Dr.WEB®
с 1992 года

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

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

16 сентября 2020 года

В августе на Android-устройствах было выявлено на 2,21% больше угроз, чем в июле. Количество вредоносных программ при этом увеличилось на 6,26%, в то время как число нежелательных приложений сократилось на 0,49%, потенциально опасных — на 13,82%, а рекламных — на 10,1%.

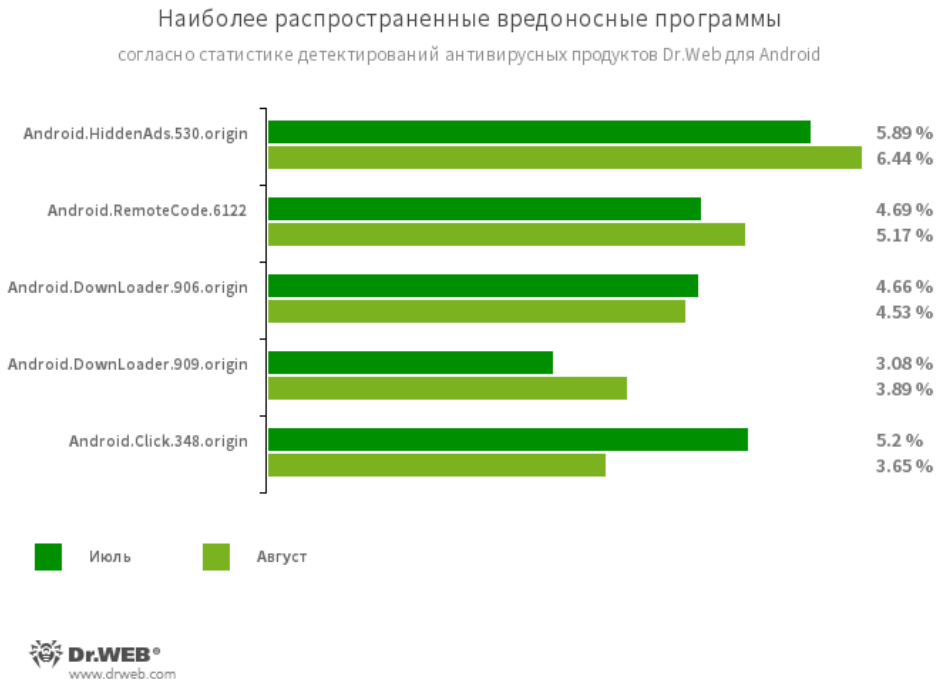
Специалисты компании «Доктор Веб» обнаружили в каталоге Google Play очередные угрозы. В их числе – различные модификации троянских приложений семейства Android.FakeApp, которые распространялись под видом программ-справочников и загружали мошеннические сайты. Кроме того, был найден новый представитель семейства многофункциональных троянов Android.Joker, подписывающий пользователей на платные услуги и способный загружать и исполнять произвольный код.

ГЛАВНЫЕ ТЕНДЕНЦИИ АВГУСТА

- Рост общего числа угроз, зафиксированных на Android-устройствах
- Появление новых угроз в каталоге Google Play

«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 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.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.DownLoader.906.origin

Android.DownLoader.909.origin

Трояны, загружающие другие вредоносные программы и ненужное ПО. Могут скрываться во внешне безобидных приложениях, которые распространяются через каталог Google Play или вредоносные сайты.

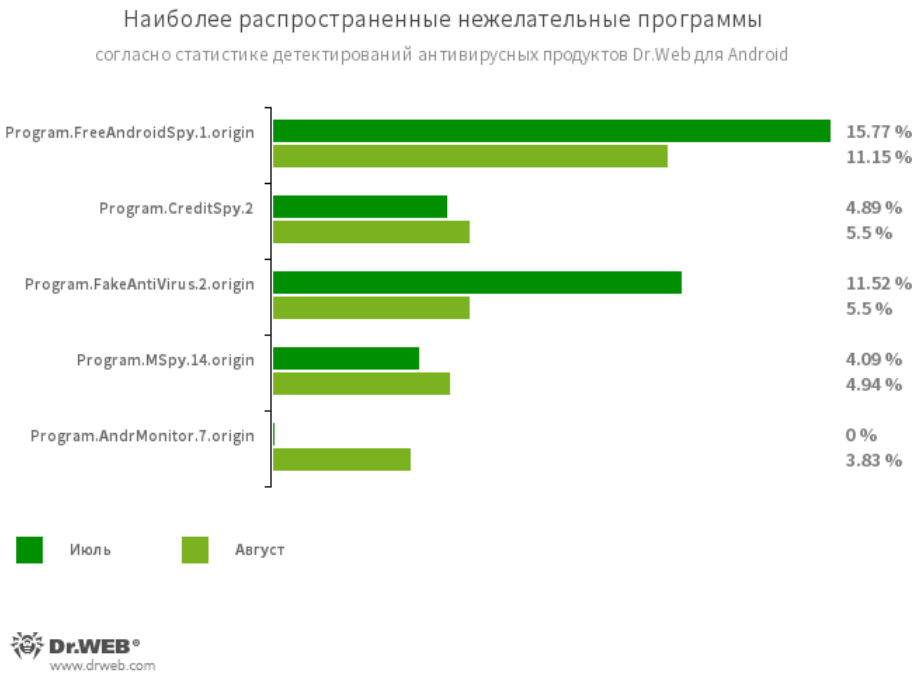
Android.Click.348.origin

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.

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

По данным антивирусных продуктов Dr.Web для Android

.



Program.FreeAndroidSpy.1.origin

Program.AndrMonitor.7.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

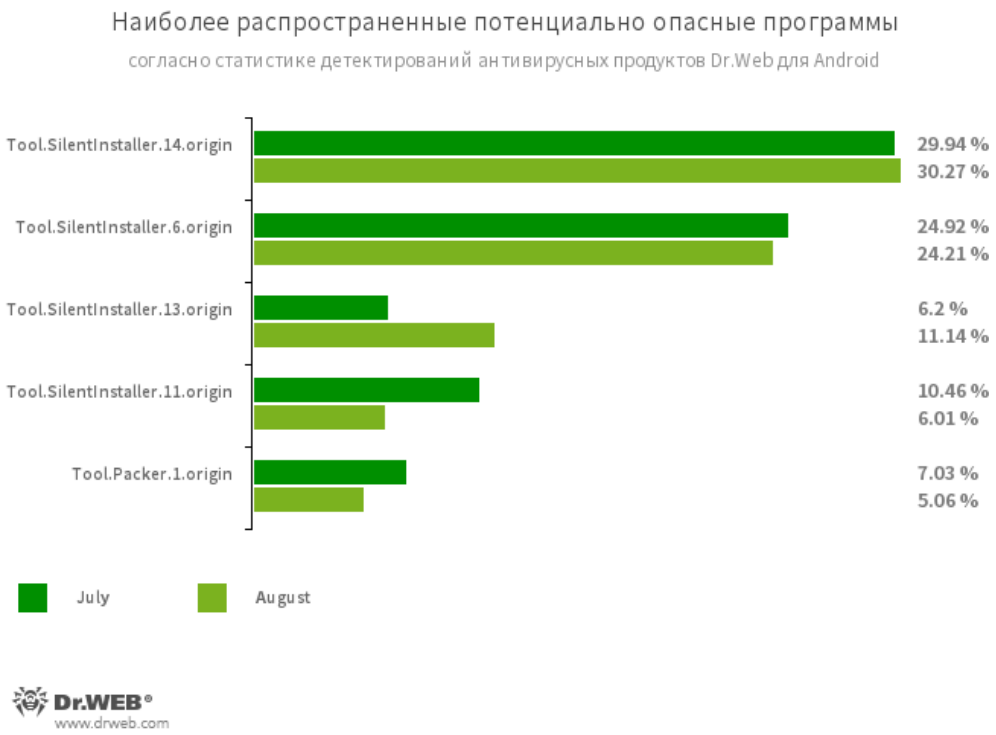
Детектирование рекламных программ, которые имитируют работу антивирусного ПО. Такие программы могут сообщать о несуществующих угрозах и вводить пользователей в заблуждение, требуя оплатить покупку полной версии.

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 августе 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 августе 2020 года

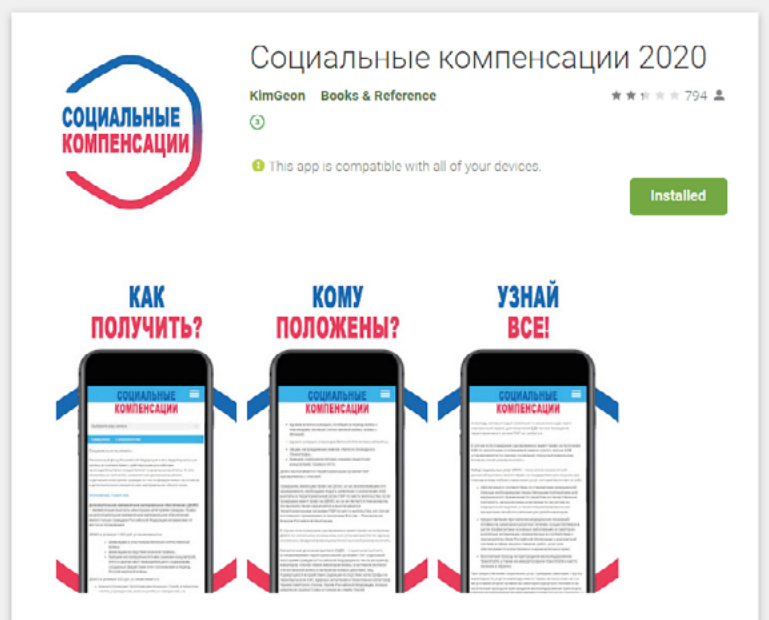
По данным антивирусных продуктов Dr.Web для Android

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.

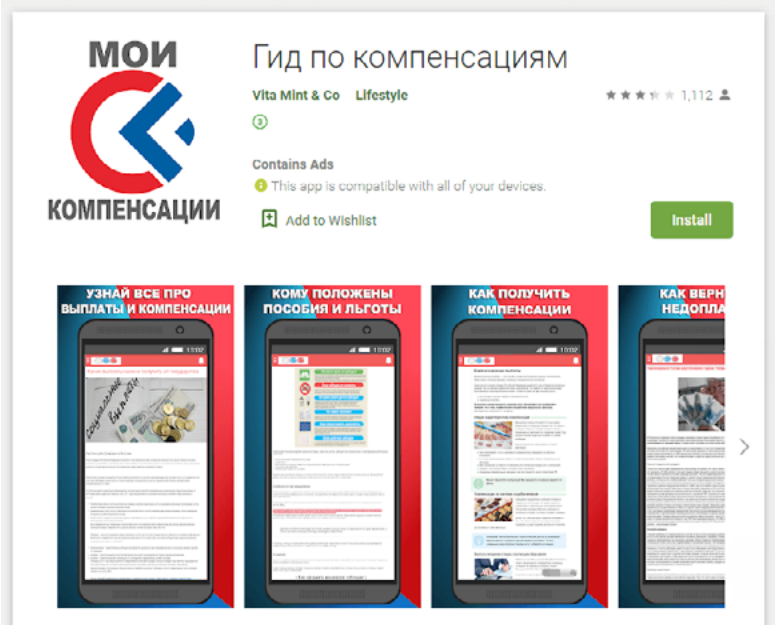
- Adware.Adpush.36.origin
- Adware.Adpush.6547
- Adware.Myteam.2.origin
- Adware.Mobby.5.origin
- Adware.Toofan.1.origin

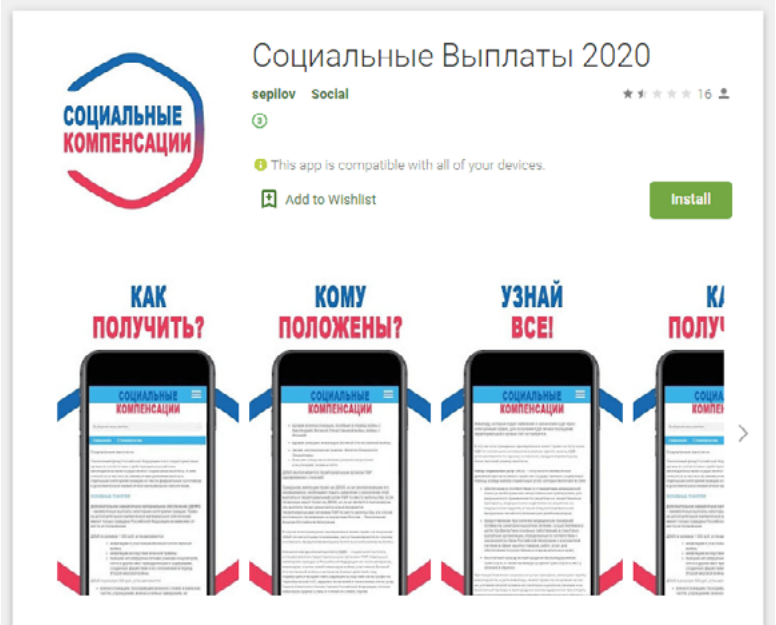
Угрозы в Google Play

В августе вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play сразу несколько новых вредоносных программ семейства Android.FakeApp, получивших имена Android.FakeApp.199, Android.FakeApp.200, Android.FakeApp.202 и Android.FakeApp.203. Они распространялись под видом справочников с информацией о получении социальных выплат и возврате НДС.



Угрозы в Google Play

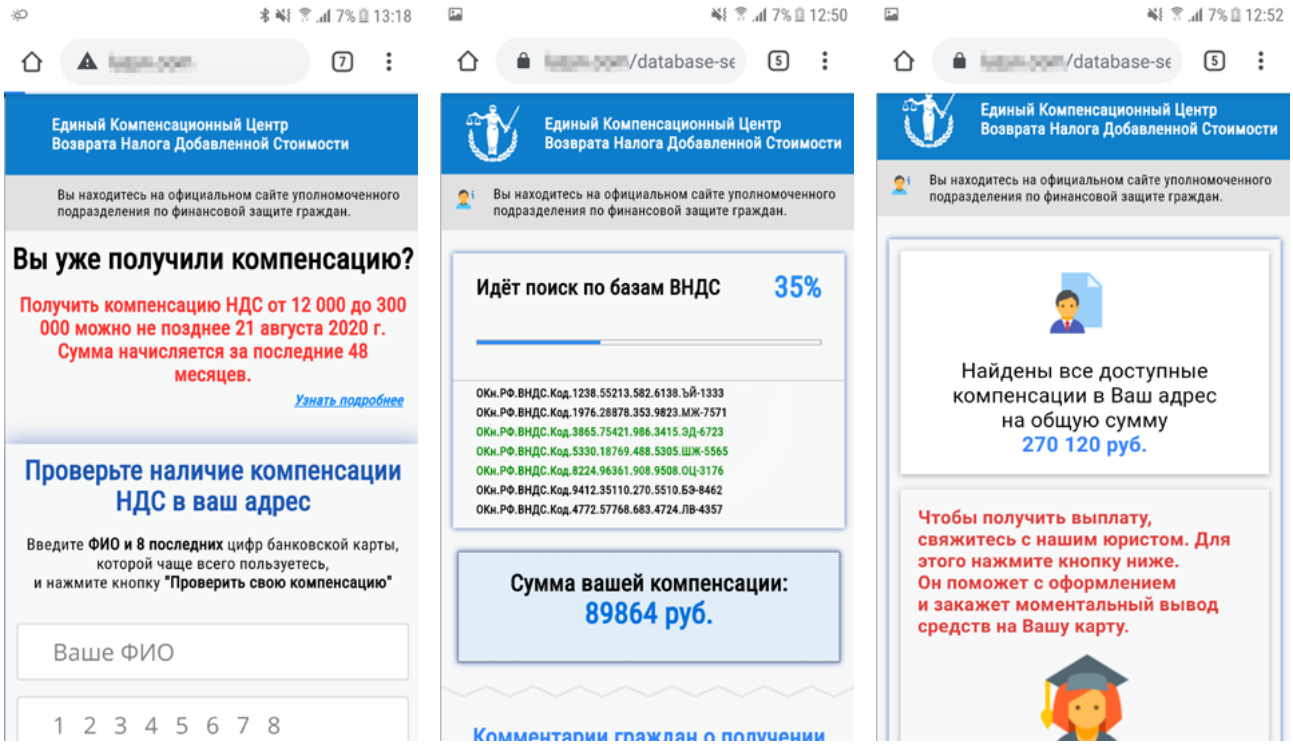




При запуске эти трояны загружают мошеннический сайт несуществующей организации «Единый Компенсационный Центр Возврата Налога Добавленной Стоимости», где потенциальным жертвам предлагается указать персональные данные якобы для проверки доступности той или иной денежной компенсации. После ввода информации

Угрозы в Google Play

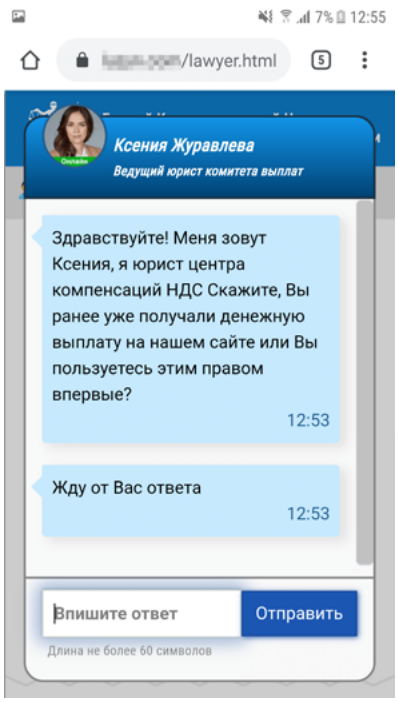
на сайте имитируется процесс поиска, и пользователи видят ложное сообщение об успешно найденных для них вариантах возврата денег.

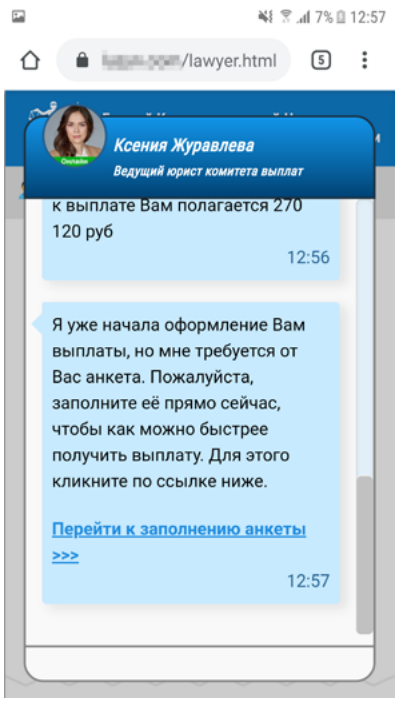


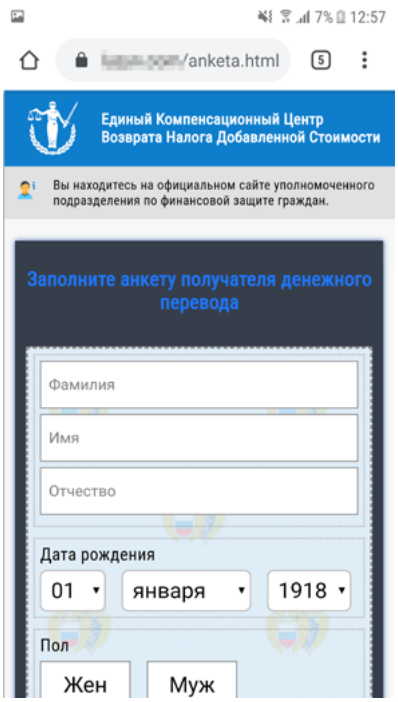
Затем чат-бот сайта имитирует диалог со специалистом. Он предлагает заполнить мнимую анкету, указав в веб-форме дополнительную конфиденциальную информацию, а также оплатить пошлину или комиссию за оформление документов и денежный перевод.

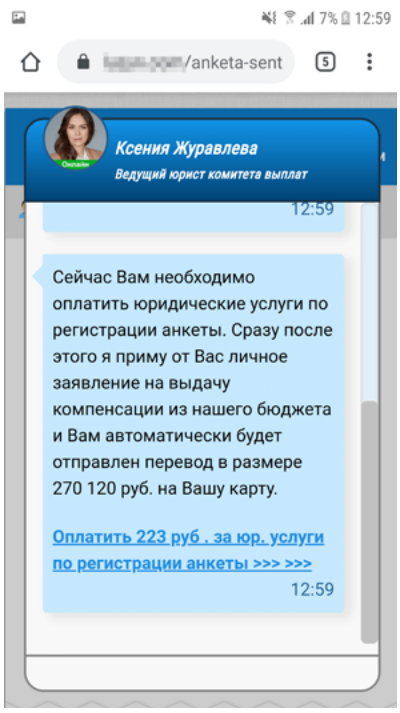
«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2020 года

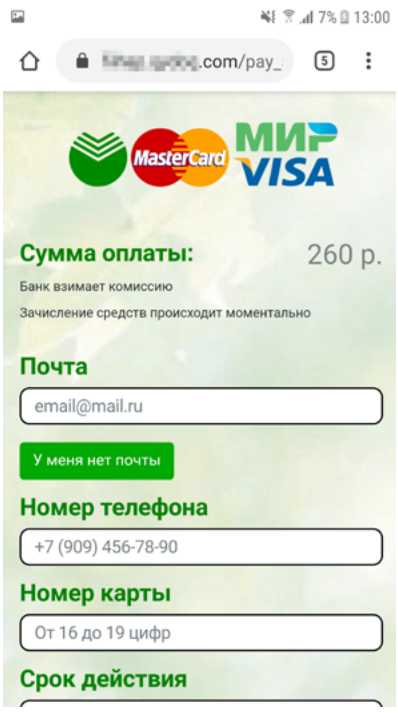
Угрозы в Google Play







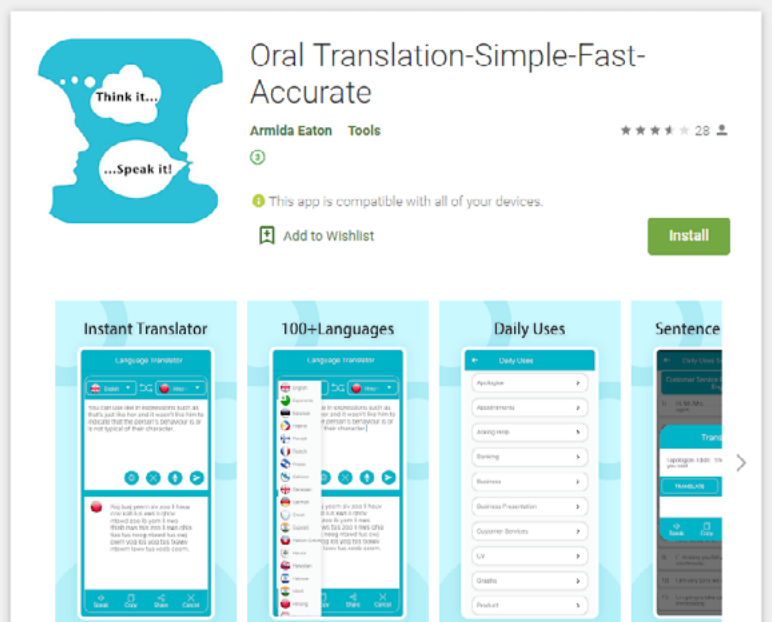




Угрозы в Google Play

В результате такого мошенничества обманутые пользователи не только передают злоумышленникам личные данные, но и добровольно переводят им собственные деньги, не получая при этом никаких обещанных выплат.

Другой угрозой, найденной в Google Play, стал очередной представитель семейства опасных троянов Android.Joker, получивший имя Android.Joker.304. Он распространялся под видом приложения-переводчика. Как и другие трояны этого семейства, Android.Joker.304 мог подписывать пользователей на дорогостоящие мобильные услуги, а также загружать и выполнять произвольный код.



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 августе 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