Dr.WEB®
с 1992 года

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

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

22 июня 2021 года

Согласно статистике детектирования, в мае антивирусные продукты Dr.Web для Android чаще всего обнаруживали на защищаемых устройствах рекламных троянов, а также вредоносные приложения, которые загружали другое ПО и выполняли произвольный код.

В течение прошлого месяца специалисты компании «Доктор Веб» выявили в каталоге Google Play множество новых угроз. Среди них были трояны, подписывающие жертв на платные услуги, а также вредоносные программы, загружавшие мошеннические сайты.

ГЛАВНЫЕ ТЕНДЕНЦИИ МАЯ

- Рекламные трояны и вредоносные программы, способные загружать и выполнять произвольный код, остаются одними из наиболее активных угроз
- Обнаружение новых троянов в официальном каталоге Android-приложений Google Play

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

По данным антивирусных продуктов Dr.Web для Android

Android.HiddenAds.1994

Android.HiddenAds.615.origin

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

Android.RemoteCode.284.origin

Android.RemoteCode.6122

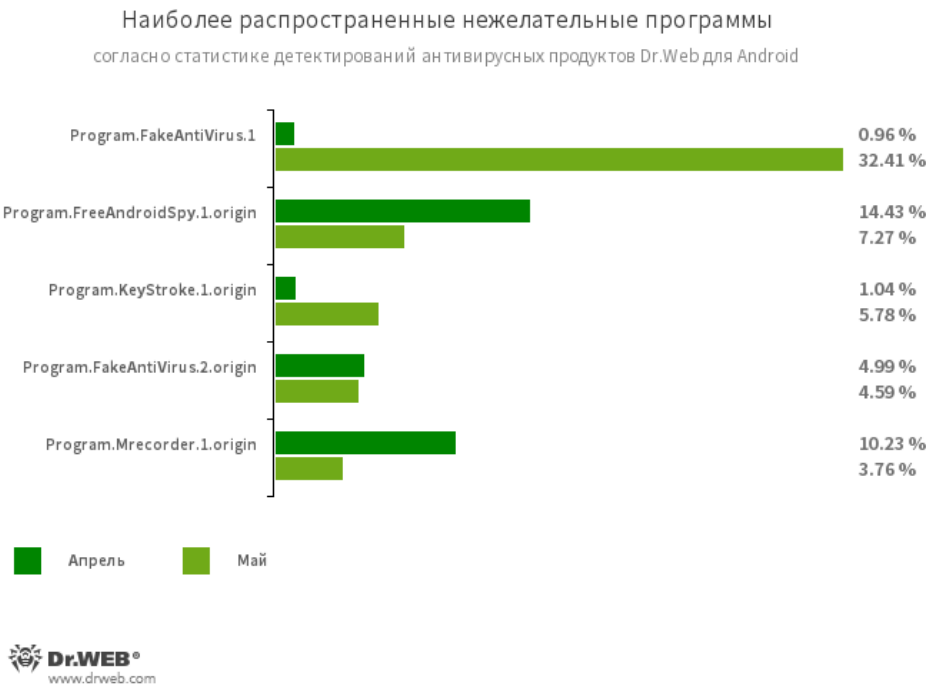
Вредоносные программы, которые загружают и выполняют произвольный код. В зависимости от модификации они также могут загружать различные веб-сайты, переходить по ссылкам, нажимать на рекламные баннеры, подписывать пользователей на платные услуги и выполнять другие действия.

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 мае 2021 года

По данным антивирусных продуктов Dr.Web для Android



Program.FakeAntiVirus.1

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.FreeAndroidSpy.1.origin

Program.Mrecorder.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.1.origin

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

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

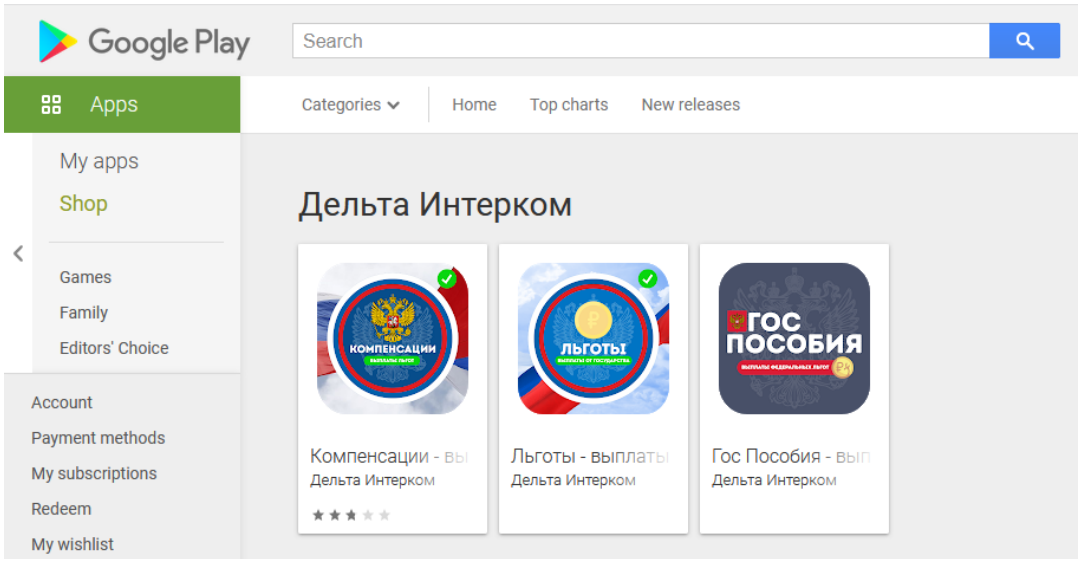
Adware.Adpush.6547

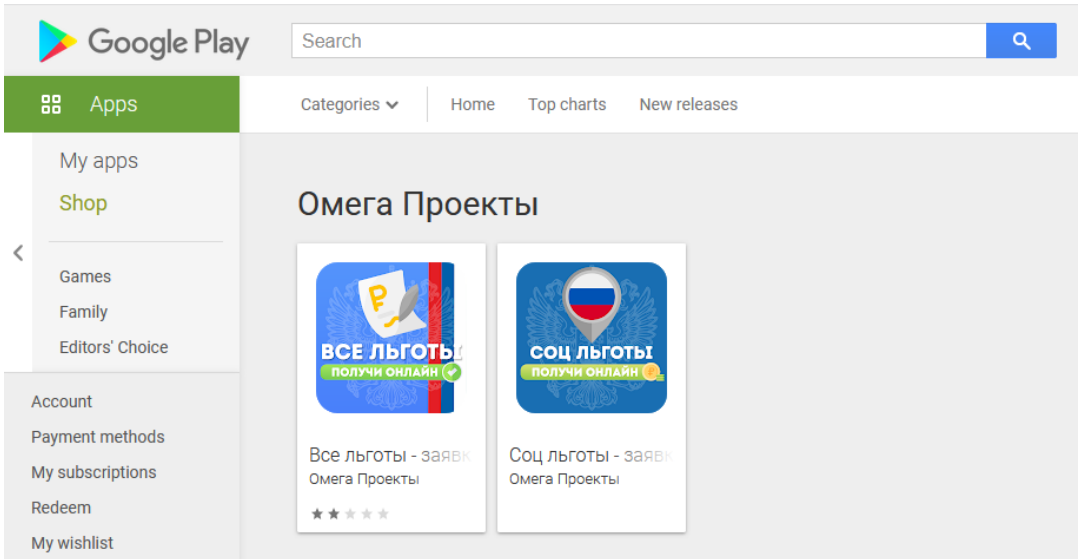
Adware.Adpush.16510

Adware.Myteam.2.origin

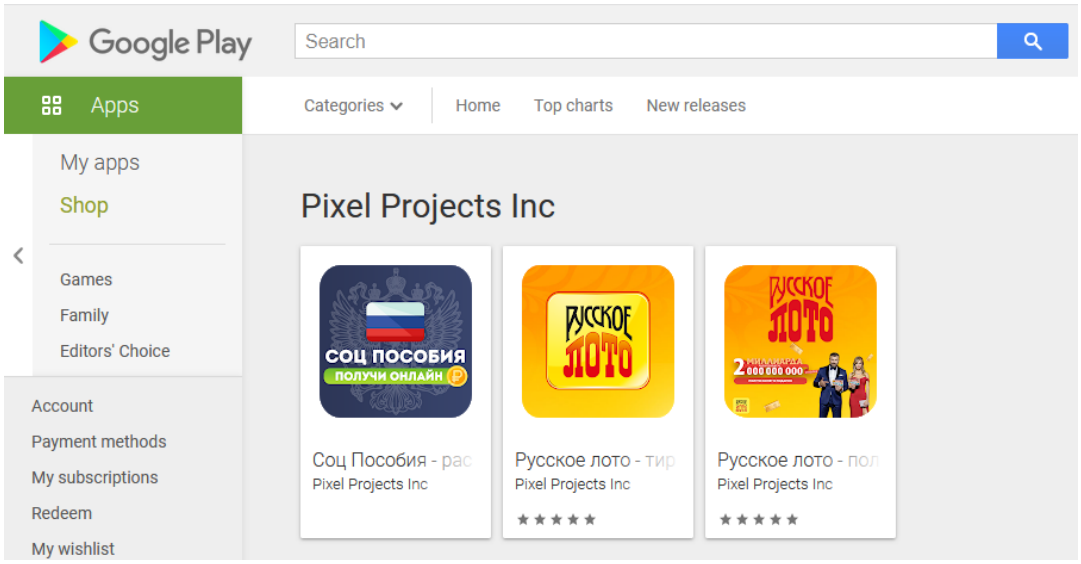
Угрозы в Google Play

В мае специалисты компании «Доктор Веб» выявили в каталоге Google Play множество новых вредоносных приложений. Среди них — очередные трояны из семейства Android.FakeApp. Большинство распространялось под видом программ, с помощью которых пользователи якобы могли найти информацию о пособиях, льготах и денежных компенсациях от государства, а также подать заявку на их получение. Остальные распространялись под видом официальных приложений лотереи «Русское лото», в которых потенциальным жертвам предлагалось получить бесплатные лотерейные билеты, а также проверить наличие выигрышей.





Угрозы в Google Play

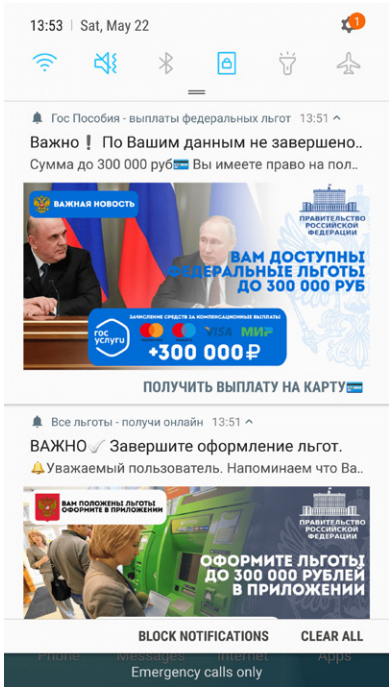


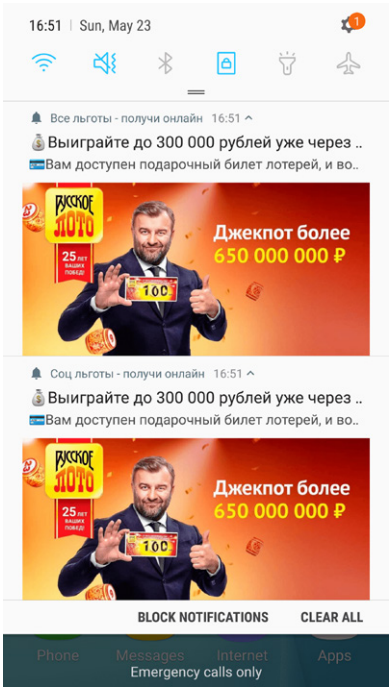
Ни одна из этих программ-подделок не предоставляла обещанной функциональности. Трояны лишь загружали мошеннические веб-сайты, с помощью которых злоумышленники похищали деньги и конфиденциальную информацию владельцев Android-устройств. При этом некоторые из них дополнительно демонстрировали навязчивые уведомления, также ведущие на сайты мошенников. Вредоносные приложения были добавлены в вирусную базу Dr.Web как Android.FakeApp.262, Android.FakeApp.263, Android.FakeApp.264, Android.FakeApp.265, Android.FakeApp.266, Android.FakeApp.269, Android.FakeApp.270, Android.FakeApp.271, Android.FakeApp.272 и Android.FakeApp.273.

Угрозы в Google Play

Вот как выглядят некоторые из этих троянов:

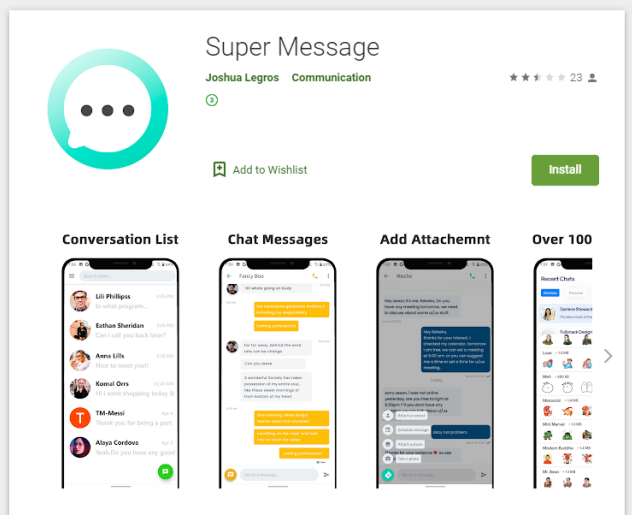
Пример уведомлений, которые они могут демонстрировать:

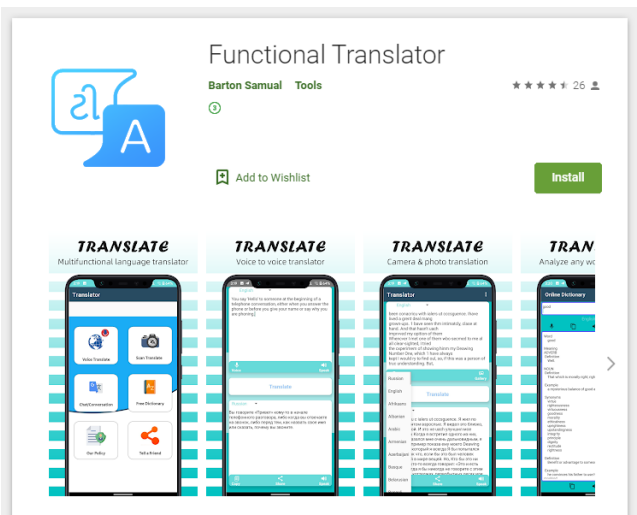


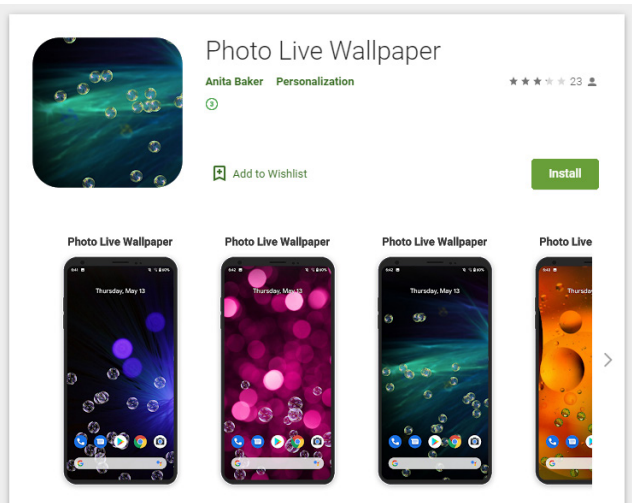


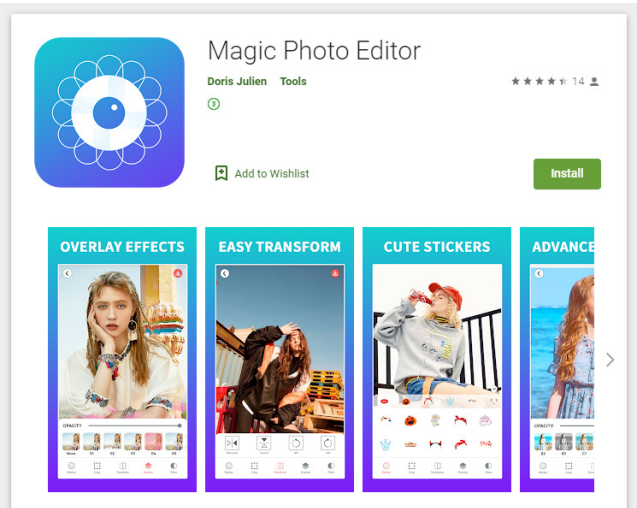
Угрозы в Google Play

Кроме того, наши вирусные аналитики обнаружили новых троянов семейства Android.Joker, способных выполнять произвольный код и подписывать жертв на платные мобильные сервисы. Вредоносные приложения распространялись под видом программ для работы с СМС, переводчика, «живых» обоев для рабочего стола, а также фоторедактора. Они были добавлены в вирусную базу Dr.Web как Android.Joker.722, Android.Joker.723, Android.Joker.729, Android.Joker.730, Android.Joker.739, Android.Joker.742 и Android.Joker.744.









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 мае 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

Узнайте больше
Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека