Dr.WEB

«Доктор Веб»:

обзор вирусной активности для мобильных устройств в августе 2023 года

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

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в августе 2023 года среди наиболее распространенных вредоносных программ вновь оказались рекламные троянские приложения семейств Android.MobiDash и Android.HiddenAds. При этом по сравнению с предыдущим месяцем первые обнаруживались на 72,23% чаще, в то время как активность вторых снизилась на 8,87%.

Количество шпионских троянских программ и программ-вымогателей, выявленных на защищаемых устройствах, снизилось на 13,88% и 18,14% соответственно. Вместе с тем пользователи на 2,13% чаще, чем в июле, сталкивались с банковскими троянскими приложениями.

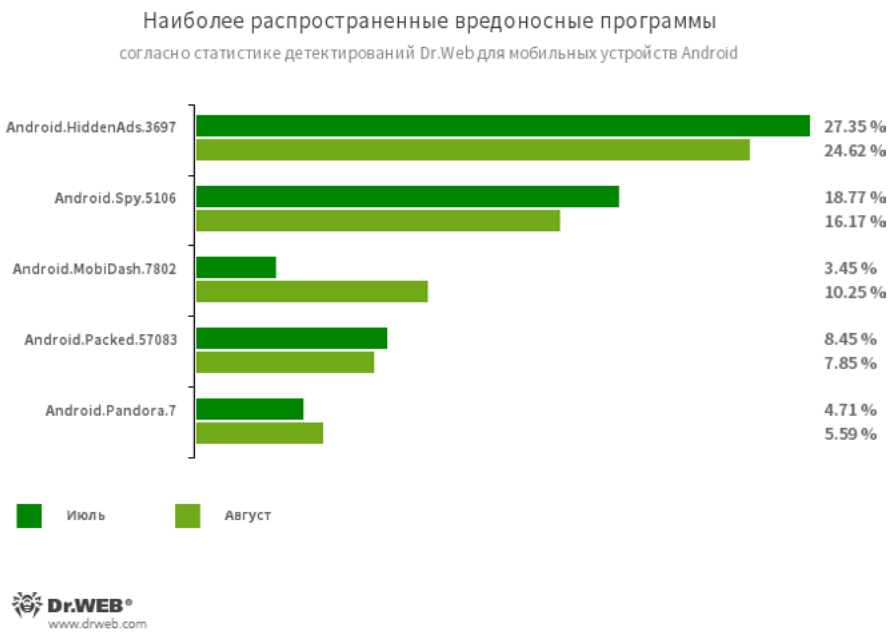
В августе в каталоге Google Play была обнаружена очередная вредоносная программа.

Главные тенденции августа

- Значительный рост активности рекламных троянских программ Android.MobiDash
- Снижение активности рекламных троянских программ Android.HiddenAds
- Снижение активности троянов-шпионов и программ-вымогателей
- Рост числа атак банковских троянских приложений

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

По данным антивирусных продуктов Dr.Web для Android



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.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.MobiDash.7802

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

Android.Packed.57083

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

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 августе 2023 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.7

Program.FakeMoney.8

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.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.

По данным антивирусных продуктов Dr.Web для Android

Program.wSpy.1.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.

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

По данным антивирусных продуктов Dr.Web для Android

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.

Tool.SilentInstaller.14.origin

Tool.SilentInstaller.7.origin

Tool.SilentInstaller.6.origin

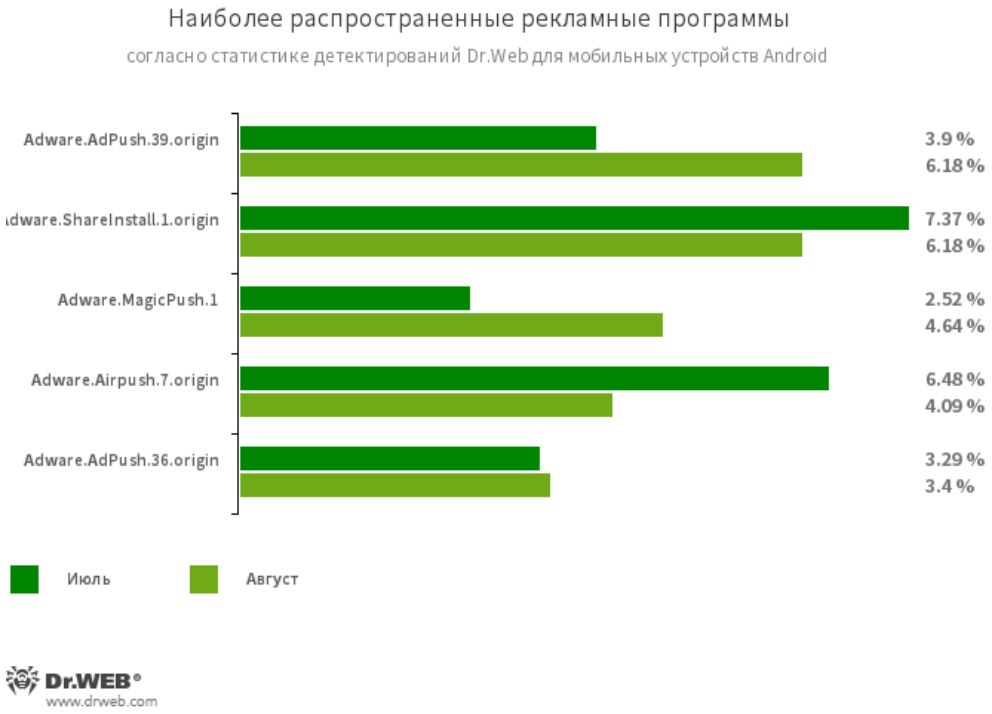
Потенциально опасные программные платформы, которые позволяют приложениям запускать APK-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

Tool.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 августе 2023 года

По данным антивирусных продуктов Dr.Web для Android



Adware.AdPush.39.origin

Adware.AdPush.36.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.ShareInstall.1.origin

Рекламный модуль, который может быть интегрирован в Android-программы. Он демонстрирует рекламные уведомления на экране блокировки ОС Android.

Adware.MagicPush.1

Рекламный модуль, встраиваемый в Android-приложения. Он демонстрирует 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.

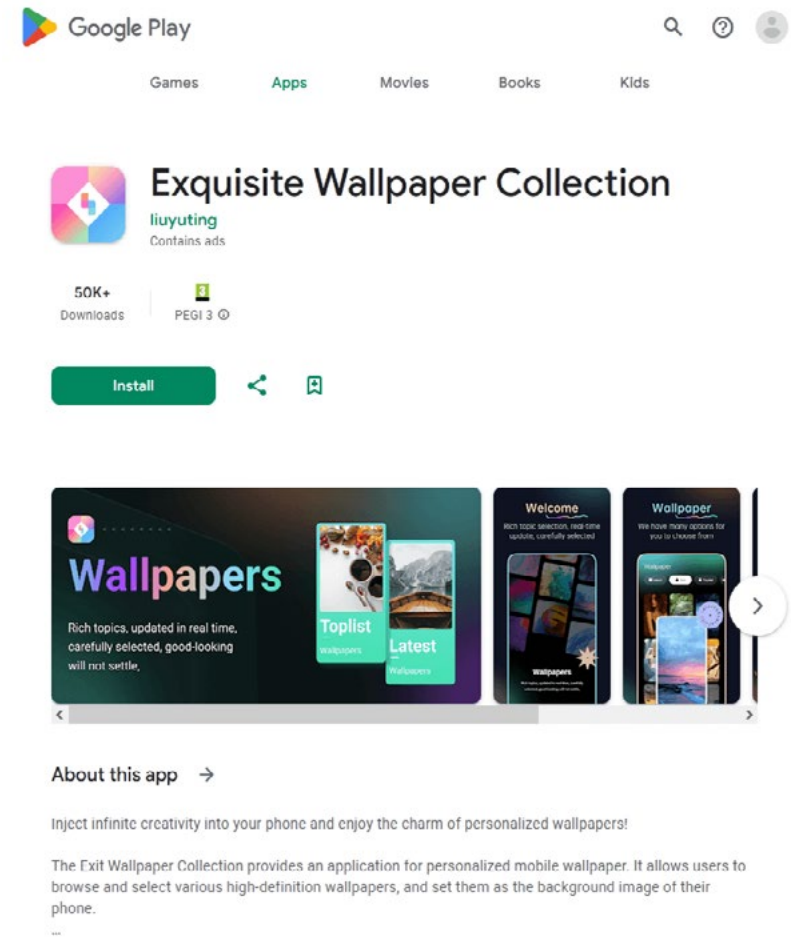
Adware.Airpush.7.origin

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 августе 2023 года

Угрозы в Google Play

В августе 2023 года в каталоге Google Play была обнаружена троянская программа Android.HiddenAds.3766. Она распространялась под видом приложения — сборника изображений Exquisite Wallpaper Collection. Однако ее основная функция — демонстрация нежелательной рекламы. При этом Android.HiddenAds.3766 пытается скрыться от пользователя. Троян заменяет свой значок на домашнем экране прозрачной версией, а также меняет его название на пустое. В ряде случаев вместо этого вредоносная программа может заменить его копией значка браузера Google Chrome, при нажатии на который запустится не вредоносное приложение, а непосредственно браузер.



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 августе 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