Dr.WEB®
с 1992 года

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

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

10 августа 2020 года

По сравнению с предыдущим месяцем, в июле на Android-устройствах было обнаружено на 6,7% меньше угроз. Число вредоносных программ сократилось на 6,75%, нежелательных — на 4,6%, потенциально опасных — на 8,42%, а рекламных — на 9,83%.

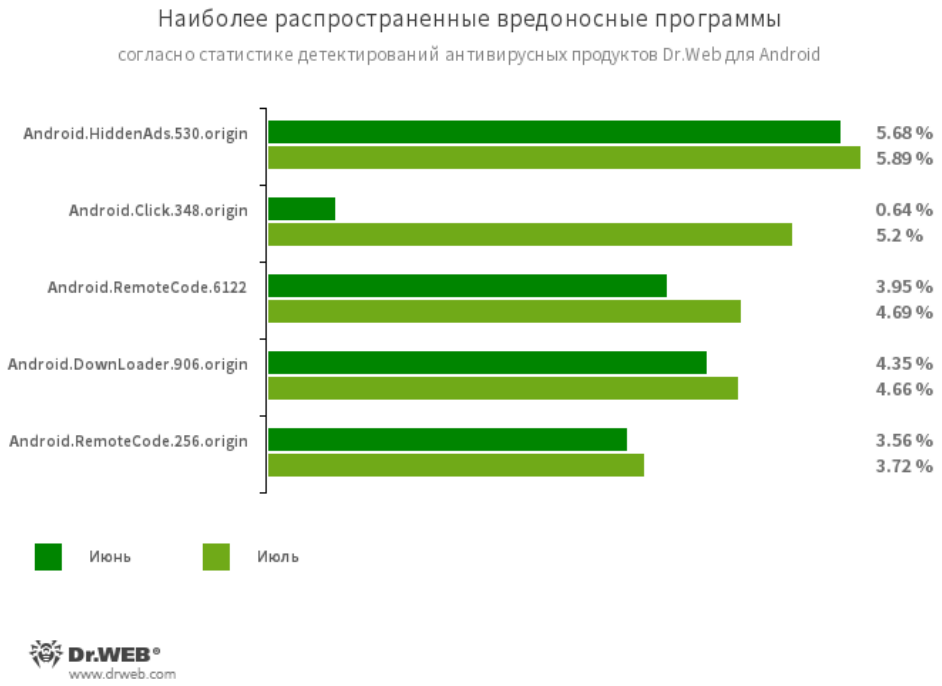
В течение месяца вирусные аналитики «Доктор Веб» выявили в каталоге Google Play несколько новых вредоносных программ. Одной из них был банковский троян Android.Banker.3259, скрывавшийся в приложении для работы с СМС. Другие оказались троянами семейства Android.HiddenAds, которые показывали надоедливые рекламные баннеры. Кроме того, был обнаружен очередной представитель семейства Android.Joker, подписывавший пользователей на премиум-сервисы и выполнявший произвольный код.

ГЛАВНЫЕ ТЕНДЕНЦИИ ИЮЛЯ

- Снижение общего числа угроз, найденных на Android-устройствах
- Распространение новых угроз в каталоге Google Play

«Доктор Веб»: обзор вирусной активности для мобильных устройств в июле 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.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.RemoteCode.6122

Android.RemoteCode.256.origin

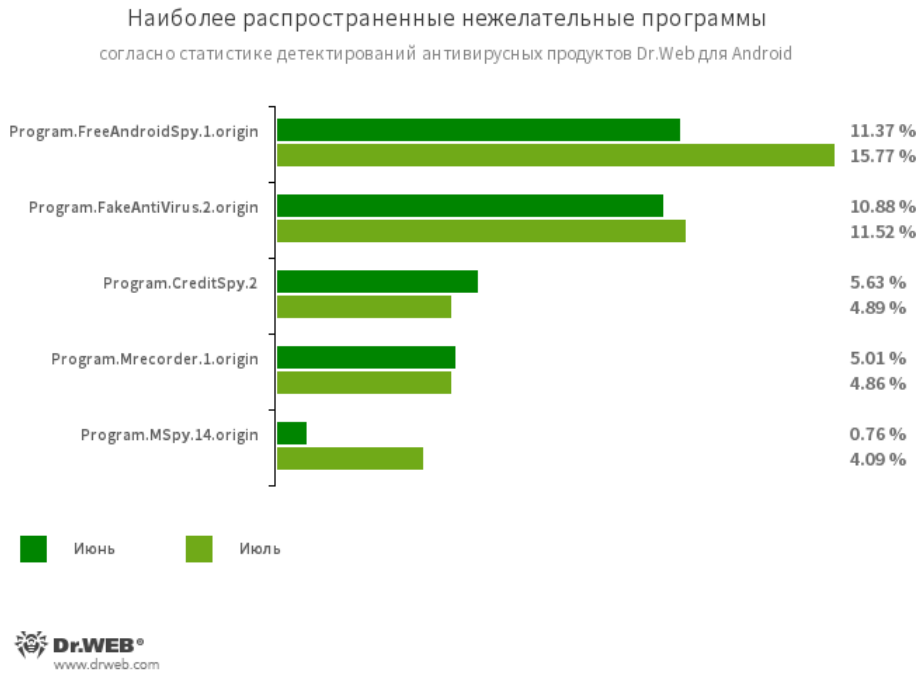
Вредоносные программы, которые загружают и выполняют произвольный код. В зависимости от модификации эти трояны могут загружать различные веб-сайты, переходить по ссылкам, нажимать на рекламные баннеры, подписывать пользователей на платные услуги и выполнять другие действия.

Android.DownLoader.906.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 июле 2020 года

По данным антивирусных продуктов Dr.Web для Android



Program.FreeAndroidSpy.1.origin

Program.Mrecorder.1.origin

Program.MSpy.14.origin

Приложения, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа. Они могут 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

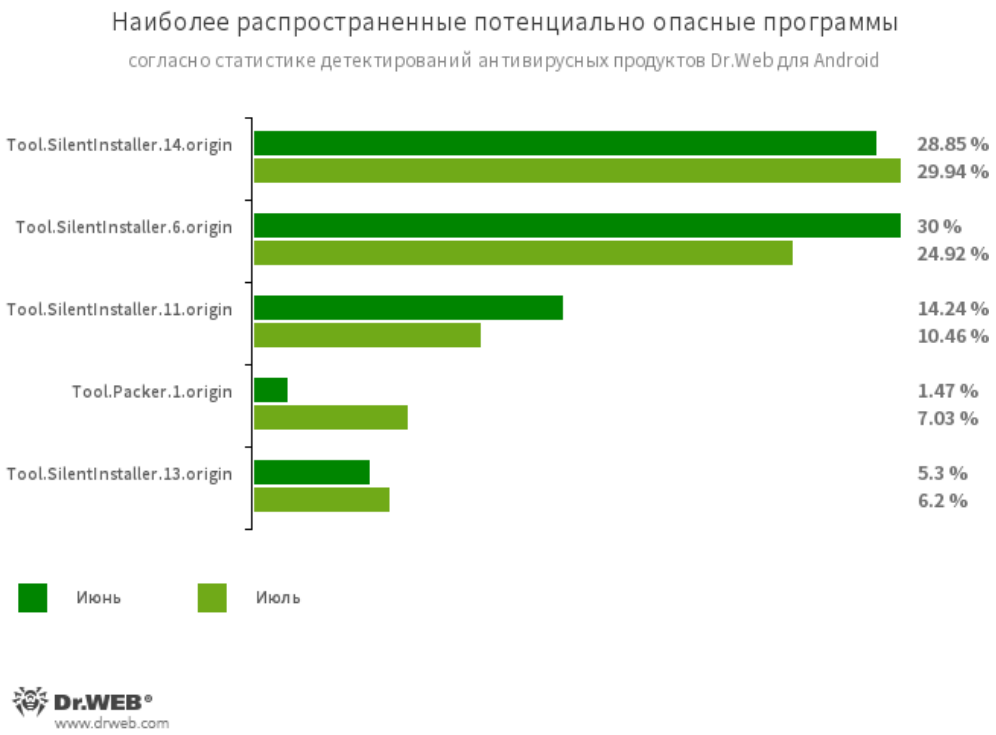
Детектирование рекламных программ, которые имитируют работу антивирусного ПО. Такие программы могут сообщать о несуществующих угрозах и вводить пользователей в заблуждение, требуя оплатить покупку полной версии.

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 июле 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

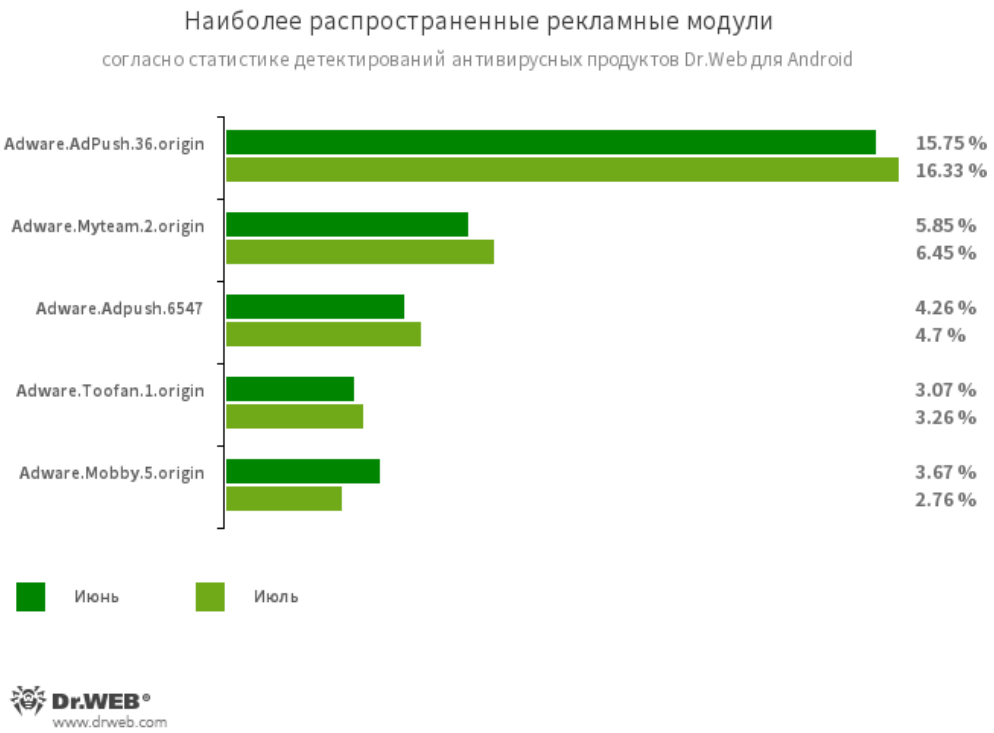
Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

Tool.Packer.1.origin

Специализированная утилита-упаковщик, предназначенная для защиты Android-приложений от модификации и обратного инжиниринга. Она не является вредоносной, но может быть использована для защиты как безобидных, так и троянских программ.

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

По данным антивирусных продуктов Dr.Web для Android

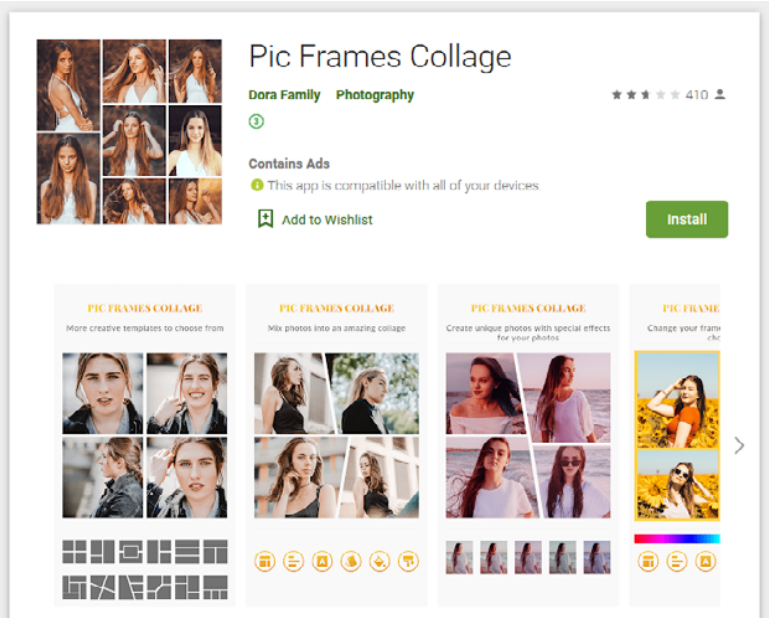


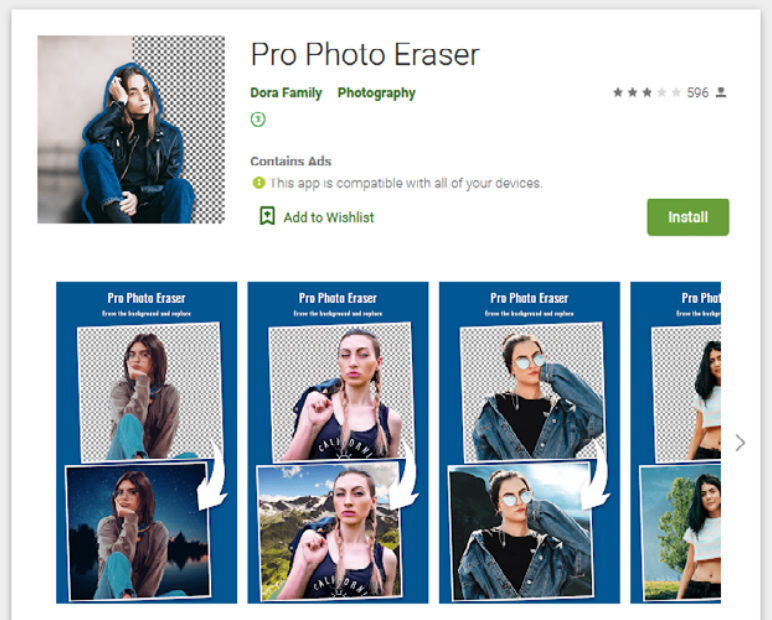
Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать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

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

Угрозы в Google Play

Среди угроз, выявленных в Google Play в июле, были новые представители семейства Android.HiddenAds, добавленные в вирусную базу Dr.Web как Android.HiddenAds.2190 и Android.HiddenAds.2193. Злоумышленники распространяли их под видом приложений для редактирования фотографий.



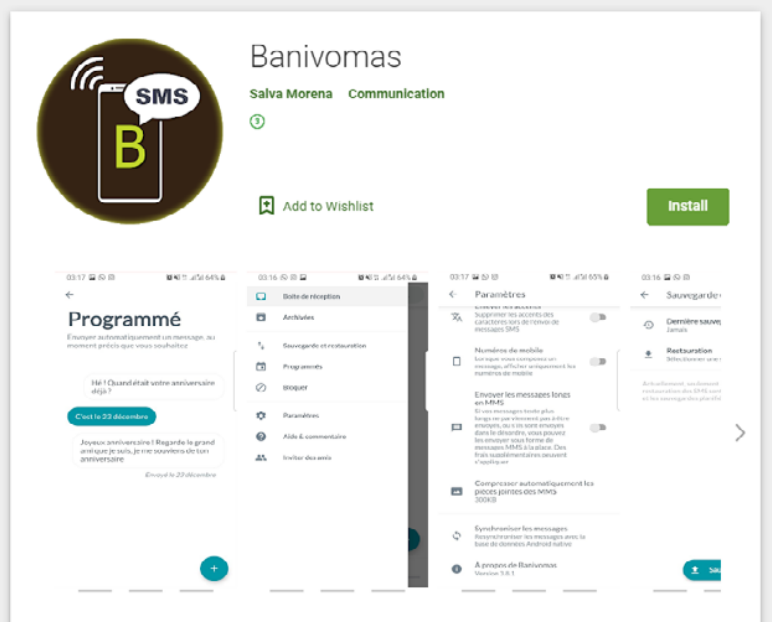


Угрозы в Google Play

Как и другие трояны этого семейства, после запуска они скрывали свои значки из списка программ в меню главного экрана, чтобы пользователям было сложнее их удалить. После этого они начинали показывать баннеры поверх окон других приложений и интерфейса операционной системы.

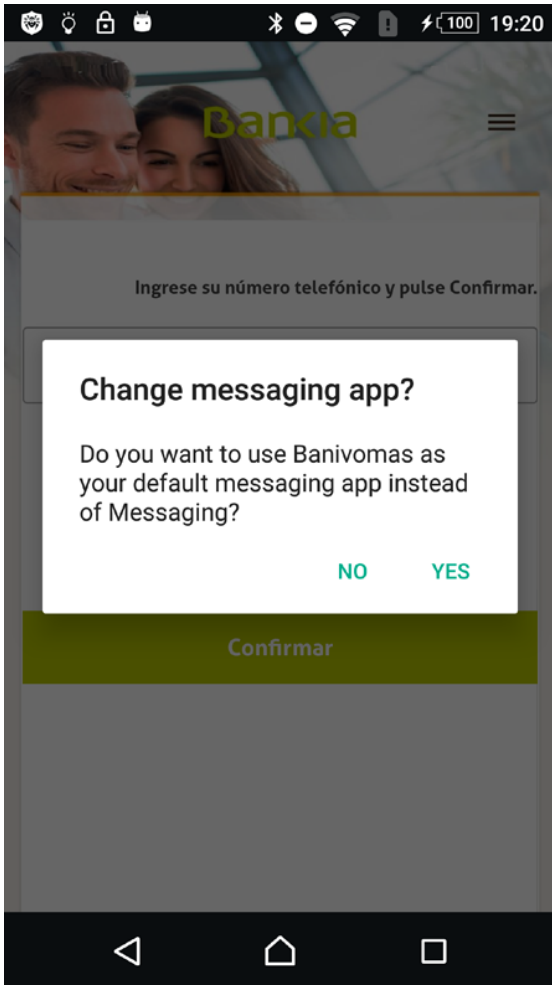
Другой троян, которого обнаружили вирусные аналитики «Доктор Веб», получил имя Android.Joker.279. Он скрывался в приложении для работы с СМС и после запуска подписывал жертв на дорогостоящие мобильные сервисы, а также мог выполнять произвольный код.

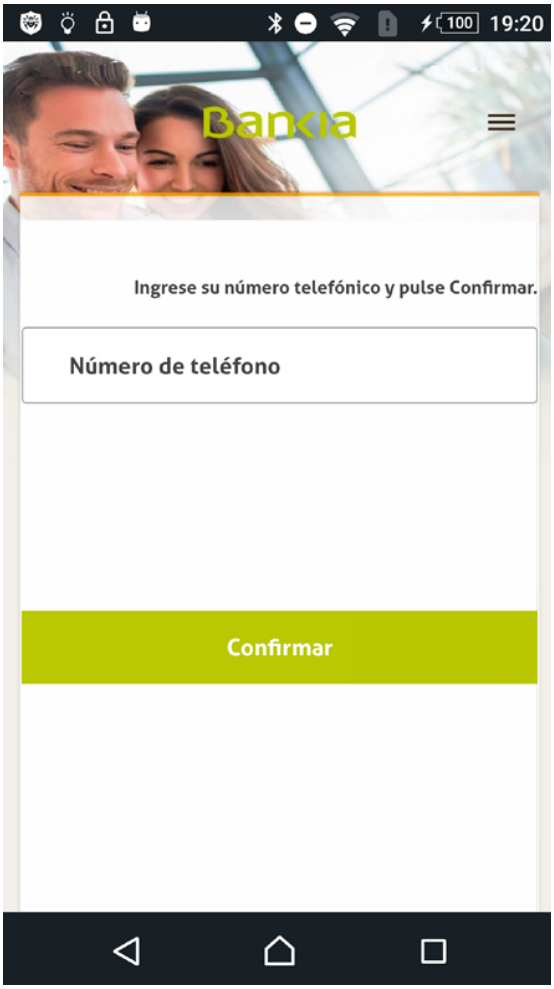
Также наши специалисты выявили банковского трояна Android.Banker.3259. Вирусописатели создали его на основе СМС-мессенджера с открытым исходным кодом.



При запуске банкер соединяется с управляющим сервером и ожидает от него дальнейших команд. В зависимости от полученного ответа троян либо продолжает работать как безобидное приложение, либо пытается украсть у жертвы ее персональные данные, показывая фишинговое окно. Кроме того, Android.Banker.3259 сохраняет все входящие и исходящие СМС в облачную базу данных Firebase. В дальнейшем злоумышленники могут использовать информацию, полученную из этих сообщений, для организации новых атак.

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 июле 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