Dr.WEB®
с 1992 года

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

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

13 мая 2021 года

В апреле компания «Доктор Веб» сообщила об обнаружении трояна Android.Triada.4912, встроенного в одну из версий клиентского приложения популярного стороннего каталога Android-программ APKPure. В то же время в официальном каталоге Google Play вновь были выявлены очередные трояны из семейства Android.FakeApp. Они распространялись под видом полезных программ и загружали различные мошеннические сайты. Кроме того, специалисты «Доктор Веб» выявили троянов Android.Joker в магазине ПО AppGallery компании Huawei. Эти вредоносные приложения подписывали пользователей на платные мобильные услуги.

ГЛАВНЫЕ ТЕНДЕНЦИИ АПРЕЛЯ

- Обнаружение трояна в клиентском приложении популярного стороннего каталога Android-программ APKPure
- Распространение новых угроз через каталог Google Play
- Обнаружение угроз в магазине приложений AppGallery

Мобильная угроза месяца

В начале апреля компания «Доктор Веб» опубликовала новость о том, что наши вирусные аналитики обнаружили вредоносную функциональность в клиентском приложении стороннего каталога Android-программ и игр APKPure. Неустановленные злоумышленники встроили в него трояна Android.Triada.4912, затронутой оказалась версия 3.17.18 приложения. Android.Triada.4912 запускал скрытый в нем вспомогательный модуль, который выполнял основные вредоносные действия: скачивал другие троянские компоненты и различные программы, а также загружал всевозможные веб-сайты.

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

По данным антивирусных продуктов Dr.Web для Android

Android.HiddenAds.1994

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.RemoteCode.284.origin

Android.RemoteCode.6122

Android.RemoteCode.319.origin

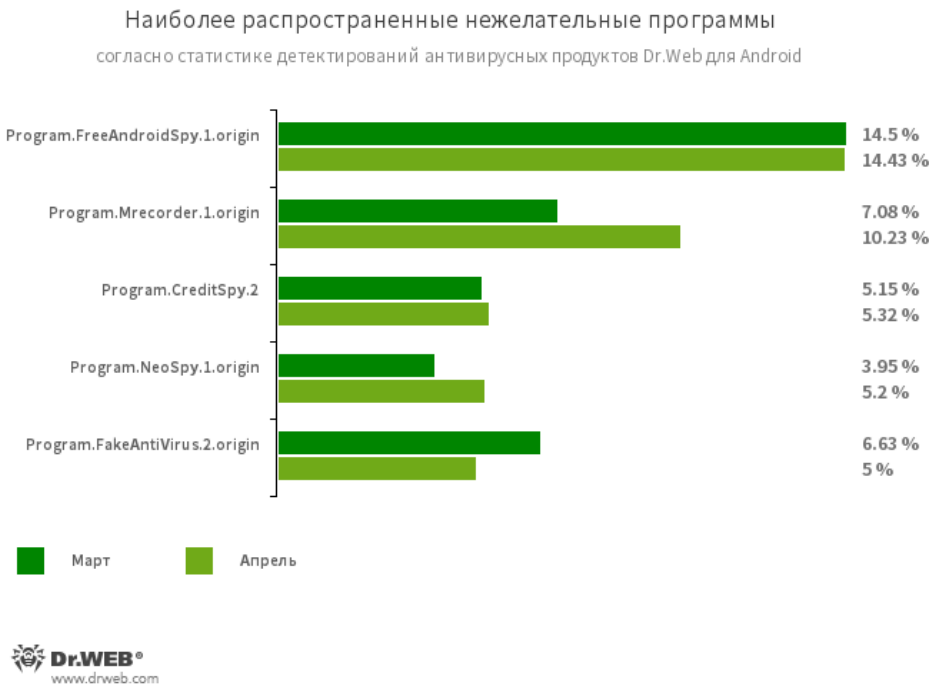
Вредоносная программа, которая загружает и выполняет произвольный код. В зависимости от модификации она также может загружать различные веб-сайты, переходить по ссылкам, нажимать на рекламные баннеры, подписывать пользователей на платные услуги и выполнять другие действия.

Android.Triada.510.origin

Многофункциональный троян, выполняющий разнообразные вредоносные действия. Относится 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 апреле 2021 года

По данным антивирусных продуктов Dr.Web для Android



Program.FreeAndroidSpy.1.origin

Program.Mrecorder.1.origin

Program.NeoSpy.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.CreditSpy.2

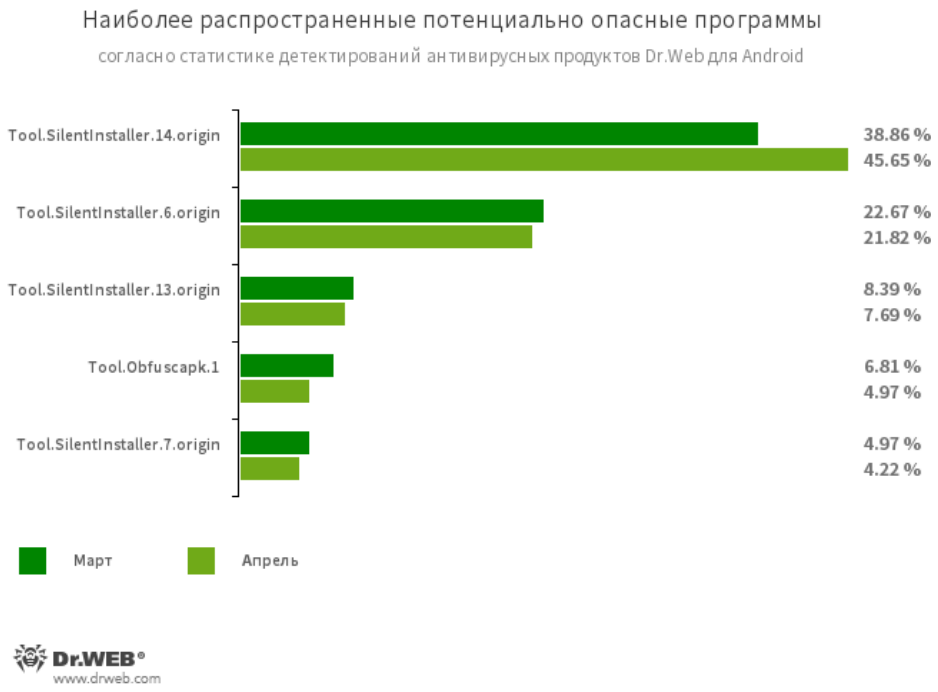
Детектирование программ, предназначенных для присвоения кредитного рейтинга на основании персональных данных пользователей. Такие приложения загружают на удаленный сервер СМС-сообщения, информацию о контактах из телефонной книги, историю вызовов, а также другие сведения.

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.

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

По данным антивирусных продуктов Dr.Web для Android



Tool.SilentInstaller.6.origin

Tool.SilentInstaller.7.origin

Tool.SilentInstaller.13.origin

Tool.SilentInstaller.14.origin

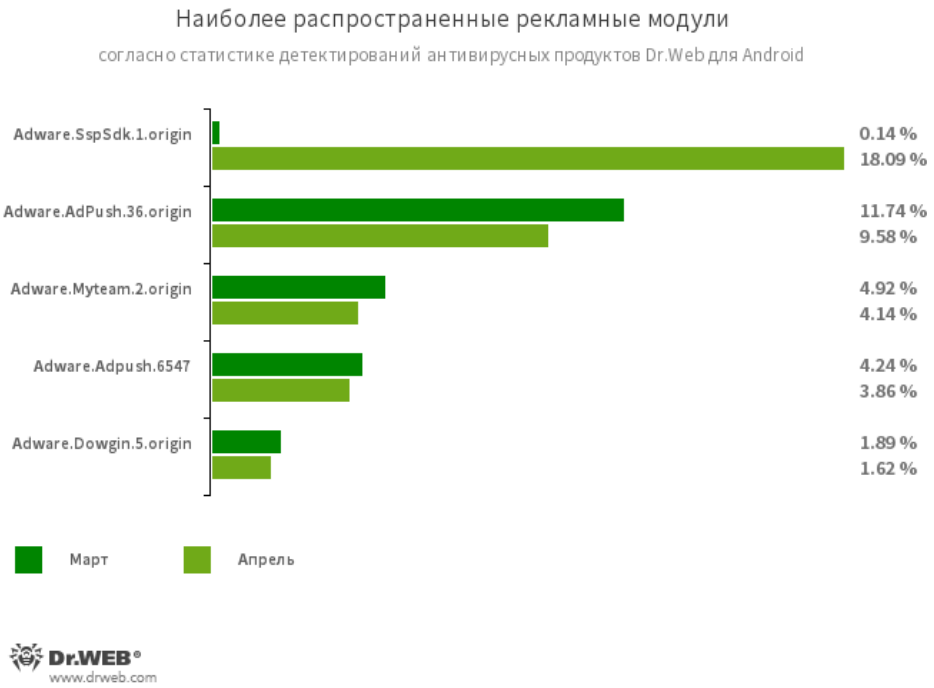
Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

Tool.Obfuscapk.1

Детектирование приложений, защищенных утилитой-обфускатором Obfuscapk. Эта утилита используется для автоматической модификации и запутывания исходного кода Android-приложений, чтобы усложнить их обратный инжиниринг. Злоумышленники применяют ее для защиты вредоносных и других опасных программ от обнаружения антивирусами.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в апреле 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

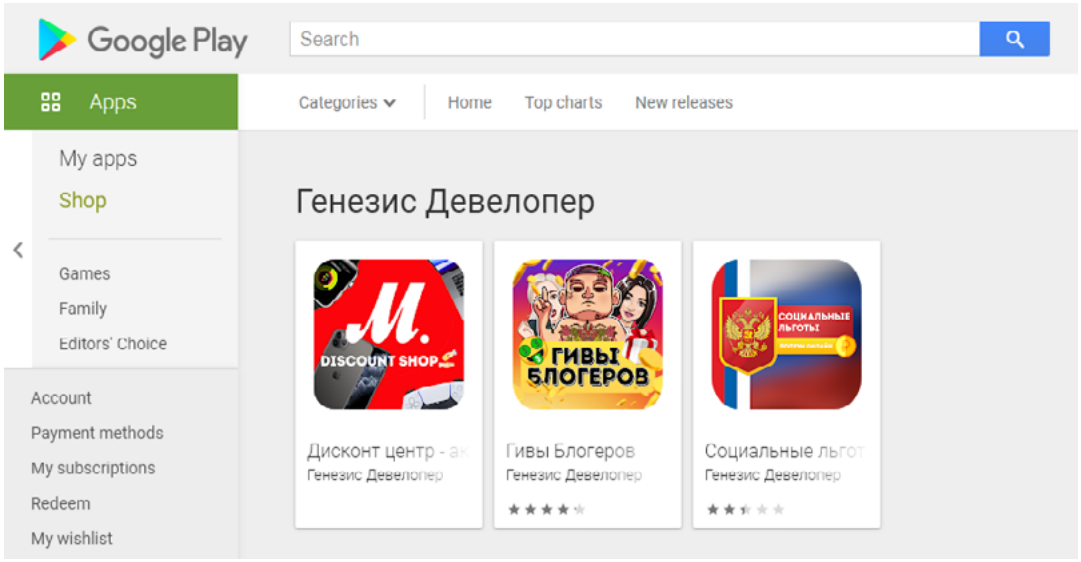
Adware.Adpush.6547

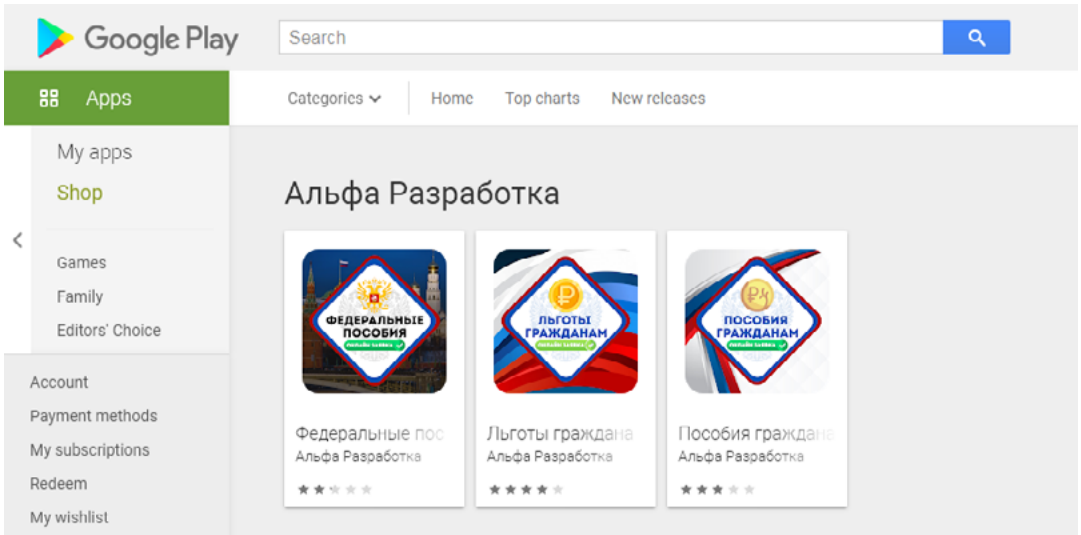
Adware.Myteam.2.origin

Adware.Dowgin.5.origin

Угрозы в Google Play

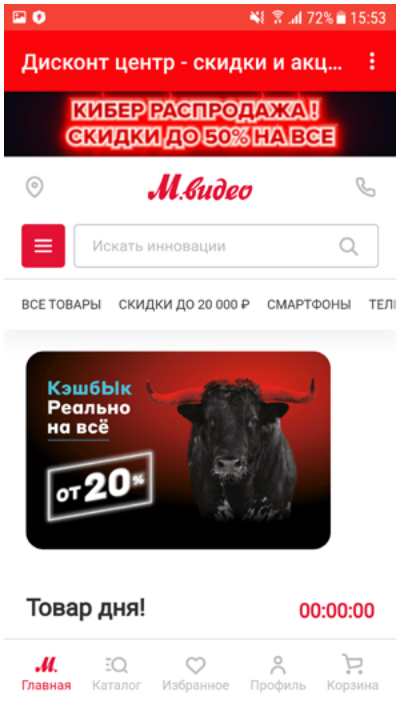
В апреле в каталоге Google Play были выявлены новые трояны, принадлежащие к семейству Android.FakeApp. Они распространялись под видом справочников с информацией о денежных выплатах и компенсациях от государства, а также приложений, с помощью которых пользователи якобы могли получить скидки на покупку товаров в известных торговых сетях и выиграть подарки от популярных блогеров. В действительности эти программы-подделки вводили жертв в заблуждение. Они не выполняли заявленных функций и лишь демонстрировали мошеннические сайты, через которые злоумышленники похищали конфиденциальные данные и деньги владельцев Android-устройств. Трояны были добавлены в вирусную базу Dr.Web как Android.FakeApp.255, Android.FakeApp.254, Android.FakeApp.256, Android.FakeApp.259, Android.FakeApp.260 и Android.FakeApp.261.

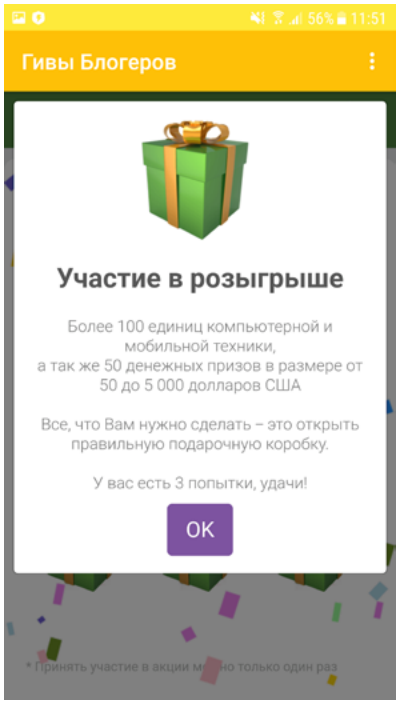




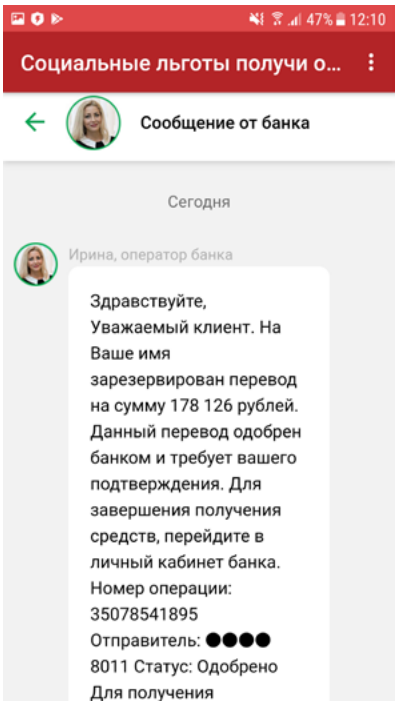
Угрозы в Google Play

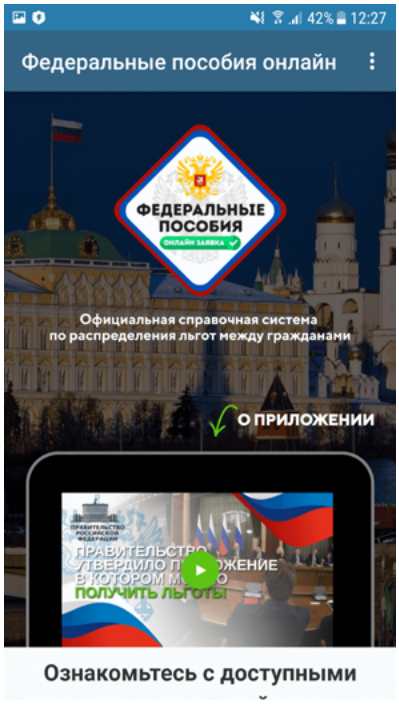
Пример внешнего вида этих мошеннических приложений:

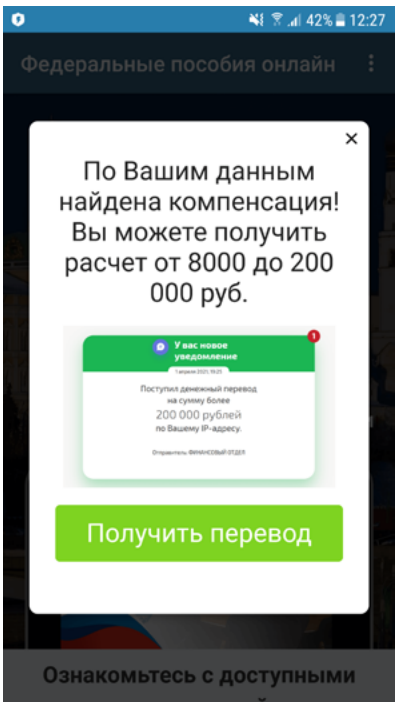




Угрозы в Google Play

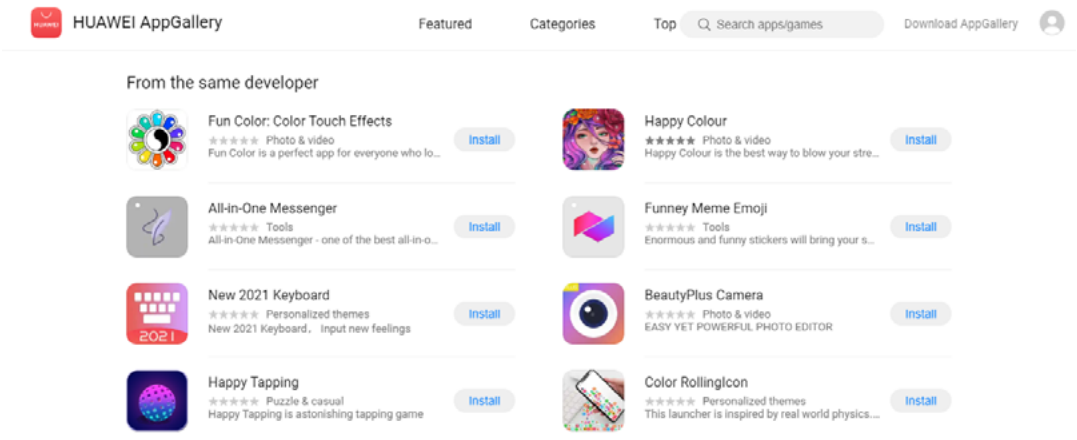






Прочие угрозы

В прошлом месяце вирусные аналитики «Доктор Веб» обнаружили первые вредоносные приложения в каталоге AppGallery компании Huawei. Это были трояны семейства Android.Joker, которые способны выполнять произвольный код и подписывать пользователей на платные мобильные услуги. Они распространялись под видом различных безобидных программ — виртуальных клавиатур, онлайн-мессенджера, программы-фотокамеры и других. В общей сложности их установили более 538 000 пользователей.



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 апреле 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
ВебIQметр | 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