Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2020 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2020 года

10 апреля 2020 года

В марте число выявленных на Android-устройствах угроз выросло на 21,24% по сравнению с февралем. Количество обнаруженных вредоносных программ увеличилось на 21,6%, нежелательных – на 13,37%, потенциально опасных – на 32,65%, рекламных – на 27,64%.

В течение месяца вирусные аналитики «Доктор Веб» выявили новые вредоносные приложения в каталоге Google Play. Среди них был троян семейства Android.Joker, показывающий рекламу и способный подписывать пользователей на платные мобильные услуги, а также опасный многофункциональный троян Android.Circle.1, выполняющий команды злоумышленников.

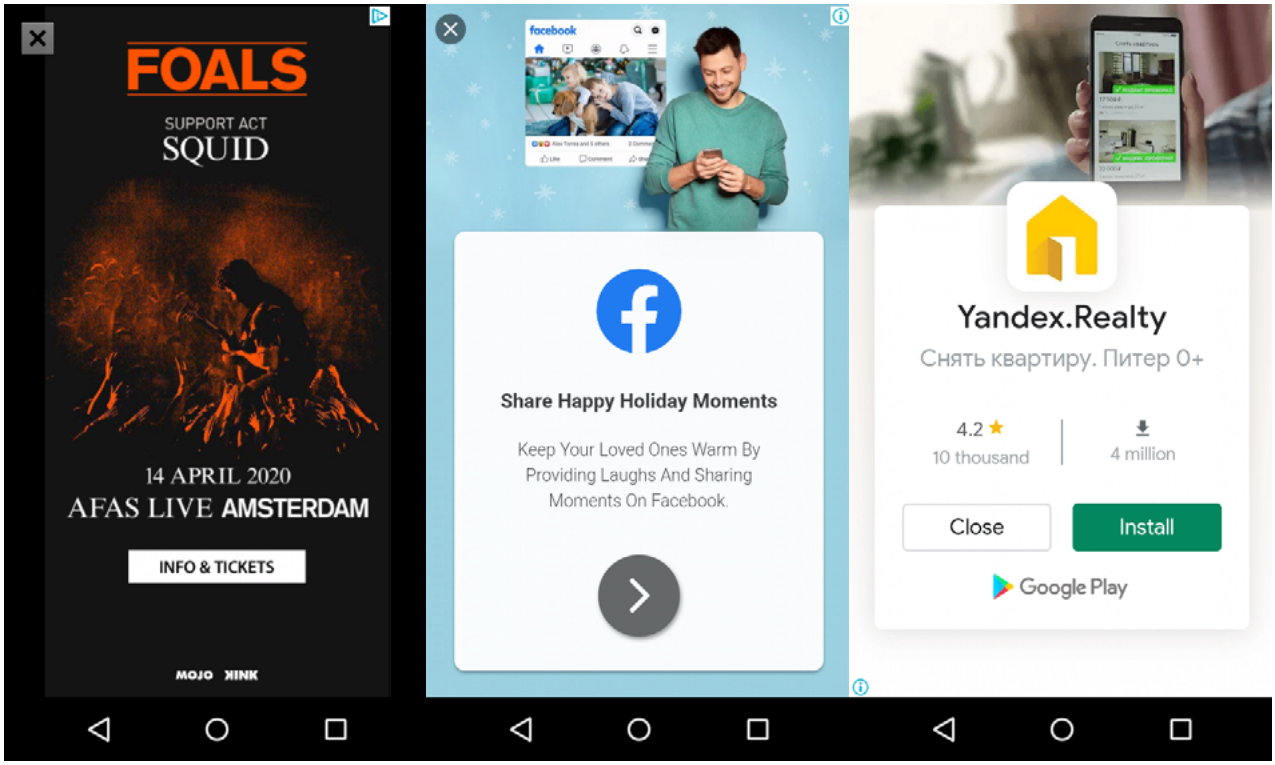
ГЛАВНЫЕ ТЕНДЕНЦИИ МАРТА

- Рост числа угроз, выявленных на Android-устройствах
- Обнаружение новых вредоносных программ в Google Play

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2020 года

Угроза месяца

В марте компания «Доктор Веб» сообщила об обнаружении в каталоге Google Play нового опасного трояна Android.Circle.1, которого установили свыше 700 000 пользователей. По команде злоумышленников он показывал рекламу и загружал различные веб-сайты, на которых имитировал действия пользователей, нажимая на баннеры и ссылки. Пример демонстрируемой им рекламы:



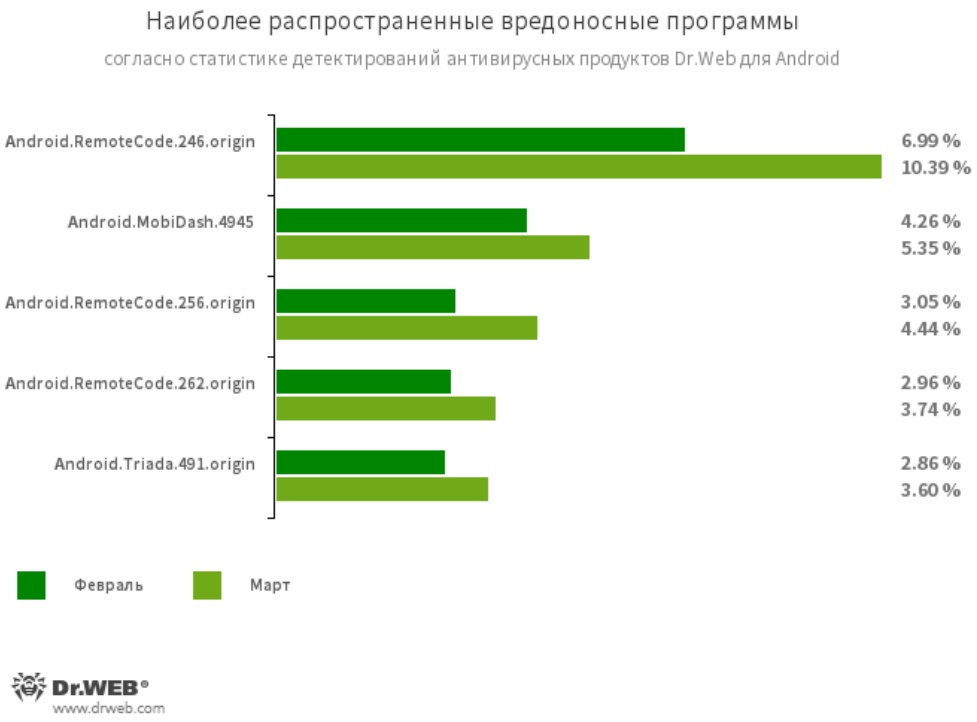
В течение месяца наши специалисты выявили несколько модификаций этого вредоносного приложения.

Особенности Android.Circle.1:

- встроен в безобидные программы;
- создан с использованием механизма Multiple APKs, который позволяет загружать в Google Play множество копий одного приложения для поддержки различных моделей устройств и процессорных архитектур;
- принимает от управляющего сервера и выполняет BeanShell-скрипты;
- часть функций трояна вынесена в отдельную нативную библиотеку;
- чтобы скрыться от пользователя, некоторые модификации Android.Circle.1 после установки выдают себя за важный системный компонент.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2020 года

По данным антивирусных продуктов Dr.Web для Android

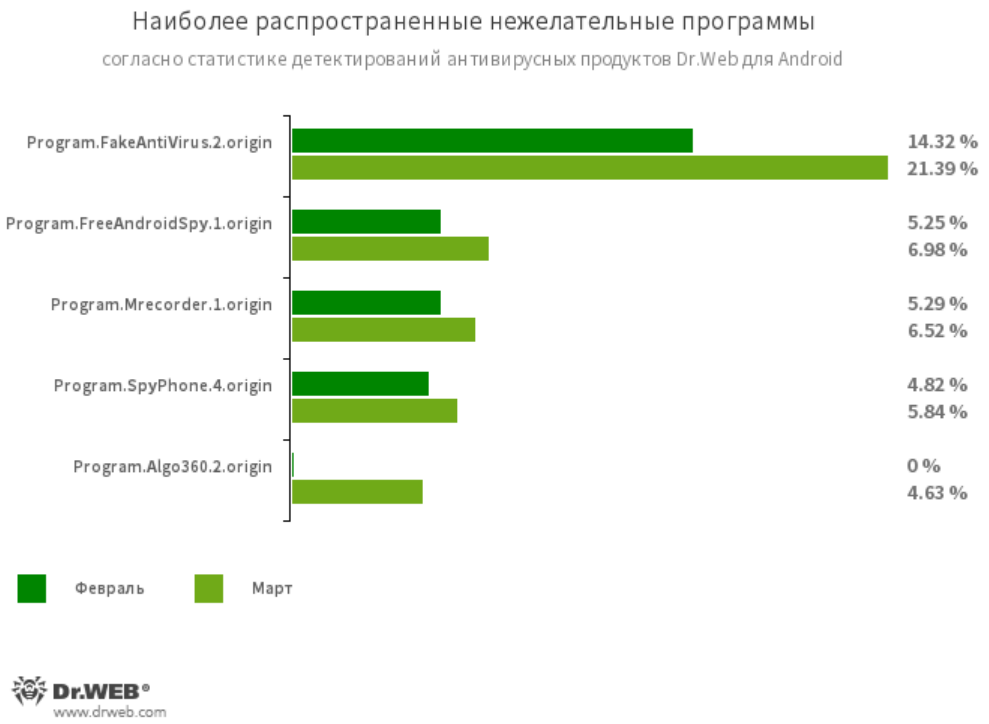


..

Android.RemoteCode.246.origin
Android.RemoteCode.256.origin
Android.RemoteCode.262.origin
Вредоносные программы, которые загружают и выполняют произвольный код.
Android.MobiDash.4945
Троянская программа, показывающая рекламу.
Android.Triada.491.origin
Многофункциональный троян, выполняющий разнообразные вредоносные действия.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2020 года

По данным антивирусных продуктов Dr.Web для Android

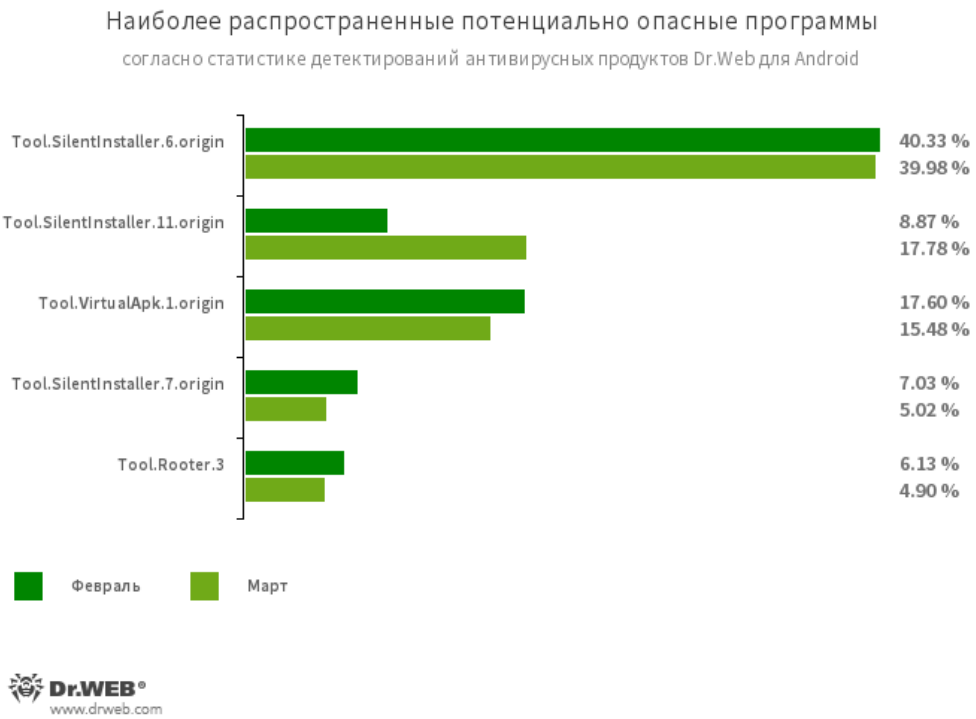


Program.FakeAntiVirus.2.origin
Детектирование рекламных программ, которые имитируют работу антивирусного ПО.
Program.FreeAndroidSpy.1.origin
Program.Mrecorder.1.origin
Program.MobileTool.2.origin
Приложения, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа.
Program.Algo360.2.origin
Детектирование программного модуля, который используется в приложениях различных финансовых организаций, выдающих денежные займы. Он представляет собой агрегатор данных пользователей, для которых формируется кредитный профиль. Модуль собирает информацию об СМС-сообщениях, закладках браузера, местоположении устройства, записях календаря и другие персональные данные.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2020 года

По данным антивирусных продуктов Dr.Web для Android

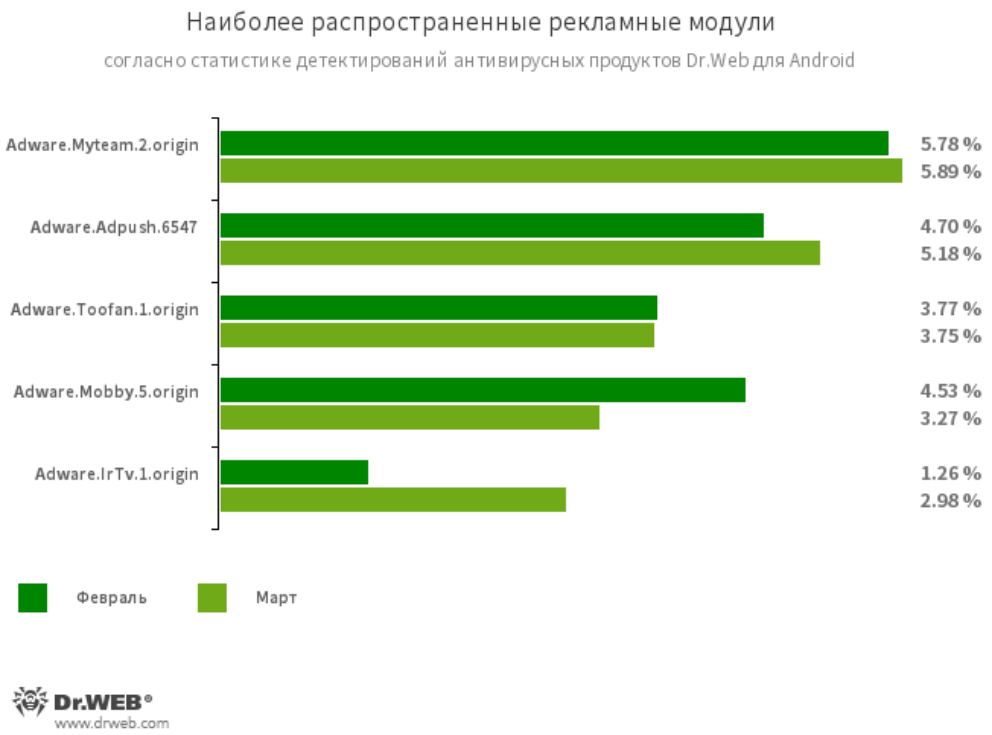
.



Tool.SilentInstaller.6.origin
Tool.SilentInstaller.7.origin
Tool.SilentInstaller.11.origin
Tool.VirtualApk.1.origin
Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки.
Tool.Rooter.3
Утилита для получения root-полномочий на Android-устройствах. Может использоваться злоумышленниками и вредоносными программами.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2020 года

По данным антивирусных продуктов Dr.Web для Android



Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах:

- Adware.Myteam.2.origin
- Adware.Adpush.6547
- Adware.Toofan.1.origin
- Adware.Mobby.5.origin
- Adware.IrTv.1.origin

Угрозы в Google Play

Наряду с троянами семейства Android.Circle в марте в Google Play был найден очередной представитель семейства Android.Joker, получивший имя Android.Joker.102.origin. Он распространялся под видом редакторов изображений и сборников обоев. Вредоносная программа могла загружать и запускать троянские модули и произвольный код, а также подписывать пользователей на дорогостоящие сервисы.

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 марте 2020 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
ВебIQметр | Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.drweb.ru | www.антивирус.рф | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах