Dr.WEB

«Доктор Веб»:

обзор вирусной активности для мобильных устройств в феврале 2024 года

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

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в феврале 2024 года значительно возросла активность рекламных троянских программ из семейства Android.HiddenAds — на 73,26% по сравнению с январем. В то же время пользователи на 58,85% реже сталкивались с другим семейством рекламных троянов, Android.MobiDash.

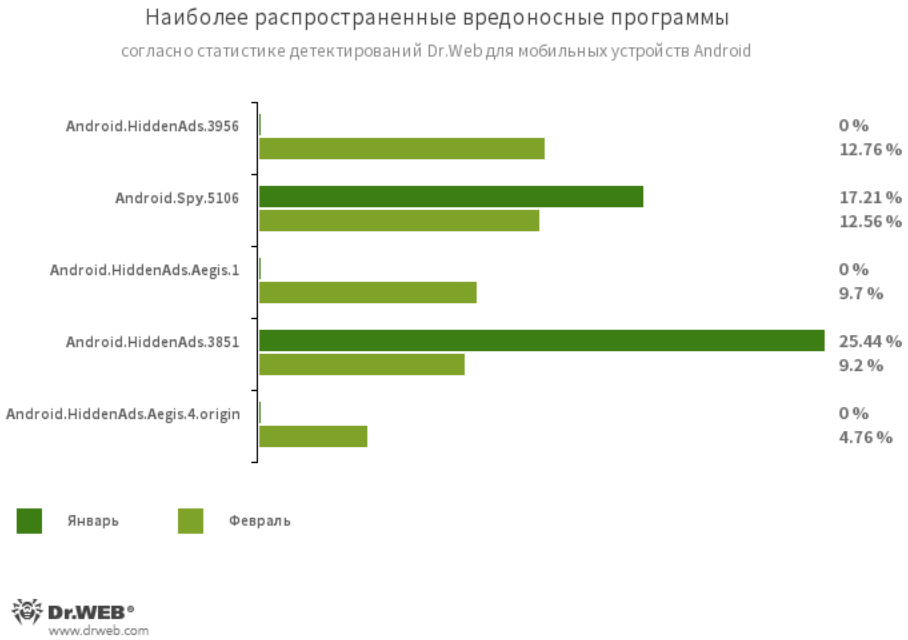
Активность банковских троянов различных семейств снизилась на 18,77%, а шпионских троянских приложений Android.Spy — на 27,33%. При этом число детектирований вредоносных программ-вымогателей Android.Locker увеличилось на 29,85%.

Главные тенденции февраля

- Значительный рост активности рекламных троянских программ семейства Android.HiddenAds
- Снижение числа атак банковских троянов и шпионских вредоносных приложений
- Увеличение числа детектирований вредоносных программ-вымогателей на защищаемых устройствах

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

По данным антивирусных продуктов Dr.Web для Android



Android.HiddenAds.3956
Android.HiddenAds.3851

Троянские программы 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

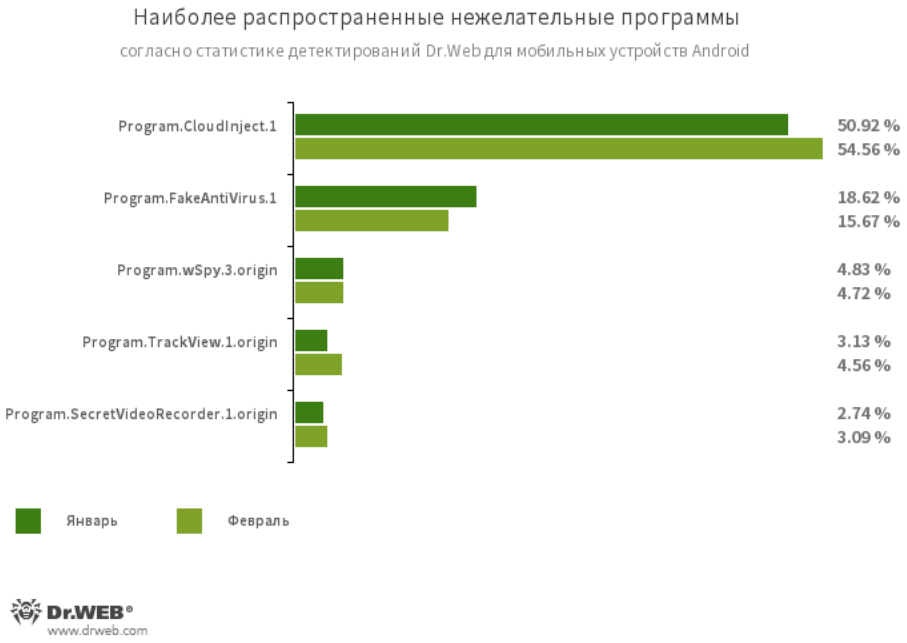
Детектирование троянской программы, представляющей собой видоизмененные версии неофициальных модификаций приложения WhatsApp. Она может похищать содержимое уведомлений, предлагать установку программ из неизвестных источников, а во время использования мессенджера — демонстрировать диалоговые окна с дистанционно настраиваемым содержимым.

Android.HiddenAds.Aegis.1
Android.HiddenAds.Aegis.4.origin

Троянские программы, которые скрывают свое присутствие на Android-устройствах и показывают надоедливую рекламу. Они отличаются от других представителей семейства Android.HiddenAds рядом признаков. Например, эти трояны способны самостоятельно запускаться после установки. Кроме того, в них реализован механизм, позволяющий их сервисам оставаться постоянно запущенными. В ряде случаев в них также могут быть задействованы скрытые функции ОС Android.

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

По данным антивирусных продуктов Dr.Web для Android



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 дистанционного 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.wSpy.3.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.

По данным антивирусных продуктов Dr.Web для Android

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.

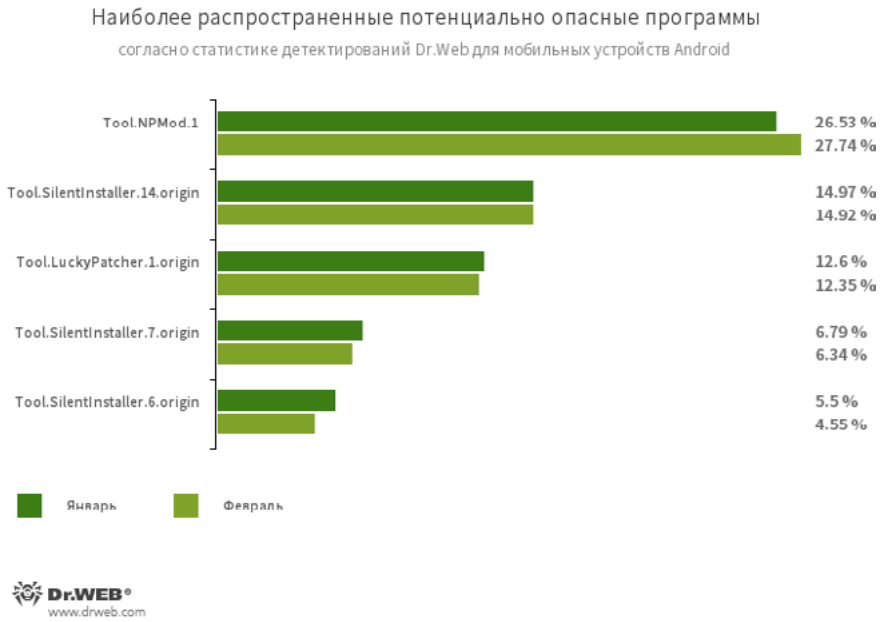
Program.SecretVideoRecorder.1.origin

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.

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

По данным антивирусных продуктов Dr.Web для Android

.



Tool.NPMod.1

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.14.origin

Tool.SilentInstaller.7.origin

Tool.SilentInstaller.6.origin

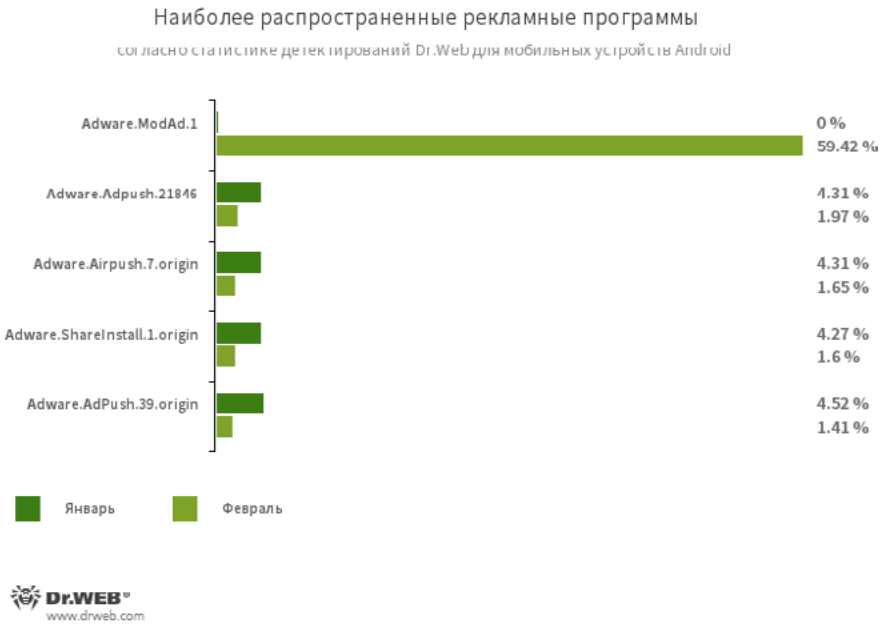
Потенциально опасные программные платформы, которые позволяют приложениям запускать APK-файлы без их установки. Эти платформы создают виртуальную среду исполнения в контексте приложений, в которые они встроены. Запускаемые с их помощью APK-файлы могут работать так, как будто являются частью таких программ, 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.

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

По данным антивирусных продуктов Dr.Web для Android



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.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.
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.
Adware.ShareInstall.1.origin
Рекламный модуль, который может быть интегрирован в Android-программы. Он демонстрирует рекламные уведомления на экране блокировки ОС.
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 феврале 2024 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
«Доктор Веб» в других странах