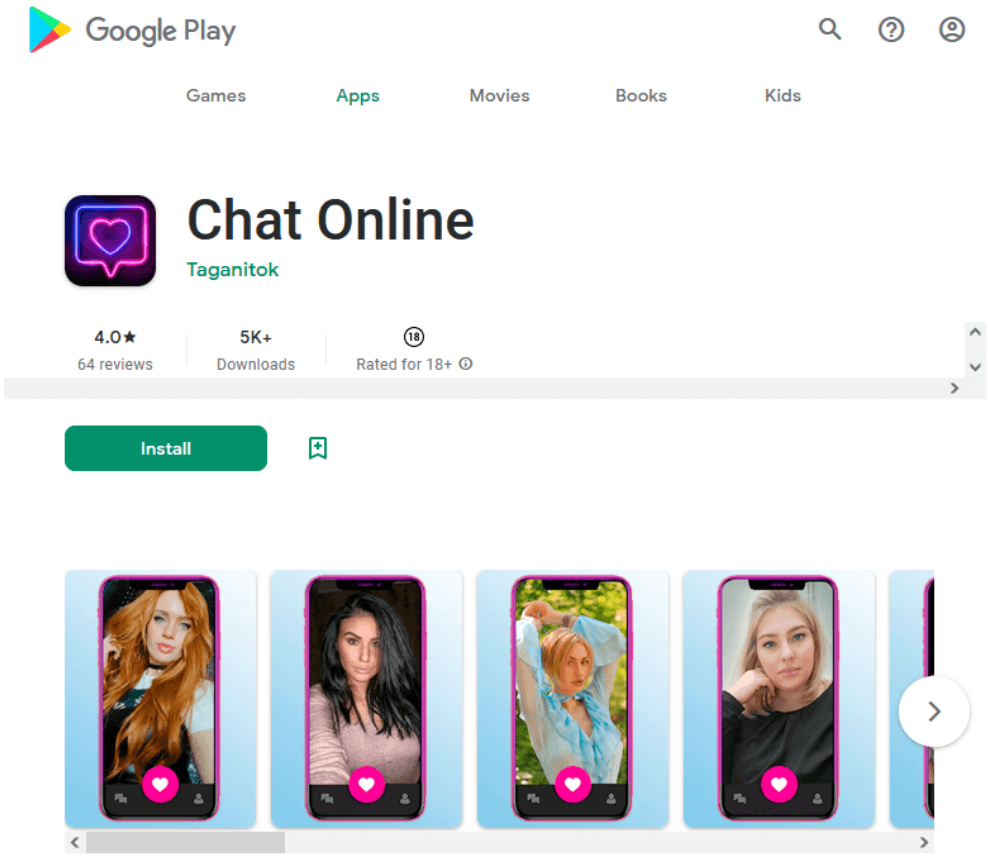
Этот троян расшифровывает и запускает находящийся среди его ресурсов основной вредоносный компонент (Android.Click.402.origin по классификации антивируса Dr.Web), который скрытно загружает различные веб-сайты в WebView. Затем данный компонент имитирует действия пользователей, автоматически нажимая на расположенные на сайтах интерактивные элементы, например — баннеры и рекламные ссылки.

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

Угрозы в Google Play



Другой выявленной угрозой стало поддельное приложение для онлайн-общения Chat Online, несколько модификаций которого были добавлены в вирусную базу Dr.Web как Android.FakeApp.963 и Android.FakeApp.964.

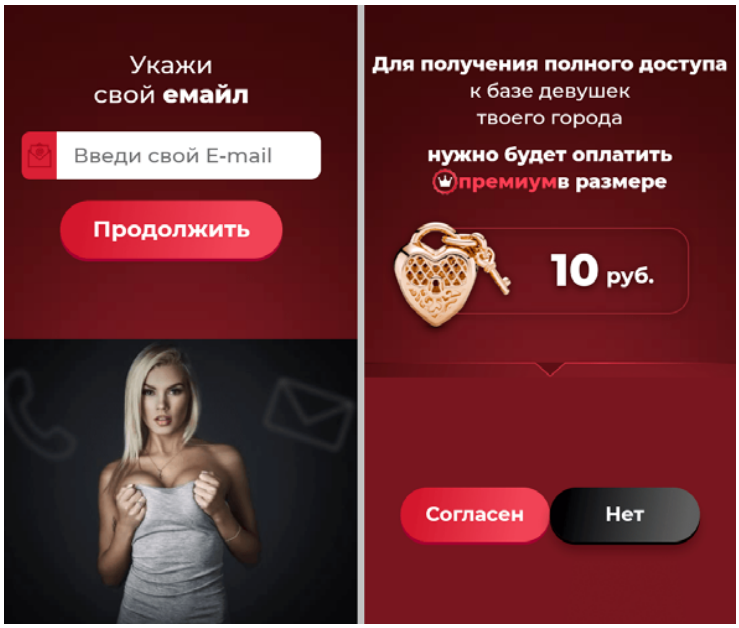


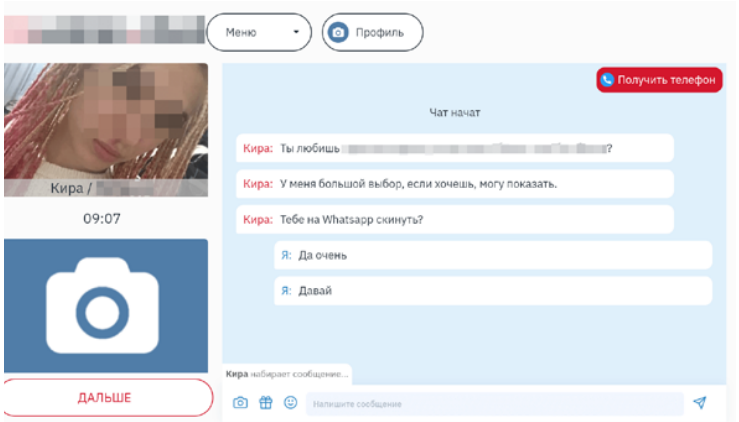
«Доктор Веб»: обзор вирусной активности для мобильных устройств в июне 2022 года

Угрозы в Google Play

В трояне нет заявленной функциональности. Он лишь загружает различные веб-сайты, в том числе мошеннические. На одних имитируется процесс регистрации в онлайн-сервисах знакомств. При этом у потенциальных жертв запрашивается номер мобильного телефона, адрес электронной почты и другие персональные данные. В дальнейшем эта информация может попадать на черный рынок и использоваться мошенниками.

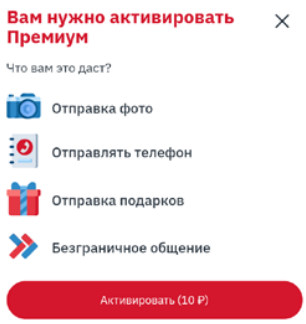
На других сайтах имитируется диалог с настоящими пользователями, после чего предлагается оплатить премиум-доступ для продолжения «общения». Согласие на это может привести не только к единовременному списанию определенной суммы или подписке на ненужную платную услугу, но и к потере всех средств, если киберпреступники получат данные банковской карты.





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

Угрозы в Google Play



Компания «Доктор Веб» передала информацию о выявленных угрозах корпорации Google. На момент выхода данного обзора часть вредоносных приложений все еще была доступна для загрузки.

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 июне 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