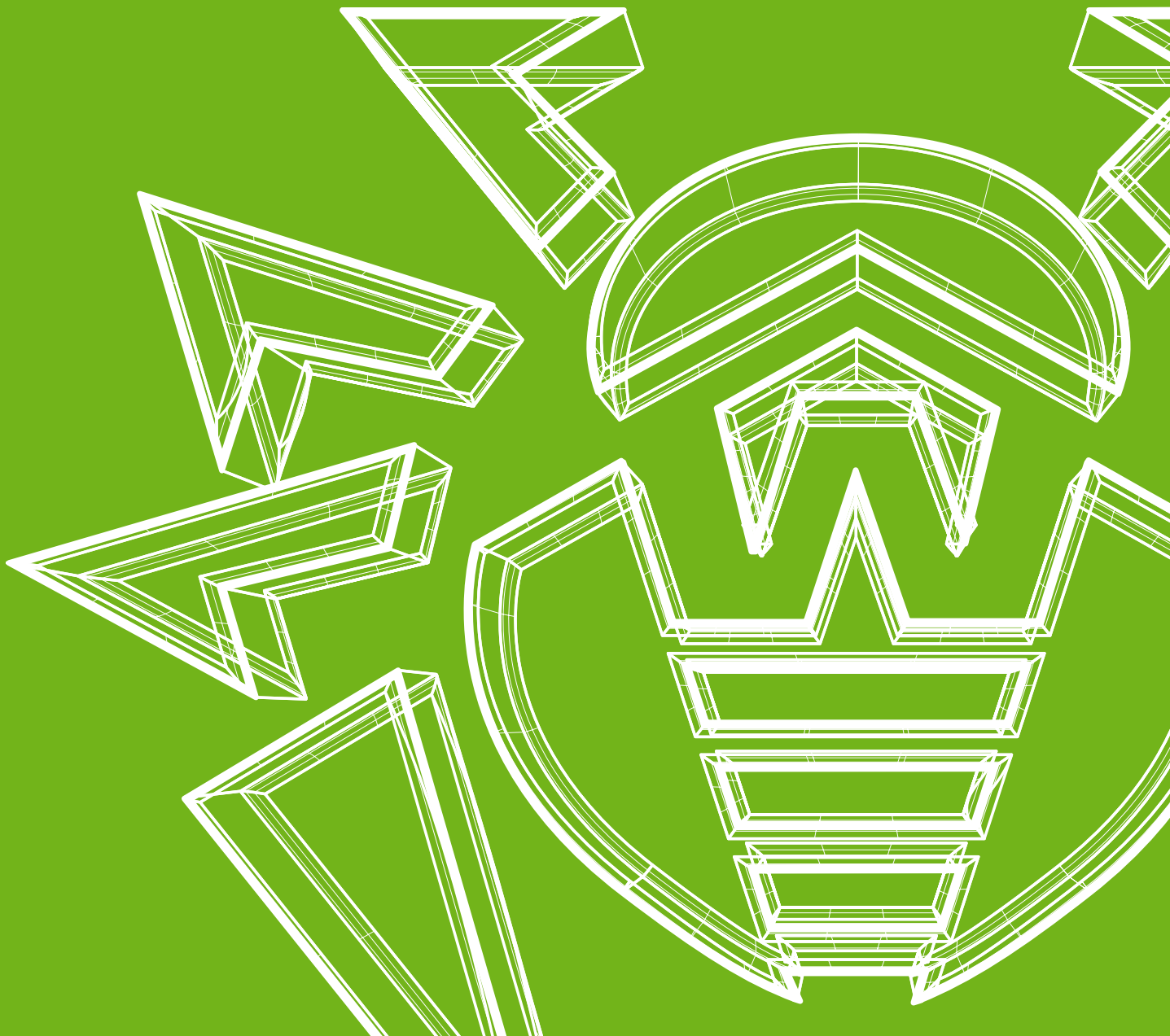
Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2021 года



«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2021 года

29 ноября 2021 года

Согласно статистике детектирований антивирусных продуктов Dr.Web для Android за октябрь, основной угрозой для пользователей остаются рекламные трояны, а также вредоносные программы, загружающие различное ПО и способные выполнять произвольный код.

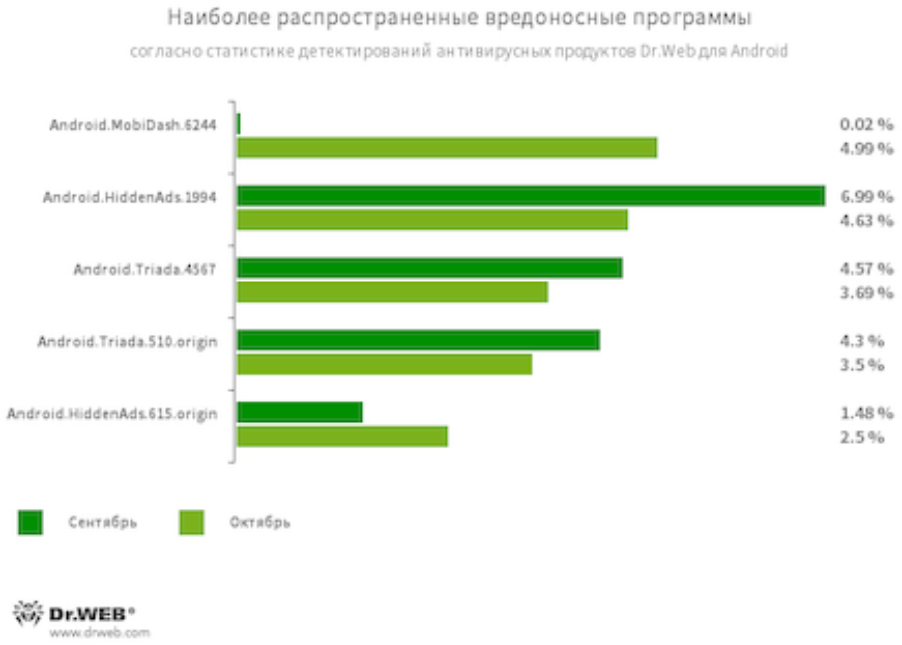
В прошлом месяце наши специалисты обнаружили в каталоге Google Play троянов, подписывающих жертв на платные услуги и крадущих логины и пароли от учетных записей социальной сети Facebook, а также вредоносные программы, превращающие Android-устройства пользователей в прокси-серверы.

ГЛАВНЫЕ ТЕНДЕНЦИИ ОКТЯБРЯ

- Активность рекламных троянов и вредоносных приложений, загружающих другое ПО
- Появление новых вредоносных программ в каталоге Google Play

«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2021 года

По данным антивирусных продуктов Dr.Web для Android



Android.MobiDash.6244

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

Android.HiddenAds.1994

Android.HiddenAds.615.origin

Трояны, предназначенные для показа навязчивой рекламы. Трояны этого семейства часто распространяются под видом безобидных приложений и в некоторых случаях устанавливаются в системный каталог другими вредоносными программами.

Android.Triada.4567

Android.Triada.510.origin

Многофункциональные трояны, выполняющие разнообразные вредоносные действия. Относятся к семейству троянских приложений, проникающих в процессы всех работающих программ. Различные представители этого семейства могут встречаться в прошивках Android-устройств, куда злоумышленники внедряют их на этапе производства. Кроме того, некоторые их модификации могут эксплуатировать уязвимости, чтобы получить доступ к защищенным системным файлам и директориям.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2021 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.SecretVideoRecorder.1.origin

Приложение, предназначенное для фоновой фото- и видеосъемки через встроенные камеры Android-устройств. Оно может работать незаметно, позволяя отключить уведомления о записи, а также изменять значок и описание приложения на фальшивые. Такая функциональность делает данную программу потенциально опасной.

Program.FreeAndroidSpy.1.origin

Program.Gemius.1.origin

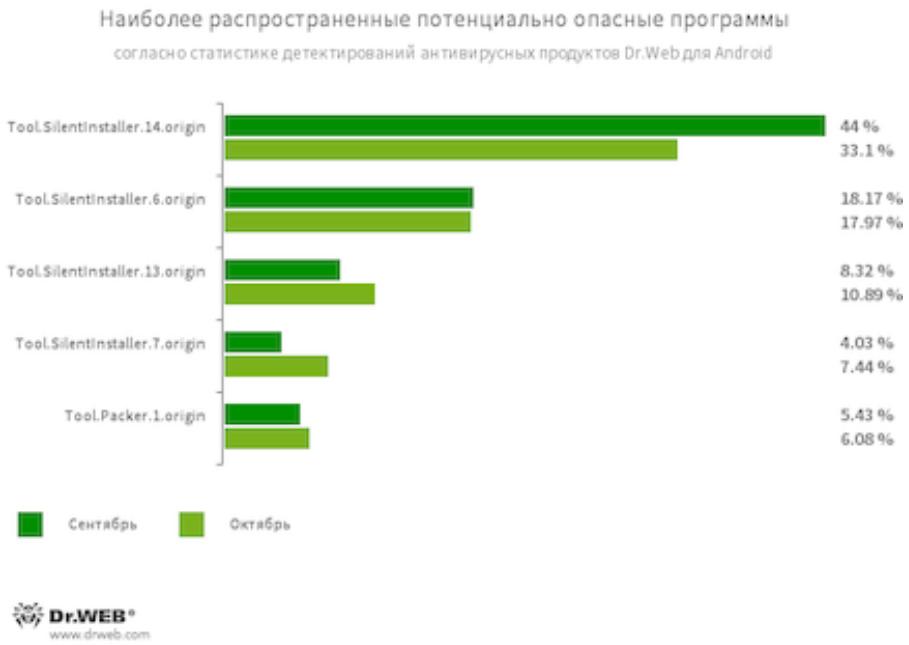
Приложения, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа. Они способны контролировать местоположение устройств, собирать данные об СМС-переписке, беседах в социальных сетях, копировать документы, фотографии и видео, прослушивать телефонные звонки и окружение и т. п.

Program.KeyStroke.3

Android-программа, способная перехватывать вводимую на клавиатуре информацию. Некоторые ее модификации также позволяют отслеживать входящие СМС-сообщения, контролировать историю телефонных звонков и выполнять запись телефонных разговоров.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2021 года

По данным антивирусных продуктов Dr.Web для Android



Tool.SilentInstaller.14.origin

Tool.SilentInstaller.6.origin

Tool.SilentInstaller.13.origin

Tool.SilentInstaller.7.origin

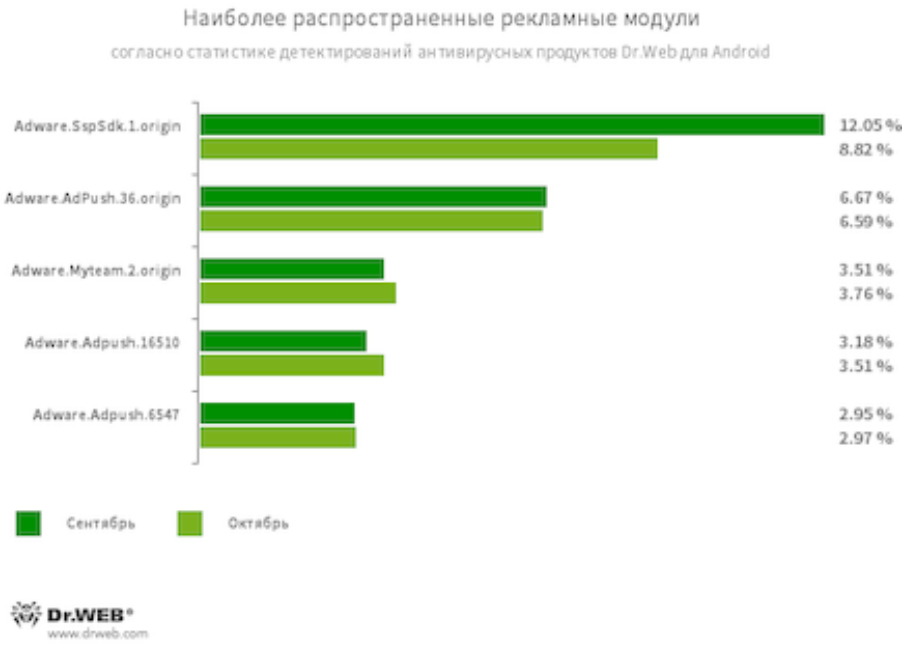
Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

Tool.Packer.1.origin

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

«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2021 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.SspSdk.1.origin

Adware.AdPush.36.origin

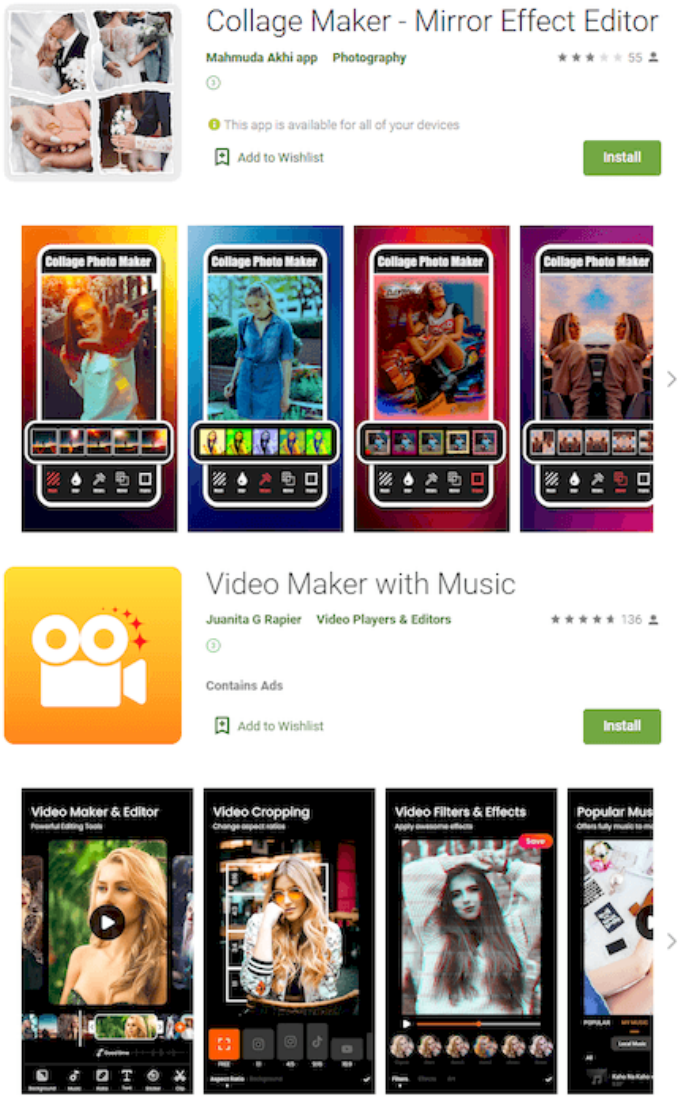
Adware.Adpush.16510

Adware.Adpush.6547

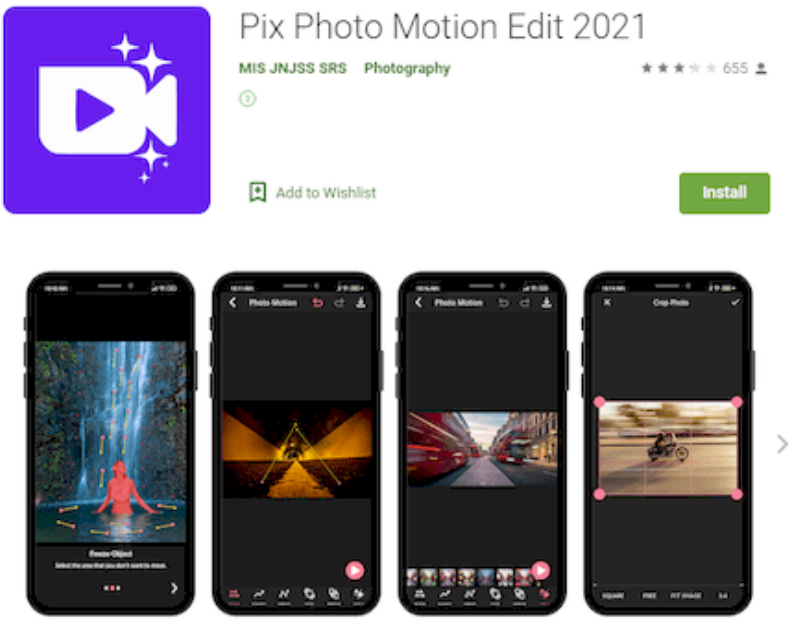
Adware.Myteam.2.origin

Угрозы в Google Play

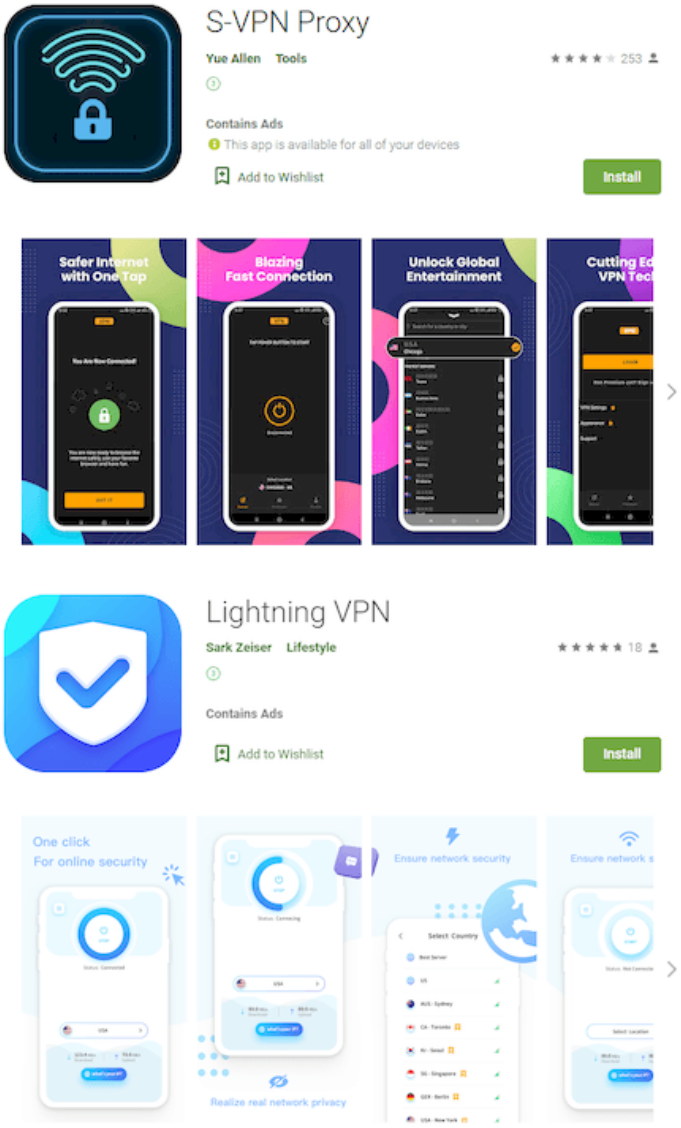
Среди выявленных в каталоге Google Play вредоносных приложений были очередные трояны, предназначенные для кражи логинов и паролей от учетных записей Facebook. Они распространялись под видом полезного ПО — фото- и видеоредакторов Pix Photo Motion Edit 2021, Collage Maker — Mirror Effect Editor и Video Maker with Music, а также VPN-клиентов Kangaroo VPN, S-VPN Proxy и Lightning VPN. Эти трояны были добавлены в вирусную базу Dr.Web как Android.PWS.Facebook.38, Android.PWS.Facebook.40, Android.PWS.Facebook.41, Android.PWS.Facebook.59, Android.PWS.Facebook.64 и Android.PWS.Facebook.67.



Угрозы в Google Play



Угрозы в Google Play

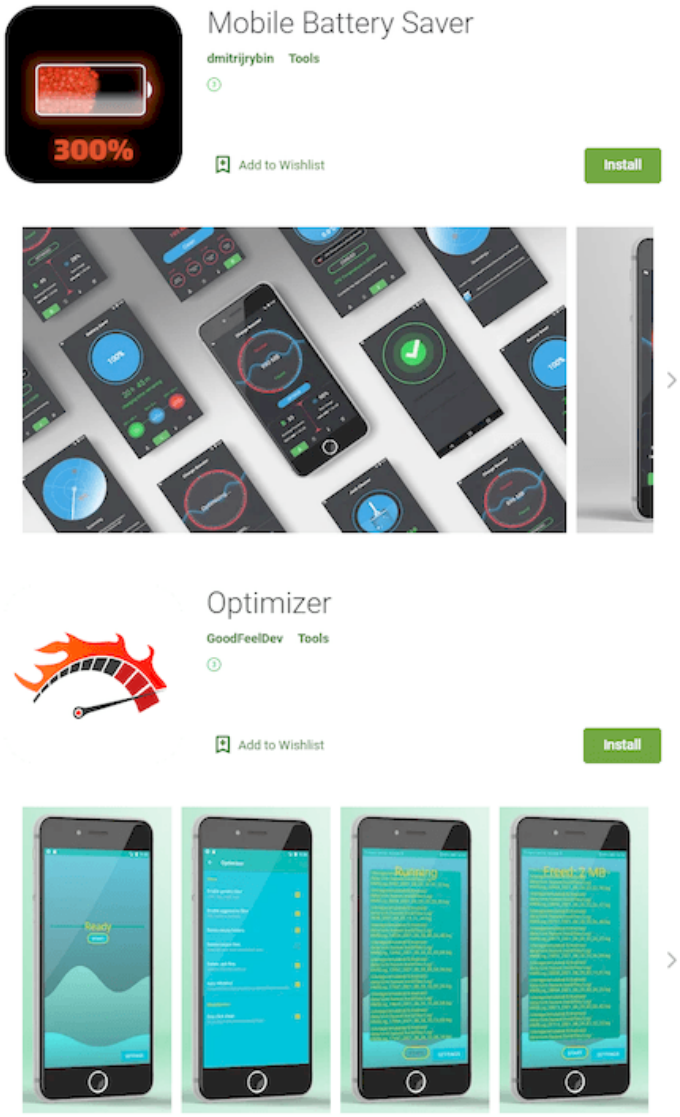


Кроме того, вирусные аналитики «Доктор Веб» обнаружили новые модификации опасных вредоносных программ из семейства Android.Joker, подписывающих пользователей на платные мобильные услуги и способные загружать и выполнять произвольный код. Они получили имена Android.Joker.1012 и Android.Joker.1017. Трояны распространялись под видом приложений Color Call Flash Alert on Call и Apply Flasher, уведомляющих о входящих звонках и сообщениях.

Угрозы в Google Play

Также наши специалисты обнаружили вредоносные программы Android.Proxy.29 и Android.Proxy.41.origin, распространявшиеся под видом приложений Mobile Battery Saver и Optimizer для оптимизации работы Android-устройств. В действительности это были трояны, превращающие устройства жертв в прокси-серверы для переадресации трафика злоумышленников.

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 октябре 2021 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, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах