Dr.WEB®
с 1992 года

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

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

22 октября 2020 года

Согласно статистике детектирований антивирусных продуктов Dr.Web для Android, в сентябре на защищаемых устройствах было зафиксировано на 3.75% больше угроз, чем в августе. По сравнению с прошлым месяцем количество обнаруженных вредоносных программ увеличилось на 5.58%, а потенциально опасных — на 4.98%. При этом число рекламных и нежелательных приложений сократилось на 6.22% и 8.83% соответственно.

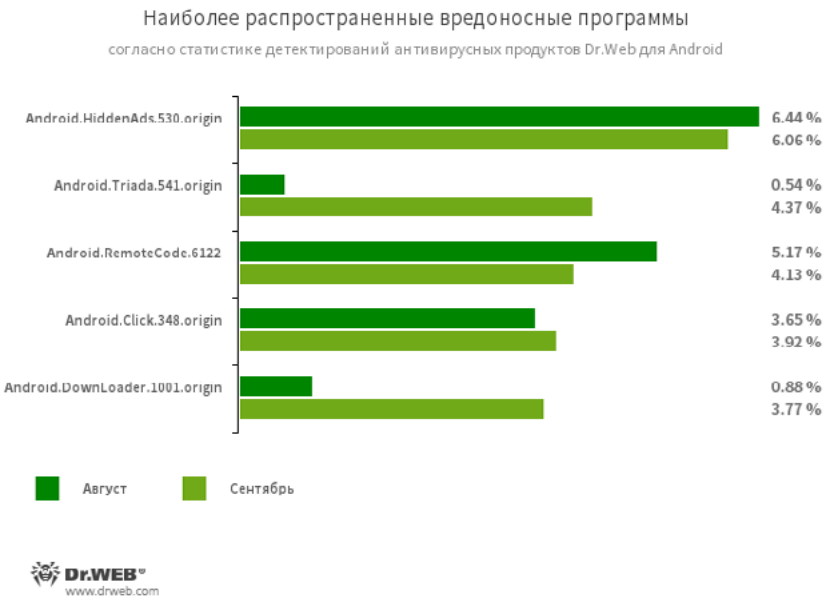
В течение сентября вирусные аналитики «Доктор Веб» выявили в каталоге Google Play несколько новых вредоносных приложений. Среди них оказались представители опасного семейства троянов Android.Joker, способных выполнять произвольный код и подписывать жертв на платные сервисы. Кроме того, злоумышленники распространяли трояна-кликера Android.Click.978, показывавшего рекламу, а также многофункционального трояна Android.Triada.545.origin, который использовался в том числе для фишинга.

ГЛАВНЫЕ ТЕНДЕНЦИИ СЕНТЯБРЯ

- Увеличение общего числа угроз, зафиксированных на Android-устройствах
- Распространение угроз в каталоге Google Play

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

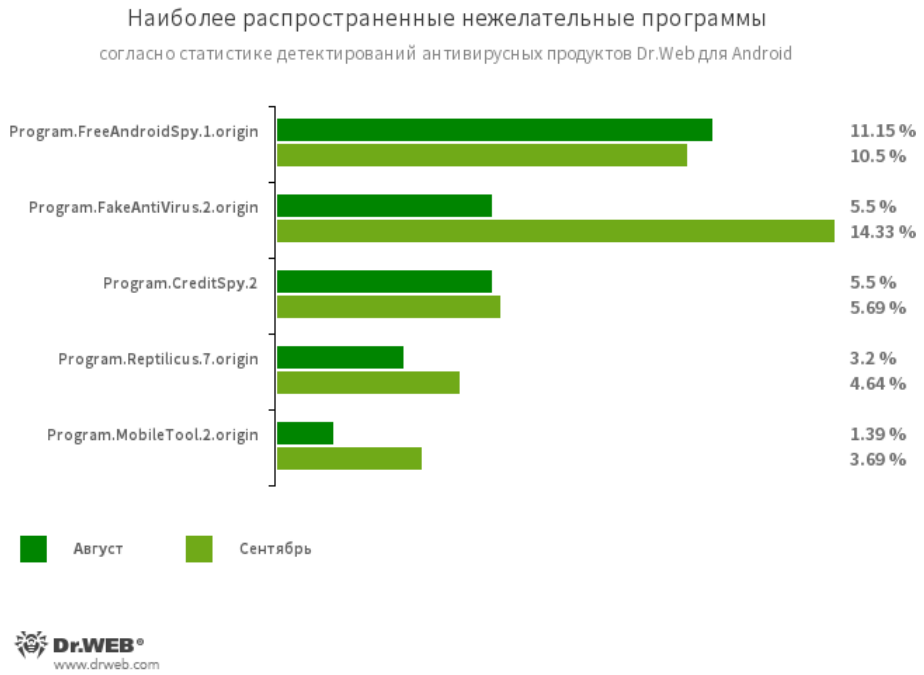
По данным антивирусных продуктов Dr.Web для Android



Android.HiddenAds.530.origin
Троян, предназначенный для показа навязчивой рекламы. Распространяется под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают его в системный каталог.
Android.Triada.541.origin
Многофункциональный троян, выполняющий разнообразные вредоносные действия. Относится к семейству троянских приложений, проникающих в процессы всех работающих программ. Некоторые модификации этого семейства встречаются в прошивках Android-устройств, куда злоумышленники внедряют их на этапе производства.
Android.RemoteCode.6122
Вредоносная программа, которая загружает и выполняет произвольный код. В зависимости от модификации она также может загружать различные веб-сайты, переходить по ссылкам, нажимать на рекламные баннеры, подписывать пользователей на платные услуги и выполнять другие действия.
Android.Click.348.origin
Вредоносное приложение, которое самостоятельно загружает веб-сайты, нажимает на рекламные баннеры и переходит по ссылкам. Может распространяться под видом безобидных программ, не вызывая подозрений у пользователей.
Android.DownLoader.1001.origin
Троян, загружающий другие вредоносные программы и ненужное ПО. Может скрываться во внешне безобидных приложениях, которые распространяются через каталог Google Play или вредоносные сайты.

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

По данным антивирусных продуктов Dr.Web для Android



Program.FreeAndroidSpy.1.origin

Program.Reptilicus.7.origin

Program.MobileTool.2.origin

Приложения, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа. Они способны контролировать местоположение устройств, собирать данные об СМС-переписке, беседах в социальных сетях, копировать документы, фотографии и видео, выполнять прослушивание телефонных звонков и окружения и т. п.

Program.FakeAntiVirus.2.origin

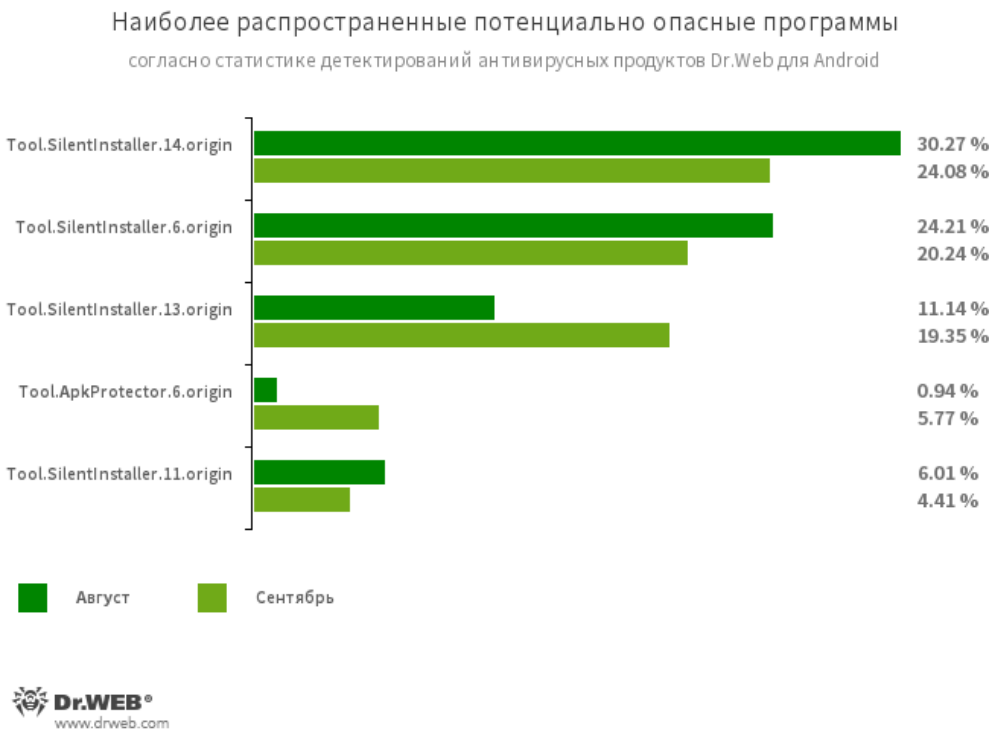
Детектирование рекламных программ, которые имитируют работу антивирусного ПО. Такие программы могут сообщать о несуществующих угрозах и вводить пользователей в заблуждение, требуя оплатить покупку полной версии.

Program.CreditSpy.2

Детектирование программ, предназначенных для присвоения кредитного рейтинга на основании персональных данных пользователей. Такие приложения загружают на удаленный сервер СМС-сообщения, информацию о контактах из телефонной книги, историю вызовов, а также другие сведения.

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

По данным антивирусных продуктов Dr.Web для Android



Tool.SilentInstaller.6.origin
Tool.SilentInstaller.11.origin
Tool.SilentInstaller.13.origin
Tool.SilentInstaller.14.origin

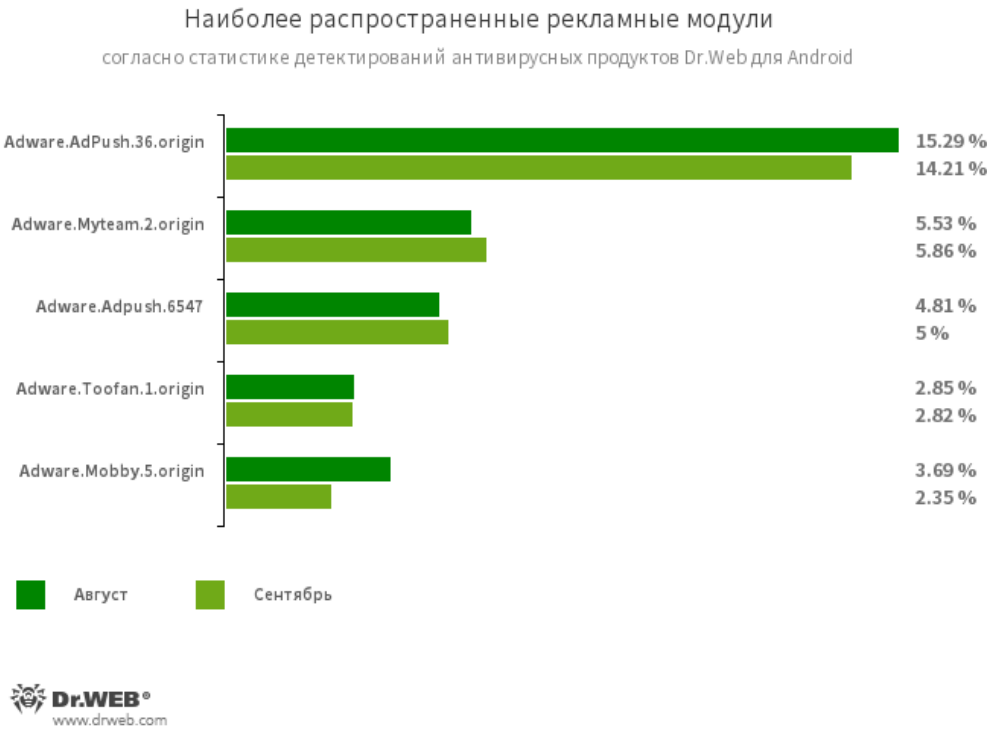
Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

Tool.ApkProtector.6.origin

Детектирование Android-приложенний, 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 сентябре 2020 года

По данным антивирусных продуктов Dr.Web для Android



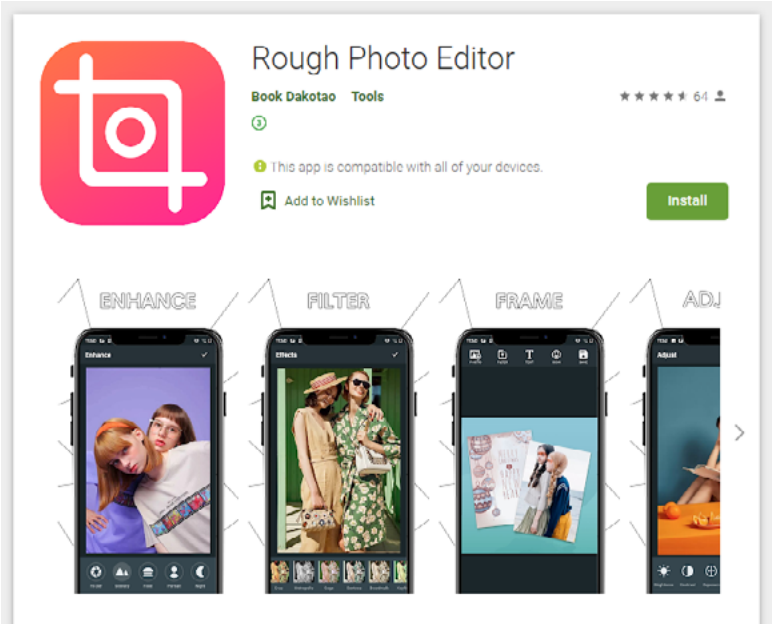
Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать ярлыки и загружать веб-сайты.

- Adware.Adpush.36.origin
- Adware.Adpush.6547
- Adware.Myteam.2.origin
- Adware.Toofan.1.origin
- Adware.Mobby.5.origin

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

Угрозы в Google Play

В сентябре в каталоге Google Play было обнаружено несколько новых модификаций троянов семейства Android.Joker, один из которых распространялся под видом графического редактора и получил имя Android.Joker.341. Как и другие представители семейства, эта вредоносная программа загружала и исполняла произвольный код, а также могла подписывать пользователей на платные услуги, получая коды подтверждений из поступающих уведомлений.

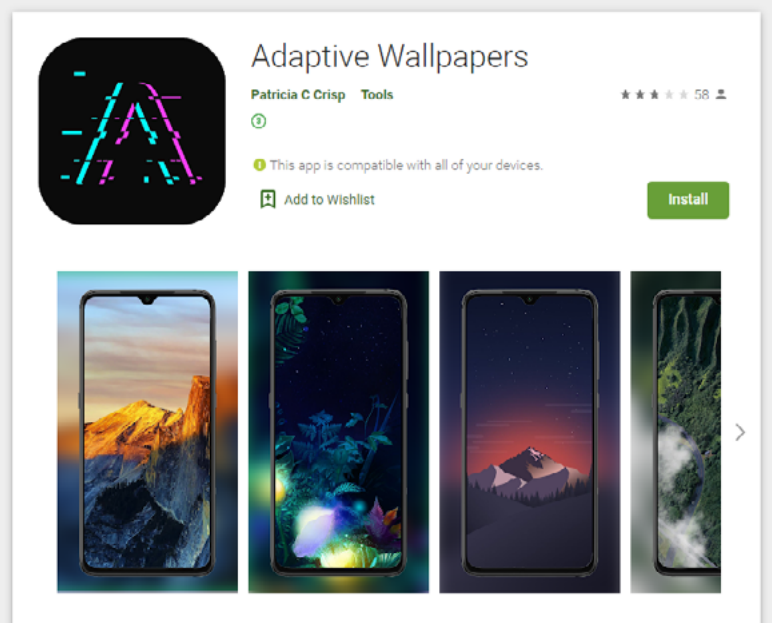


В зависимости от архитектуры процессора, используемой на зараженном устройстве, при старте троян загружает в память одну из скрытых в его apk-файле нативных библиотек (антивирус Dr.Web детектирует их как Android.Joker.339 и Android.Joker.340).

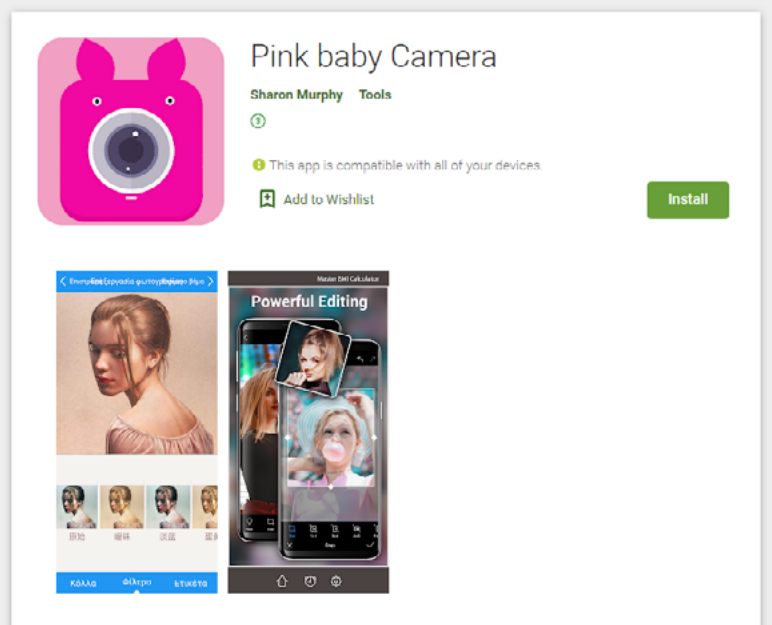
В свою очередь, загруженная библиотека извлекает из себя вредоносный модуль Android.Joker.177.origin, который скачивает с удаленного сервера модуль Android.Joker.192.origin. Тот получает доступ к содержимому уведомлений и загружает с сервера еще один модуль — Android.Joker.107.origin. В нем содержится основная вредоносная функциональность.

Позднее вирусные аналитики «Доктор Веб» обнаружили аналогичного трояна, которого злоумышленники распространяли под видом сборника изображений. Он был добавлен в вирусную базу Dr.Web как Android.Joker.344.

Угрозы в Google Play

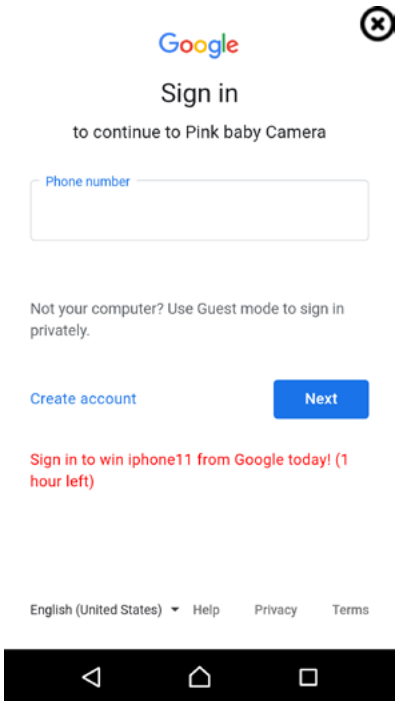


Другой угрозой оказался многофункциональный троян Android.Triada.545.origin, принадлежащий семейству опасных вредоносных программ Android.Triada. Он скрывался в приложении-фотокамере.



Угрозы в Google Play

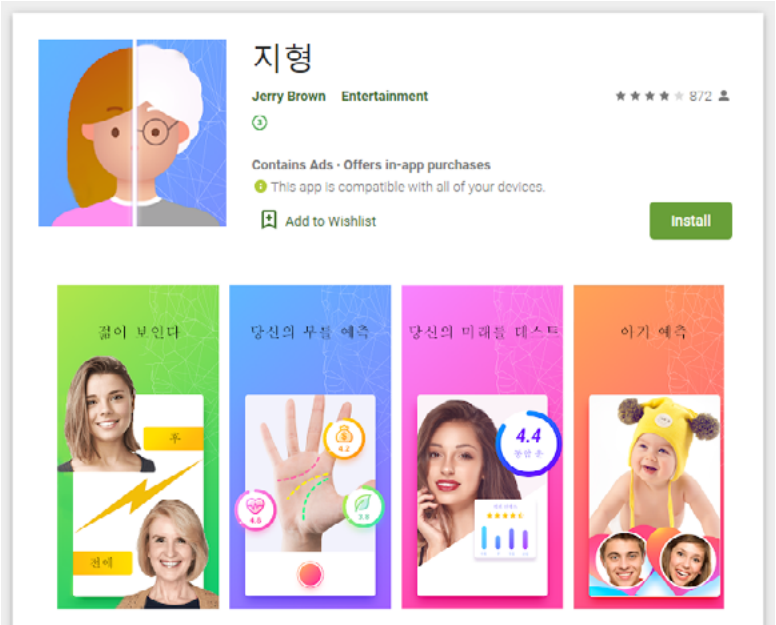
Одной из функций Android.Triada.545.origin является фишинг. При запуске троян демонстрирует поддельное окно авторизации в сервисах Google. В нем жертвам предлагается ввести информацию для доступа к их учетной записи — якобы чтобы продолжить использовать приложение. Чтобы еще больше сбить пользователей с толку, в окне также говорится о возможности принять участие в розыгрыше нового телефона после входа в учетную запись. Однако все это — лишь уловка, и вводимые данные передаются злоумышленникам.



Кроме того, Android.Triada.545.origin может загружать и выполнять произвольный код, а также перехватывать уведомления и похищать из них информацию — например, пин-коды.

Еще одной Android-угрозой, обнаруженной в Google Play в сентябре, стал троян-кликер Android.Click.978, распространявшийся под видом приложения с предсказаниями. После запуска он скрывал свой значок из списка приложений в меню главного экрана устройства и начинал показывать рекламу, которая демонстрировалась даже после закрытия Android.Click.978. Троян также загружал веб-сайты и автоматически нажимал на расположенные на них ссылки и баннеры.

Угрозы в Google Play



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 сентябре 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.антивирус.рф | www.drweb.ru | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах