Dr.WEB®
с 1992 года

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

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

24 февраля 2021 года

В январе антивирусные продукты Dr.Web для Android зафиксировали на защищаемых устройствах на 11,32% меньше угроз по сравнению с декабрем прошлого года. Число обнаруженных вредоносных приложений снизилось на 11,5%, а рекламных — на 15,93%. При этом количество выявленных нежелательных и потенциально опасных программ возросло на 11,66% и 7,26% соответственно. Согласно полученной статистике, наиболее часто пользователи сталкивались с троянами, демонстрировавшими рекламу, а также с вредоносными приложениями, которые загружали другое ПО и выполняли произвольный код.

В течение предыдущего месяца вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play множество угроз. Среди них — многочисленные модификации рекламных модулей семейства Adware.NewDich, которые распространялись в составе программ для ОС Android. Кроме того, были выявлены новые трояны семейства Android.FakeApp, загружавшие мошеннические сайты, а также вредоносные приложения семейства Android.Joker, подписывавшие пользователей на дорогостоящие мобильные услуги и выполнявшие произвольный код.

Вместе с тем наши специалисты зафиксировали очередные атаки с применением банковских троянов. Один из них был найден в поддельном банковском приложении, размещенном в Google Play, другие распространялись через вредоносные сайты, созданные злоумышленниками.

ГЛАВНЫЕ ТЕНДЕНЦИИ ЯНВАРЯ

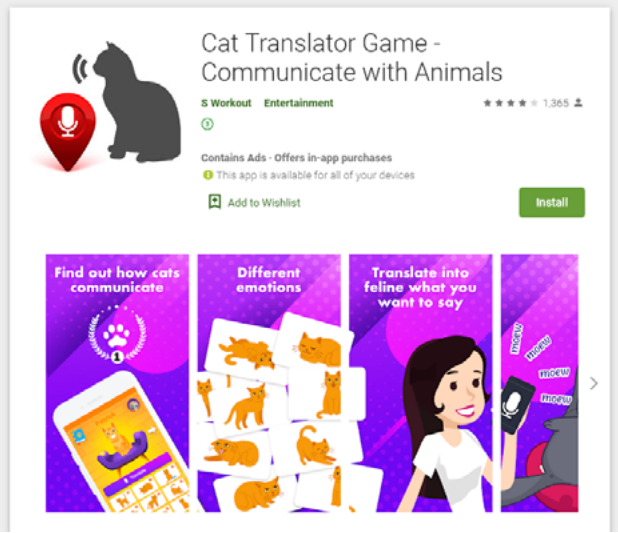
- Снижение общего числа угроз, зафиксированных на Android-устройствах
- Обнаружение множества новых вредоносных и нежелательных программ в каталоге Google Play

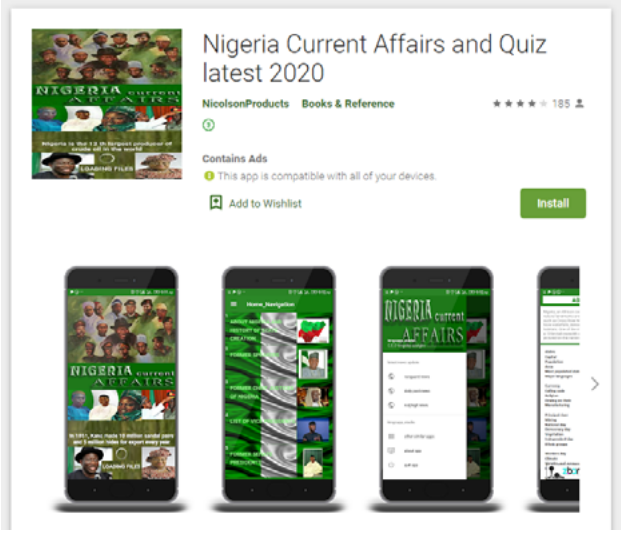
«Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2021 года

Угроза месяца

В начале января вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play приложения со встроенными в них рекламными модулями семейства Adware.NewDich, которые по команде управляющего сервера загружают в браузере различные веб-сайты. Это могут быть как безобидные интернет-ресурсы, так и сайты с рекламой или мошеннические сайты, используемые для фишинга. Их загрузка происходит, когда пользователи не работают с приложениями, содержащими Adware.NewDich. Из-за этого становится сложнее определить причину странного поведения Android-устройств.

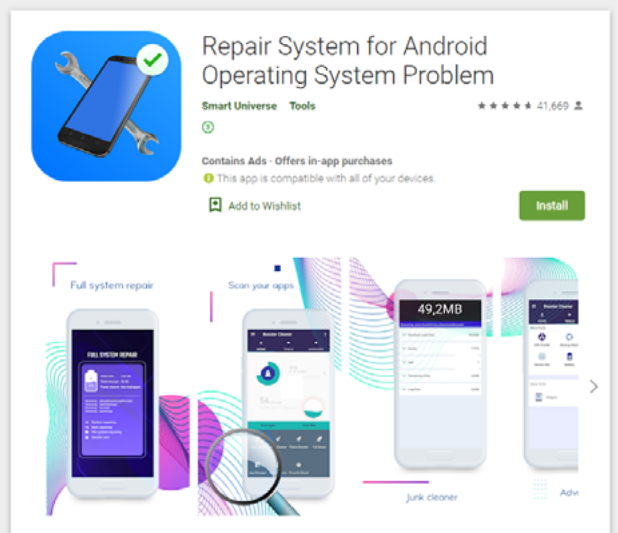
Примеры приложений, в которых были найдены такие рекламные модули:



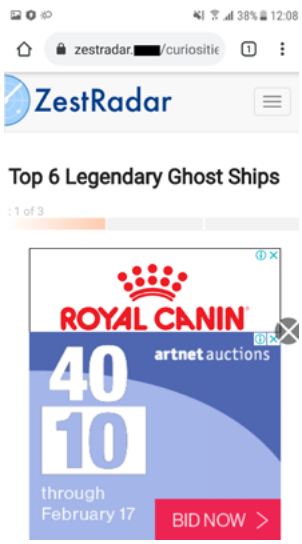


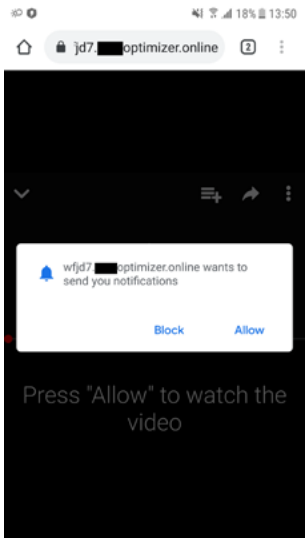
«Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2021 года

Угроза месяца



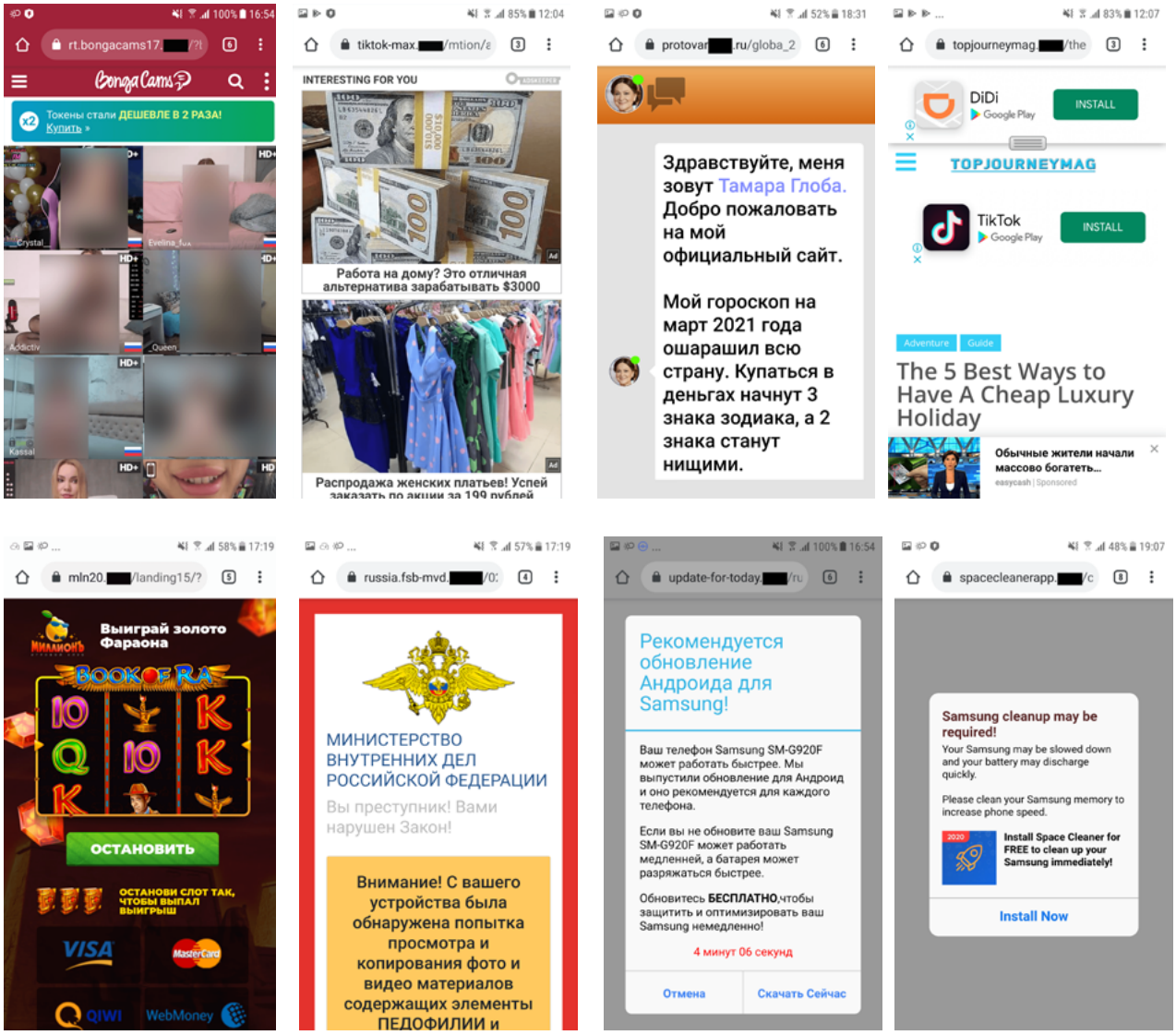
Примеры загружаемых ими сайтов:





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

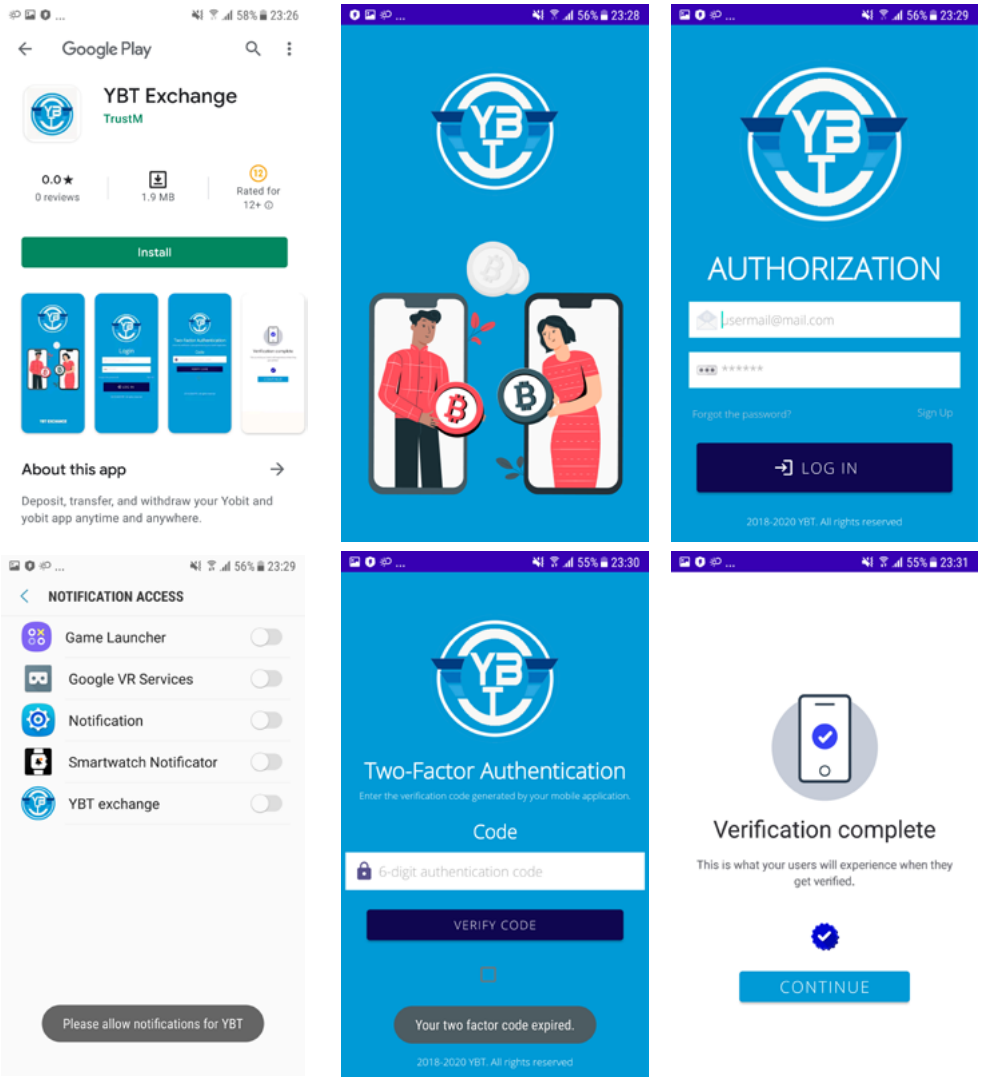
Угроза месяца



Среди разнообразия веб-ресурсов, загружаемых модулями Adware.NewDich, часто встречаются страницы партнерских и рекламных сервисов, которые перенаправляют пользователей на разделы размещенных в Google Play программ. Одной из них было приложение под названием YBT Exchange, якобы предназначенное для работы с одной из криптобирж. Однако вирусные аналитики компании «Доктор Веб» выяснили, что это не что иное как банковский троян — он получил имя Android.Banker.3684. В его функции входил перехват вводимых логинов, паролей, одноразовых проверочных кодов, а также содержимого поступающих уведомлений, для чего троян запрашивал соответствующее системное разрешение. После нашего обращения в корпорацию Google банкер был удален из каталога.

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

Угроза месяца



Вирусные аналитики «Доктор Веб» выяснили, что различные модификации этих модулей присутствовали как минимум в 21 программе. Исследование показало, что с большой долей вероятности их владельцы непосредственно связаны и с разработкой Adware.NewDich. После того как рекламная платформа привлекла внимание специалистов по информационной безопасности, ее администраторы запаниковали и начали выпускать обновления приложений, в которых старались «сбить» детектирование антивирусов или полностью исключали из них рекламный модуль. Одна из затронутых программ в дальнейшем была удалена из каталога. Вместе с тем ничто не мешает злоумышленникам выпускать новые версии ПО, в которых Adware.NewDich будет присутствовать вновь, что уже несколько раз наблюдали наши специалисты.

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

Угроза месяца

Список программ с обнаруженными в них модулями Adware.NewDich:

Имя пакета	Наличие модуля Adware.NewDich	Приложение удалено из Google Play
com.qrcodescanner.barcodescanner	Присутствовал в последней актуальной версии 1.75	Да
com.speak.better.correctspelling	Присутствует в актуальной версии 679.0	Нет
com.correct.spelling.learn.english	Присутствует в актуальной версии 50.0	Нет
com.bluetooth.autoconnect.anybtdevices	Присутствует в актуальной версии 2.5	Нет
com.bluetooth.share.app	Присутствует в актуальной версии 1.8	Нет
org.strong.booster.cleaner.fixer	Отсутствует в актуальной версии 5.9	Нет
com.smartwatch.bluetooth.sync.notifications	Отсутствует в актуальной версии 85.0	Нет
com.blogspot.bidatop.nigeriacurrentaffairs2018	Присутствует в актуальной версии 3.2	Нет
com.theantivirus.cleanerandbooster	Отсутствует в актуальной версии 9.3	Нет
com.clean.booster.optimizer	Отсутствует в актуальной версии 9.1	Нет
flashlight.free.light.bright.torch	Отсутствует в актуальной версии 66.0	Нет
com.meow.animal.translator	Отсутствует в актуальной версии 1.9	Нет
com.gogamegone.superfileexplorer	Отсутствует в актуальной версии 2.0	Нет
com.super.battery.full.alarm	Отсутствует в актуальной версии 2.2	Нет
com.apps.best.notepad.writing	Отсутствует в актуальной версии 7.7	Нет
ksmart.watch.connecting	Отсутствует в актуальной версии 32.0	Нет
com.average.heart.rate	Отсутствует в актуальной версии 7.0	Нет
com.apps.best.alam.clocks	Отсутствует в актуальной версии 4.7	Нет
com.booster.game.accelerator.top	Отсутствует в актуальной версии 2.1	Нет
org.booster.accelerator.optimizer.colorful	Отсутствует в актуальной версии 61.0	Нет
com.color.game.booster	Отсутствует в актуальной версии 2.1	Нет

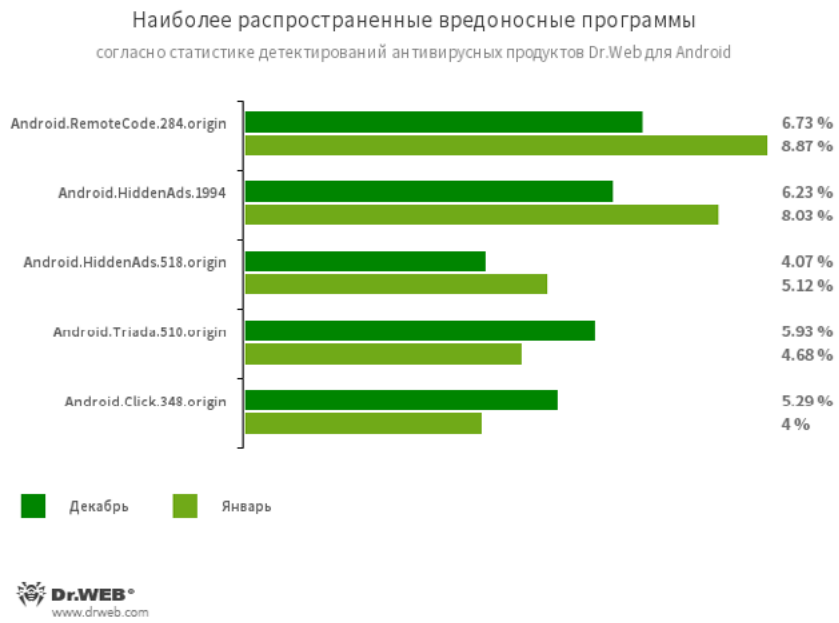
Угроза месяца

Особенности модулей Adware.NewDich:

- встроены в полнофункциональные приложения, чтобы не вызывать подозрений у пользователей;
- их активность проявляется с некоторой задержкой (до нескольких дней) после запуска содержащих их программ;
- загрузка рекламируемых сайтов выполняется, когда приложения, в которые встроены модули, закрыты, и пользователи не работают с ними;
- злоумышленники постоянно контролируют, обнаруживают ли антивирусы данные модули, оперативно вносят в них изменения и выпускают обновленные версии, чтобы противостоять детектированию.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2021 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.HiddenAds.1994

Android.HiddenAds.518.origin

Трояны, предназначенные для показа навязчивой рекламы. Распространяются под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают их в системный каталог.

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.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 январе 2021 года

По данным антивирусных продуктов Dr.Web для Android

Program.FreeAndroidSpy.1.origin

Program.NeoSpy.1.origin

Program.Mrecorder.1.origin

Program.Reptilicus.7.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.

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

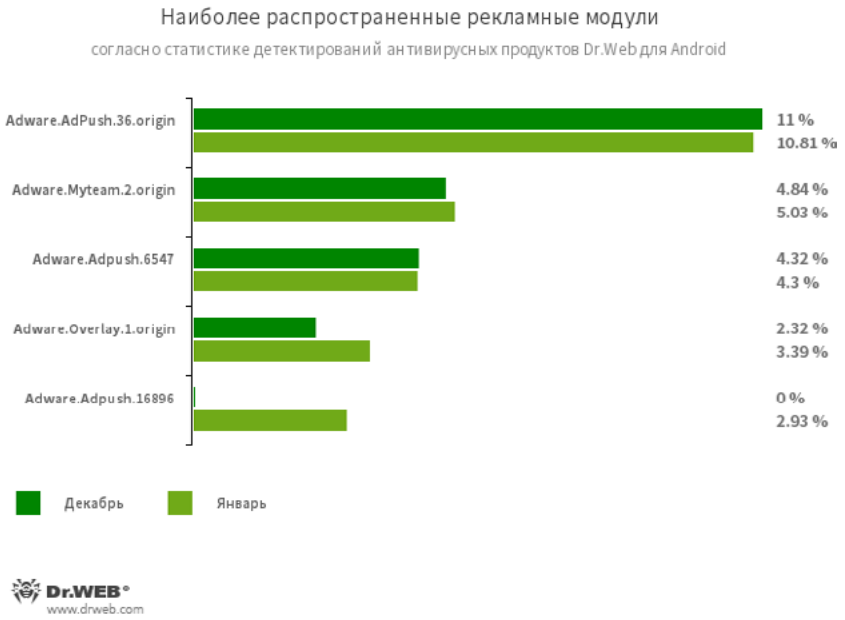
Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

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 январе 2021 года

По данным антивирусных продуктов Dr.Web для Android

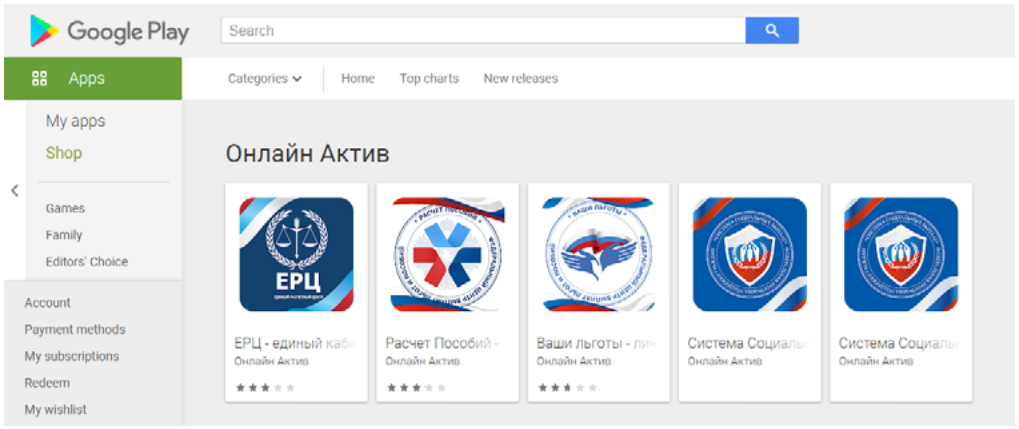


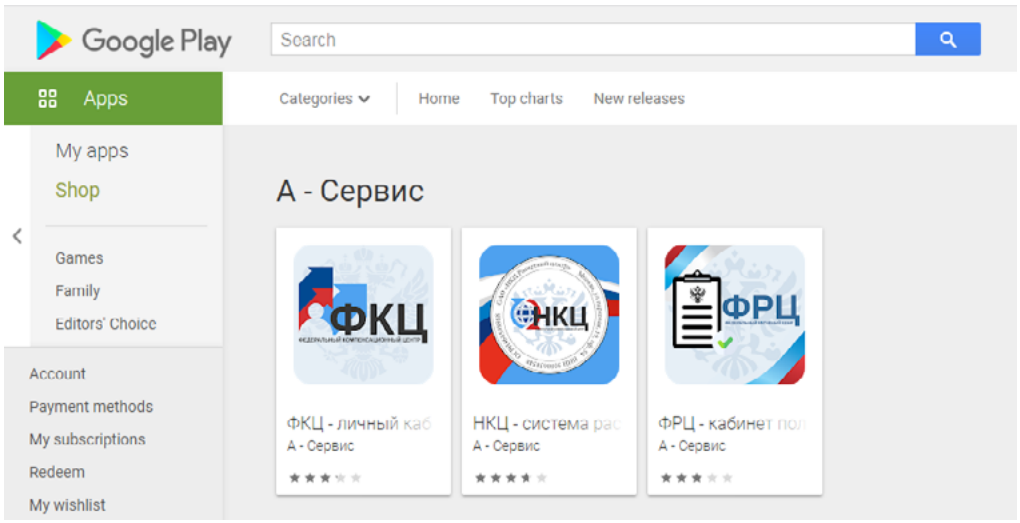
Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать ярлыки и загружать веб-сайты.

- Adware.Adpush.36.origin
- Adware.Adpush.6547
- Adware.Adpush.16896
- Adware.Myteam.2.origin
- Adware.Overlay.1.origin

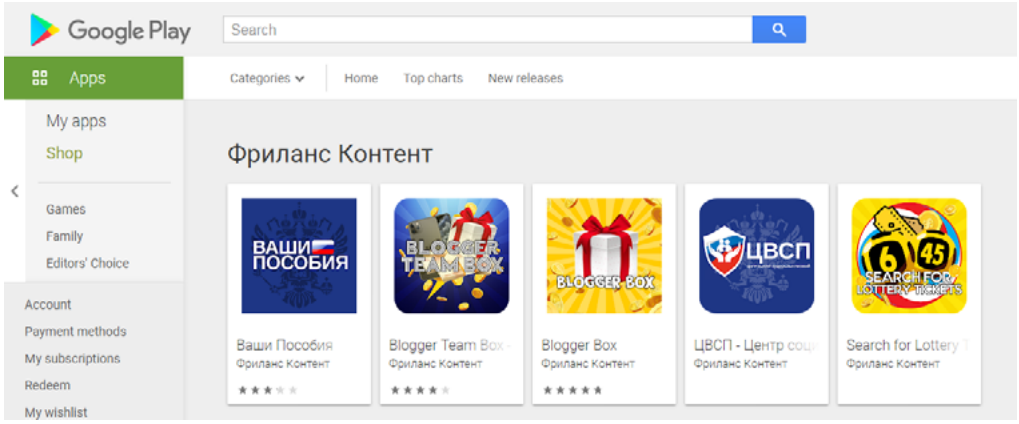
Угрозы в Google Play

Помимо приложений с рекламными модулями Adware.NewDich в январе специалисты «Доктор Веб» выявили в каталоге Google Play множество новых троянов семейства Android.FakeApp, которые распространялись под видом ПО с информацией о социальных выплатах, льготах, возврате НДС и других денежных компенсациях. При этом среди них встречались и другие модификации — например, выдаваемые за программы для поиска информации о лотереях и получения подарков от популярных блогеров.





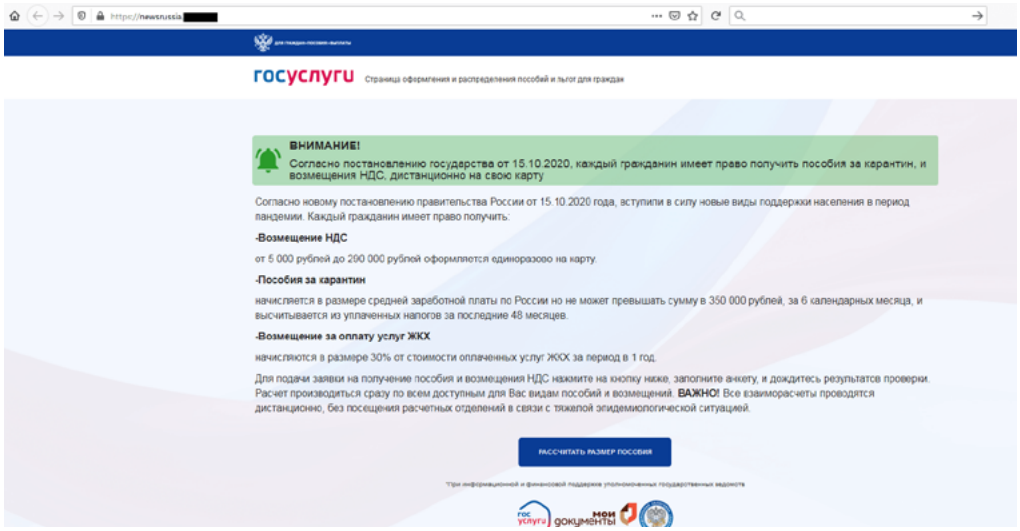
Угрозы в Google Play



Как и другие аналогичные трояны, обнаруженные ранее, последние версии загружали мошеннические сайты, где потенциальным жертвам сообщалось о якобы доступных для них выплатах от государства. Для «получения» денег им предлагалось указать персональную информацию, а также оплатить работу юристов, оформление документов, госпошлину или комиссию за перевод на банковский счет. На самом деле никаких средств пользователи не получали, и злоумышленники похищали у них конфиденциальные данные и деньги.

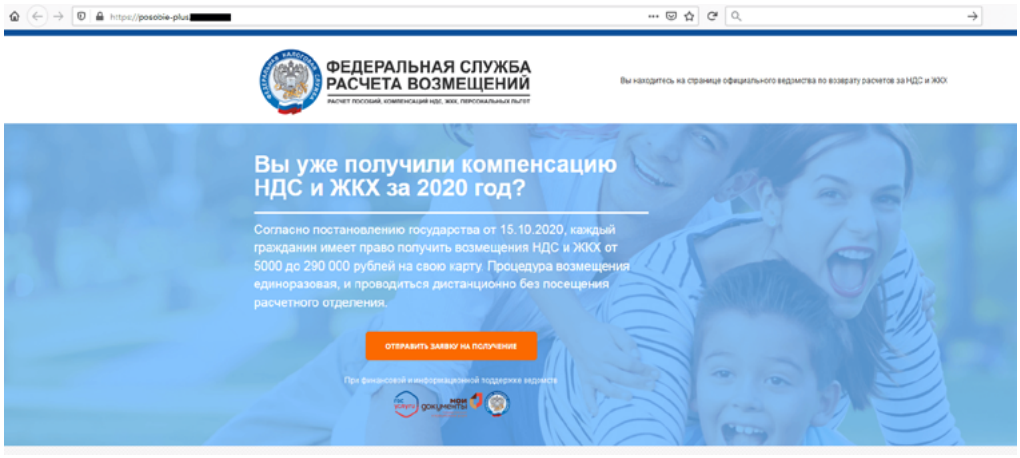
Некоторые модификации этих вредоносных приложений периодически демонстрировали уведомления, в которых также сообщалось о доступных выплатах и компенсациях. Таким образом киберпреступники пытались привлечь дополнительное внимание потенциальных жертв, чтобы те чаще переходили на мошеннические сайты.

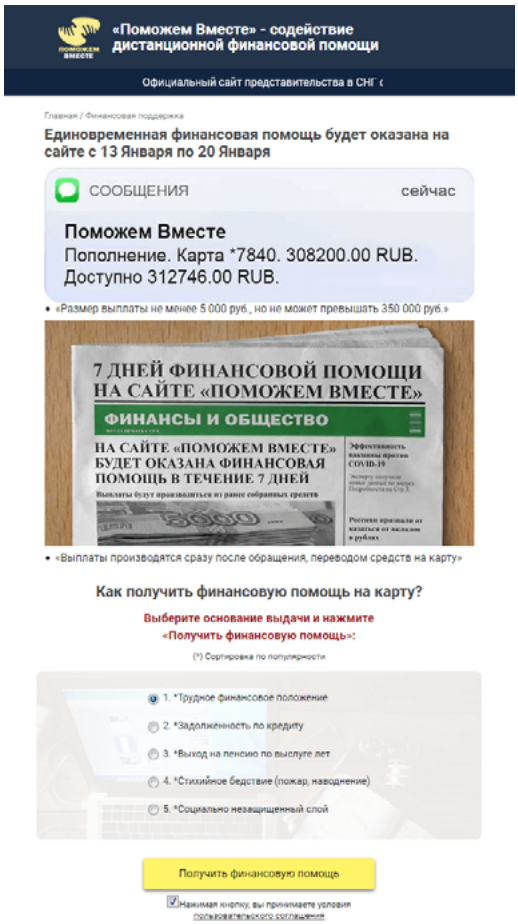
Примеры сайтов, загружаемых различными модификациями троянов Android.FakeApp:



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

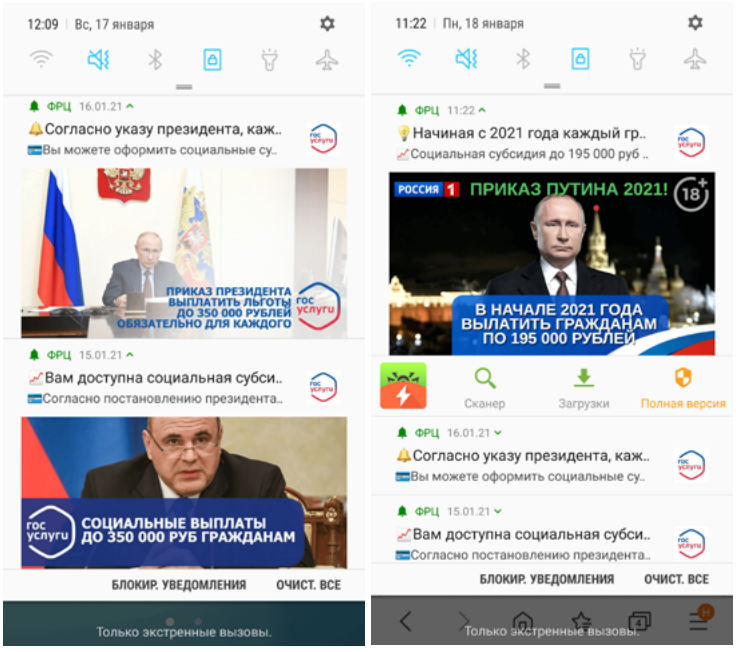
Угрозы в Google Play

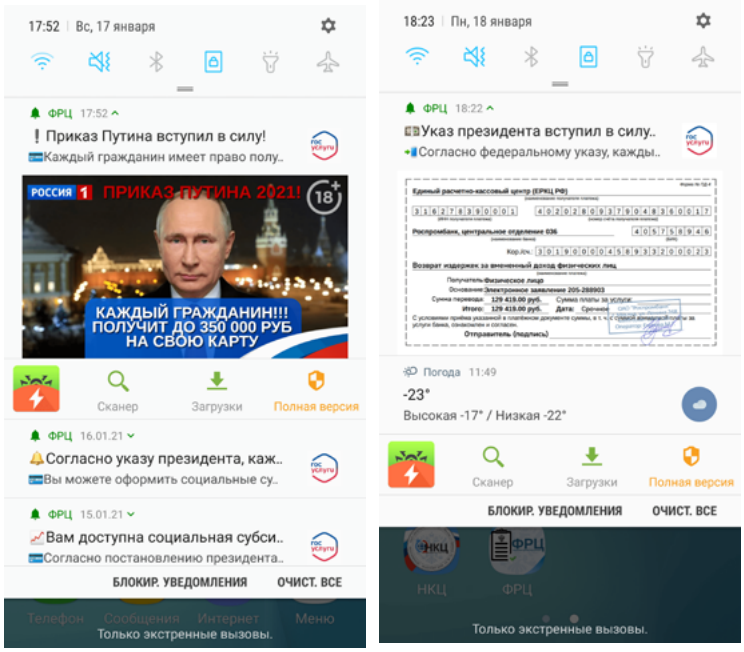




Угрозы в Google Play

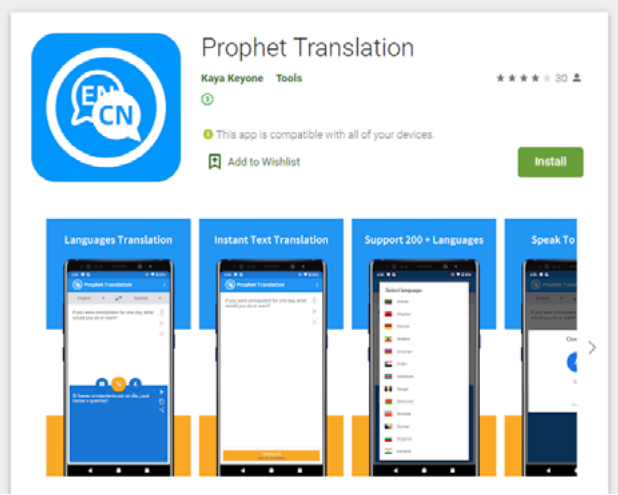
Примеры мошеннических уведомлений с информацией о «выплатах» и «компенсациях», которые демонстрируют эти вредоносные приложения:

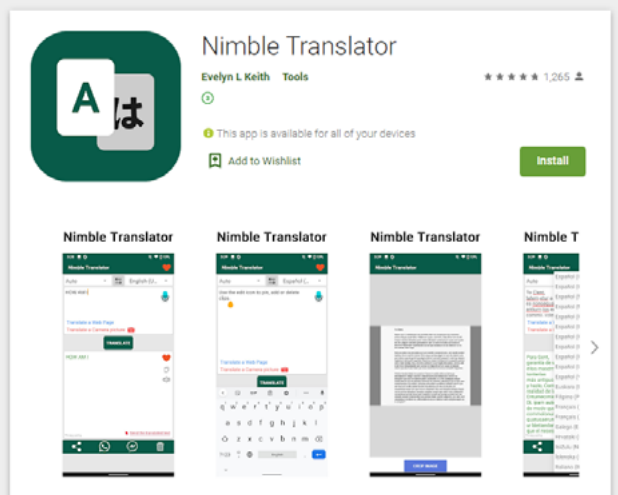




Угрозы в Google Play

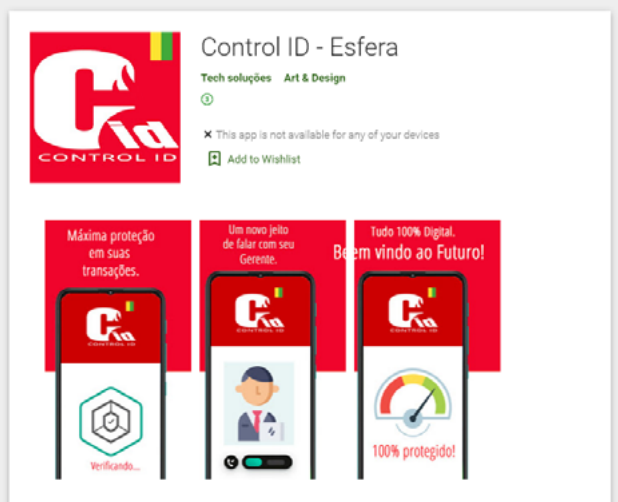
Кроме того, были обнаружены очередные многофункциональные трояны, принадлежащие к семейству Android.Joker и получившие имена Android.Joker.496, Android.Joker.534 и Android.Joker.535. Они распространялись под видом безобидных приложений — программ-переводчиков и мультимедийного редактора для создания gif-анимации. Однако настоящими их функциями были загрузка и выполнение произвольного кода, а также перехват содержимого уведомлений и подписка пользователей на премиум-услуги.



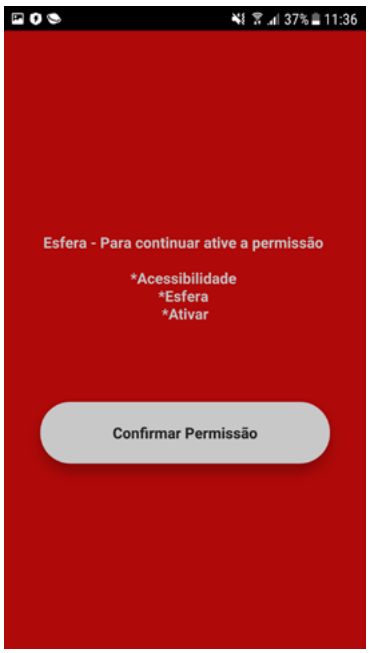


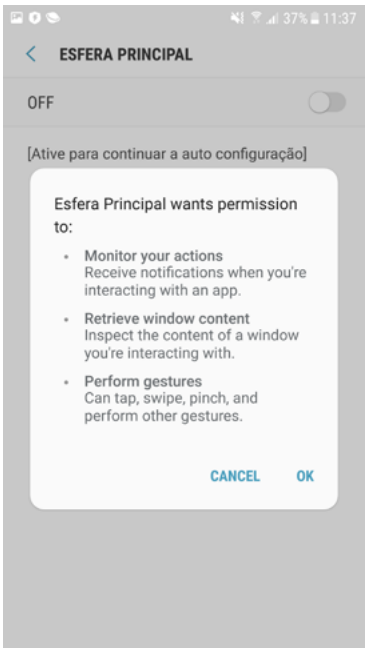
Среди выявленных угроз оказался и новый троян, добавленный в вирусную базу Dr.Web как Android.Banker.3679. Он распространялся под видом приложения для работы с бонусной программой Esfera банка Santander и предназначался для бразильских пользователей. Основными функциями Android.Banker.3679 являлись фишинг и кража конфиденциальных данных, а его целью было банковское приложение Santander Empresas.

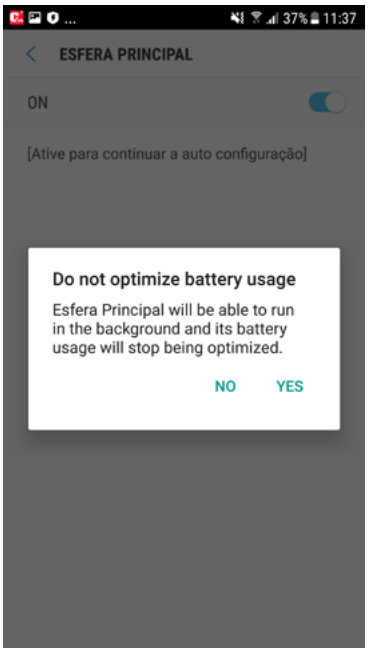
Угрозы в Google Play



После установки и запуска троян запрашивал доступ к специальным возможностям ОС Android — якобы для продолжения работы с приложением. На самом деле они были нужны ему для автоматического выполнения вредоносных действий. Если жертва соглашалась предоставить ему необходимые полномочия, банкер получал контроль над устройством и мог самостоятельно нажимать на различные элементы меню, кнопки, считывать содержимое окон приложений и т. д.

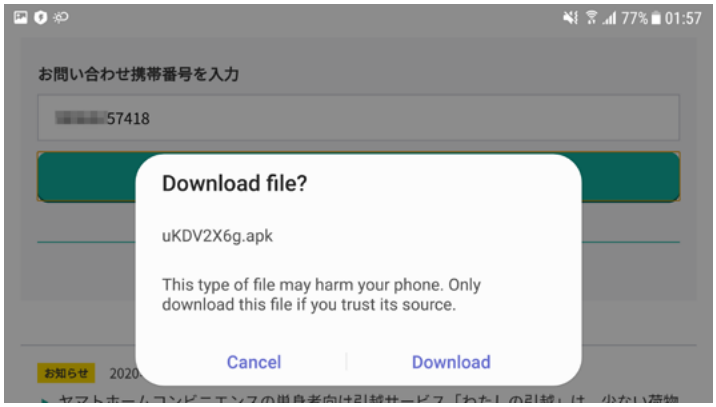






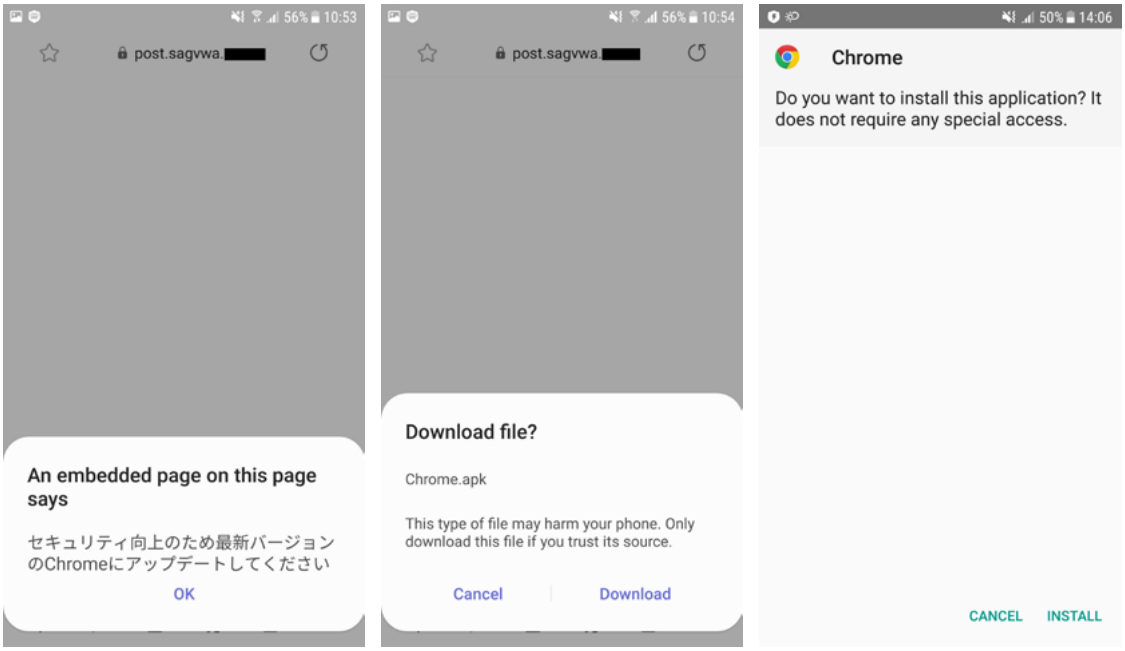
Банковские трояны

Наряду с банковскими троянами, выявленными в Google Play, владельцам Android-устройств угрожали банкеры, которые распространялись через вредоносные сайты. Например, специалисты компании «Доктор Веб» зафиксировали очередные атаки на японских пользователей, где применялись вредоносные приложения из различных семейств — Android.BankBot.3954, Android.SmsSpy.833.origin, Android.SmsSpy.10809, Android.Spy.679.origin и другие. Они загружались с поддельных сайтов курьерских и почтовых служб под видом обновлений браузера Chrome, программы Play Маркет и прочего безобидного ПО.



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

Банковские трояны



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 январе 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