Dr.WEB®
с 1992 года

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

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

28 декабря 2020 года

По сравнению с ноябрем в декабре антивирусные продукты Dr.Web для Android выявили на защищаемых устройствах на 25,34% меньше угроз. Согласно полученной статистике, количество обнаруженных вредоносных программ сократилось на 25,35%, нежелательных — на 21%, потенциально опасных — на 68,1%, а рекламных — на 25,01%. Чаще всего пользователи Android-устройств сталкивались с рекламными троянами, вредоносными приложениями, способными выполнять произвольный код, а также различными троянами-загрузчиками.

В середине месяца вирусные аналитики копании «Доктор Веб» обнаружили в каталоге Google Play многофункционального трояна Android.Joker.477, который распространялся под видом программы с коллекцией изображений. Кроме того, были зафиксированы очередные атаки с использованием банковских троянов, в частности — Android.BankBot.684.origin и Android.BankBot.687.origin. В ряде случаев злоумышленники выдавали их за программы, позволяющие получить финансовую.

ГЛАВНЫЕ ТЕНДЕНЦИИ ДЕКАБРЯ

- Снижение общего числа угроз, обнаруженных на Android-устройствах
- Рекламные трояны и вредоносные программы-загрузчики остаются одними из самых активных Android-угроз
- Киберпреступники продолжают активно эксплуатировать тему пандемии при проведении атак

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

По данным антивирусных продуктов Dr.Web для Android

Android.RemoteCode.284.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.
Android.HiddenAds.1994
Android.HiddenAds.518.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.

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

По данным антивирусных продуктов Dr.Web для Android

Program.FreeAndroidSpy.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.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

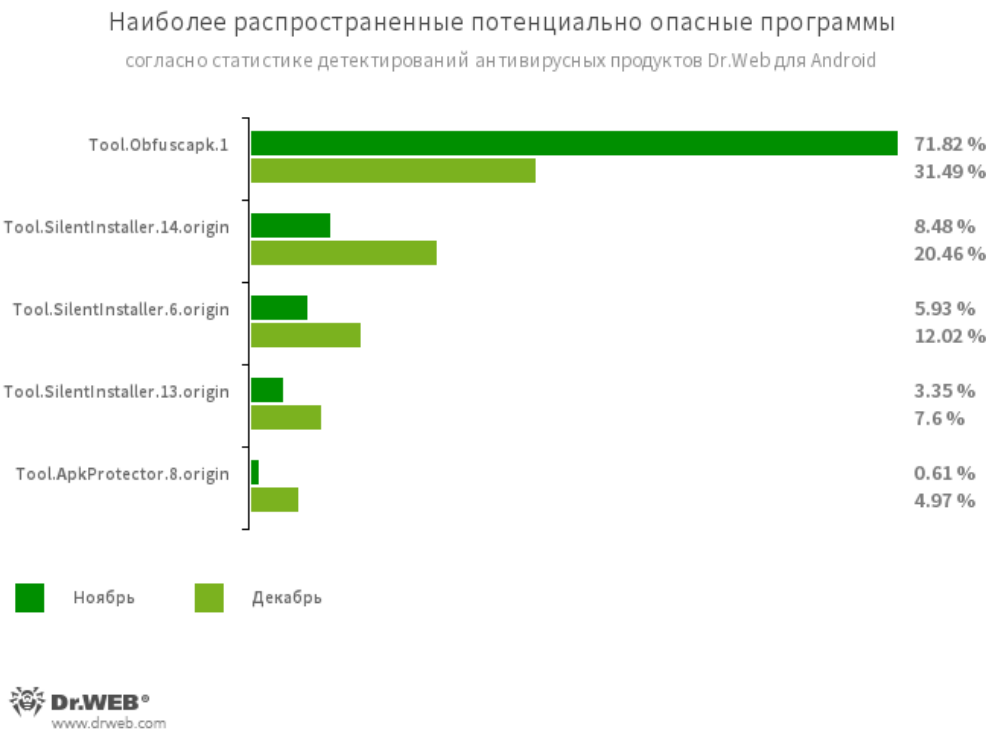
Детектирование программ, предназначенных для присвоения кредитного рейтинга на основании персональных данных пользователей. Такие приложения загружают на удаленный сервер СМС-сообщения, информацию о контактах из телефонной книги, историю вызовов, а также другие сведения.

Program.KeyLogger.2.origin

Android-программа, позволяющая отслеживать вводимые на клавиатуре символы. Она не является вредоносной, но может использоваться для кражи конфиденциальной информации.

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

По данным антивирусных продуктов Dr.Web для Android



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.

Tool.SilentInstaller.14.origin
Tool.SilentInstaller.6.origin
Tool.SilentInstaller.13.origin
Tool.SilentInstaller.8.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.

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

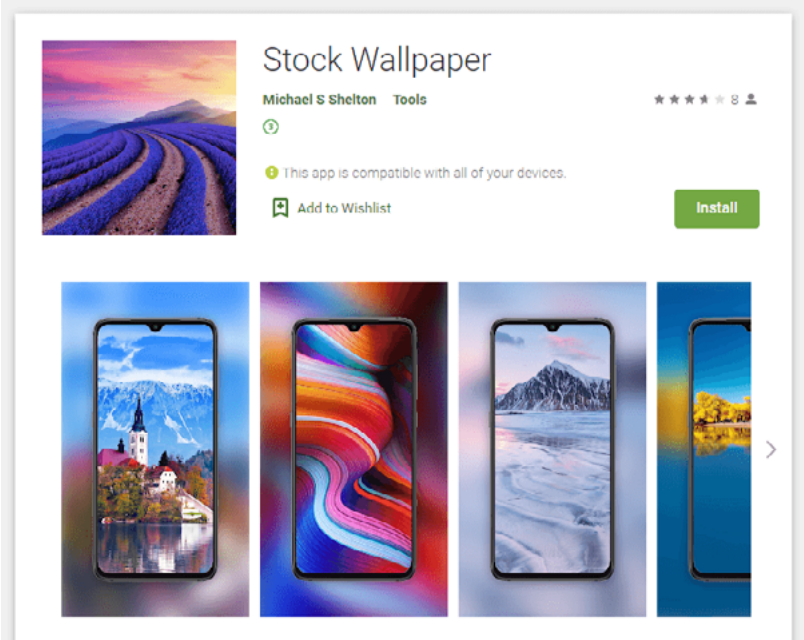
По данным антивирусных продуктов Dr.Web для Android

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.SspSdk.1.origin
- Adware.Adpush.36.origin
- Adware.Adpush.6547
- Adware.Myteam.2.origin
- Adware.Overlay.1.origin

Угрозы в Google Play

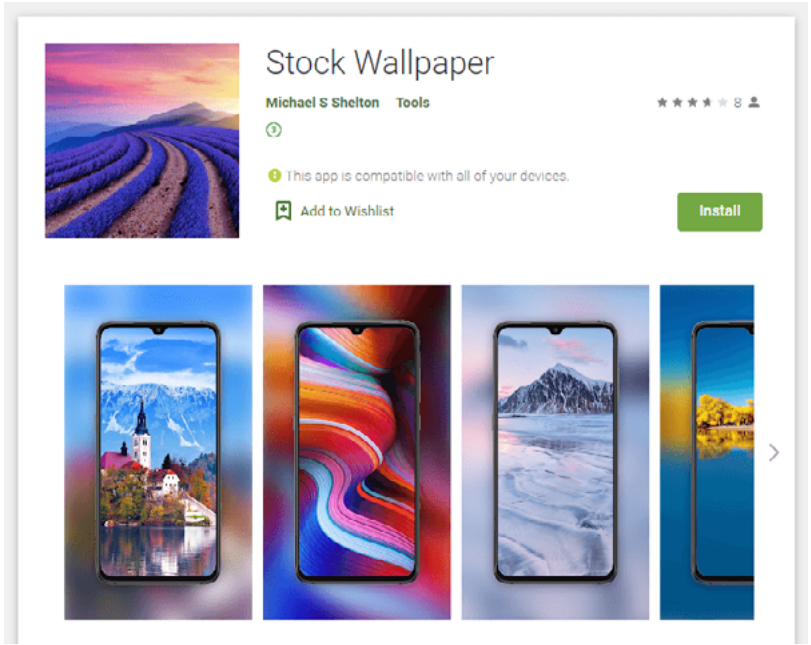
В декабре вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play очередного трояна. Это был представитель семейства Android.Joker, получивший имя Android.Joker.477. Троян распространялся под видом сборника изображений, но в действительности предназначался для подписки пользователей на платные услуги, а также загрузки и выполнения произвольного кода.



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

Банковские трояны

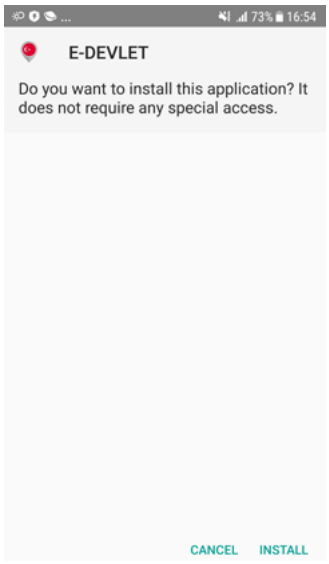
Среди троянских программ, угрожавших пользователям в прошедшем месяце, были банкеры Android.BankBot.684.origin и Android.BankBot.687.origin. Новые модификации этих вредоносных приложений, обнаруженные нашими специалистами, атаковали жителей Турции. Трояны распространялись через мошеннические сайты, на которых потенциальным жертвам предлагалось получить материальную помощь от государства в связи с пандемией. Для этого пользователи должны были загрузить и установить специализированное ПО, которое на самом деле являлось вредоносным.

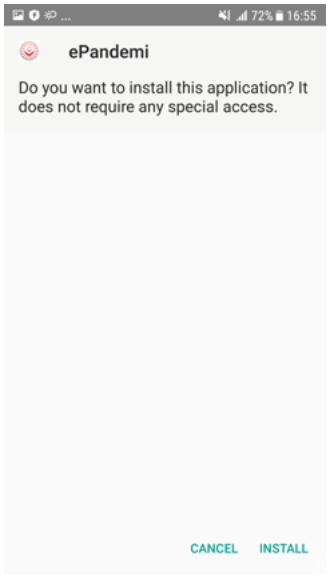


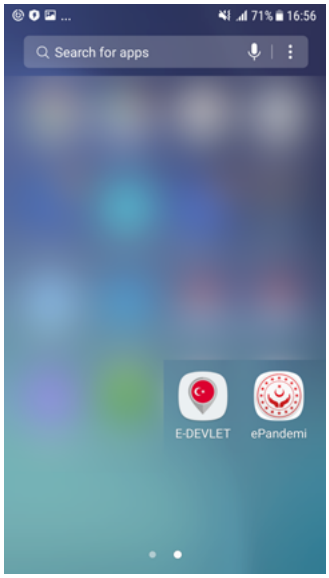
«Доктор Веб»: обзор вирусной активности для мобильных устройств в декабре 2020 года

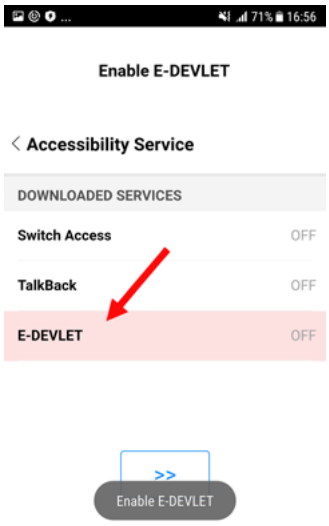
Банковские трояны

Попадая на Android-устройства, банкеры запрашивали доступ к специальным возможностям (Accessibility Service) ОС Android для расширения своих полномочий, скрывали свои значки из списка установленных приложений на главном экране и приступали к выполнению основных функций. Они похищали конфиденциальную информацию, демонстрируя фишинговые окна поверх окон других приложений, перехватывали СМС, могли блокировать экран, а также выполняли другие вредоносные действия.









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 декабре 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