Dr.WEB®
с 1992 года

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

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

16 марта 2021 года

В феврале антивирусные продукты Dr.Web для Android чаще всего обнаруживали на защищаемых устройствах вредоносные и нежелательные программы, демонстрирующие надоедливую рекламу, а также трояны, выполняющие произвольный код и загружающие различные приложения без ведома пользователей.

В течение прошлого месяца вирусные аналитики компании «Доктор Веб» вновь обнаружили в каталоге Google Play множество угроз. Среди них были многочисленные мошеннические приложения, принадлежащие к семейству Android.FakeApp, многофункциональные трояны Android.Joker, вредоносные приложения семейства Android.HiddenAds, демонстрирующие рекламу, а также другие опасные программы.

ГЛАВНЫЕ ТЕНДЕНЦИИ ФЕВРАЛЯ

- Появление очередных угроз в каталоге Google Play
- Активность вредоносных Android-приложений, используемых в различных мошеннических схемах

«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 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
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.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.
Android.MobiDash.5135
Троянская программа, показывающая надоедливую рекламу. Представляет собой программный модуль, который разработчики ПО встраивают в приложения.

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

По данным антивирусных продуктов Dr.Web для Android

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.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

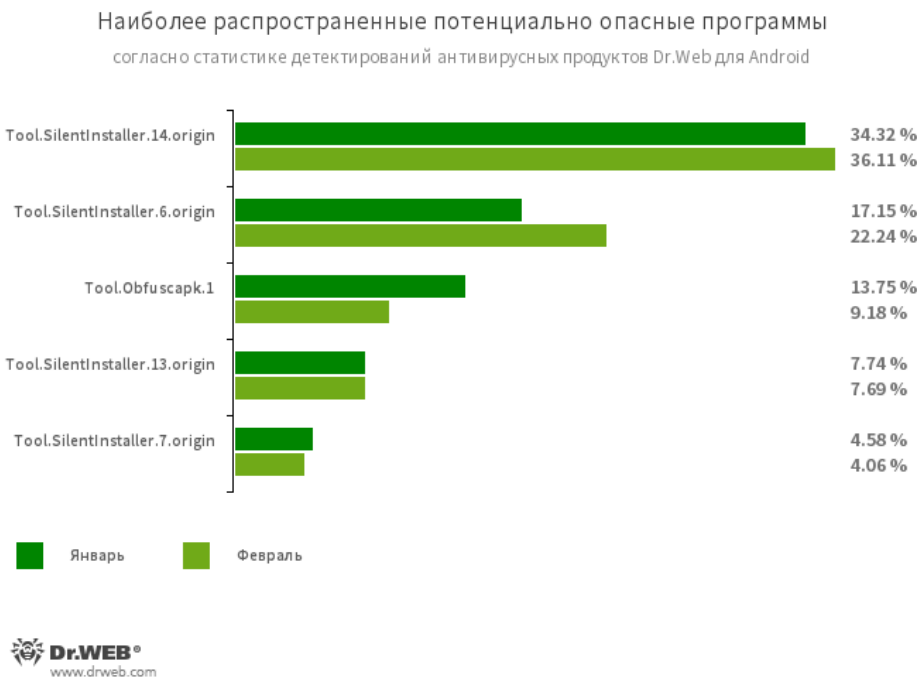
Детектирование программ, предназначенных для присвоения кредитного рейтинга на основании персональных данных пользователей. Такие приложения загружают на удаленный сервер СМС-сообщения, информацию о контактах из телефонной книги, историю вызовов, а также другие сведения.

Program.Gemius.1.origin

Программа, собирающая информацию о мобильных Android-устройствах и о том, как их используют их владельцы. Вместе с техническими данными она собирает конфиденциальные сведения — информацию о местоположении устройства, сохраненных в браузере закладках, истории посещенных сайтов, а также о вводимых интернет-адресах.

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

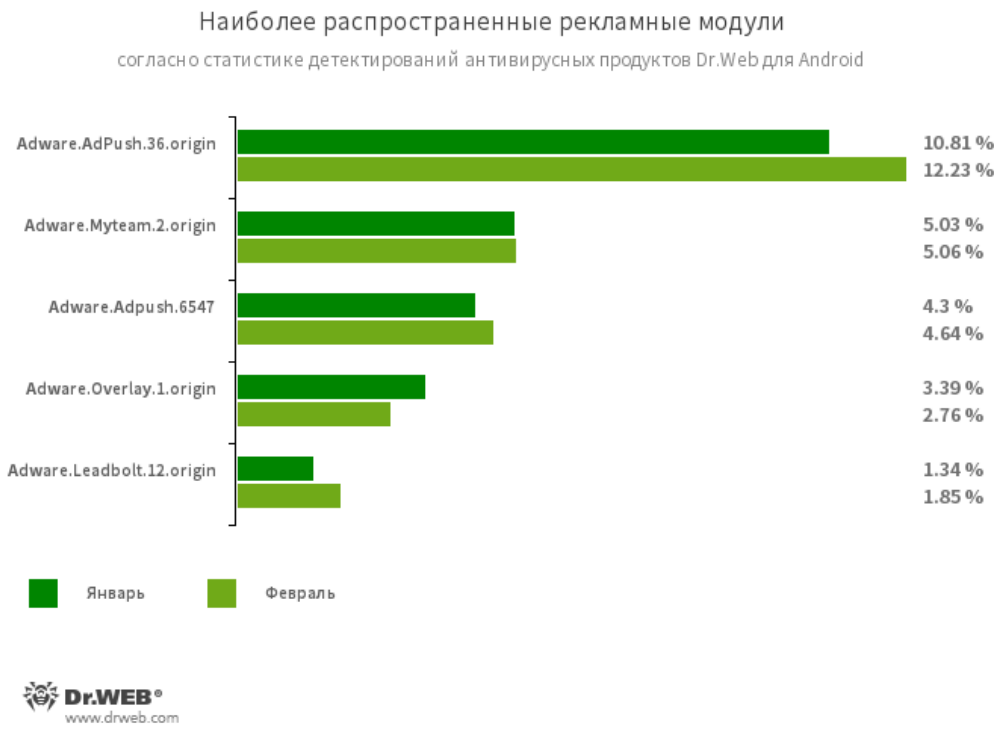
Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

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 феврале 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.Myteam.2.origin

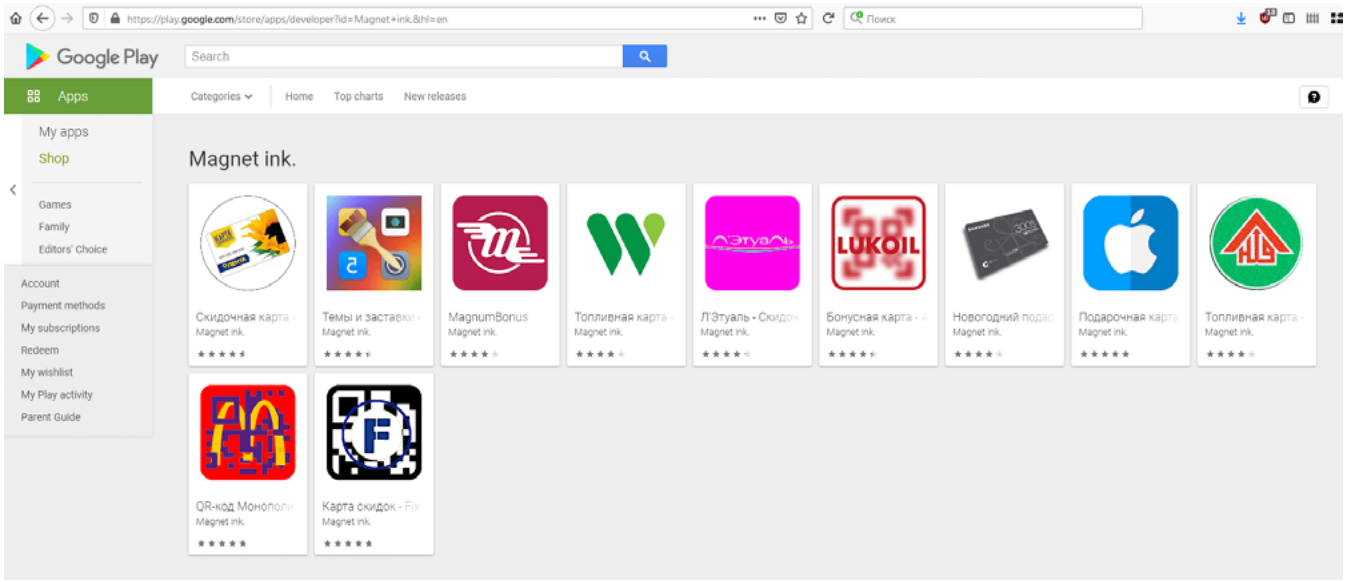
Adware.Overlay.1.origin

Adware.LeadBolt.12.origin

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

Угрозы в Google Play

В течение февраля специалисты компании «Доктор Веб» фиксировали распространение большого числа вредоносных приложений семейства Android.FakeApp, многие их которых злоумышленники применяли в мошеннических схемах. Одна из групп таких троянов распространялась под видом программ, якобы предоставлявших доступ к скидкам, акционным и бонусным картам, а также подаркам от известных магазинов и компаний. Для большей убедительности в программах использовалась символика и названия соответствующих брендов — производителей электроники, АЗС и торговых сетей.



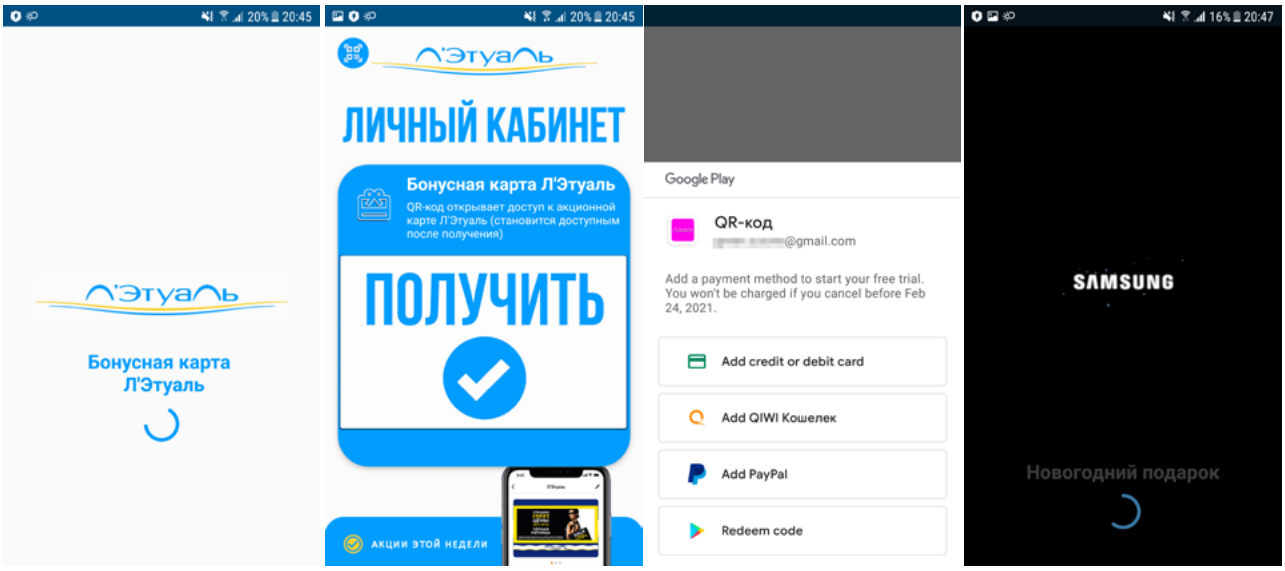
При запуске таких программ потенциальным жертвам предлагалось оформить платную подписку стоимостью от 449 до 1499 рублей в неделю — якобы чтобы воспользоваться всеми функциями приложений и получить обещанные бонусы. Однако в результате они получали лишь бесполезные штрих- или QR-коды, одинаковые для всех троянов, а также обещание новых кодов, которые будут поступать в виде уведомлений. При этом функциональность для работы с уведомлениями была лишь у нескольких модификаций этих программ, что само по себе ставило под сомнение честность их создателей.

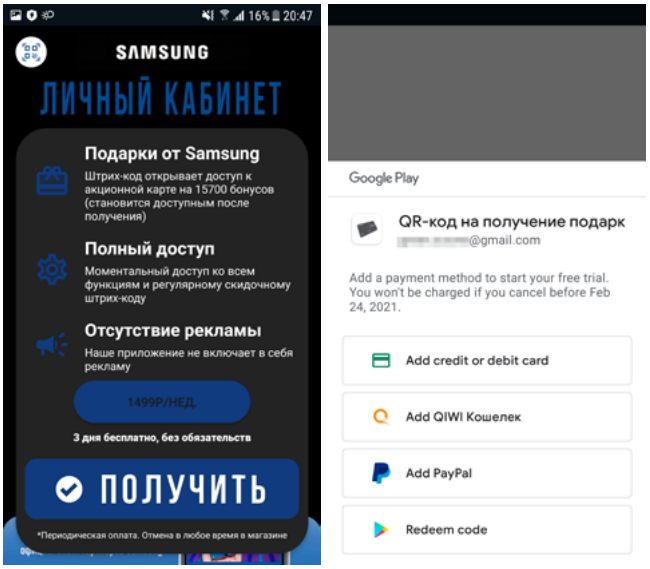
При согласии на оплату услуг внутри этих приложений владельцам Android-устройств предоставлялся пробный период на 3 дня, в течение которого они могли отказаться от платежа или же подтвердить подписку. Расчет злоумышленников в этой схеме заключался в том, что пользователи забудут о тестовом периоде или даже о том, что установили эти программы, либо из-за неопытности не поймут, что подключили дорогостоящую услугу с периодической оплатой.

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

Угрозы в Google Play

Различные модификации указанных троянов были добавлены в вирусную базу Dr.Web как Android.FakeApp.239, Android.FakeApp.240, Android.FakeApp.246 и Android.FakeApp.247. Пример работы нескольких из них показан на изображениях ниже:

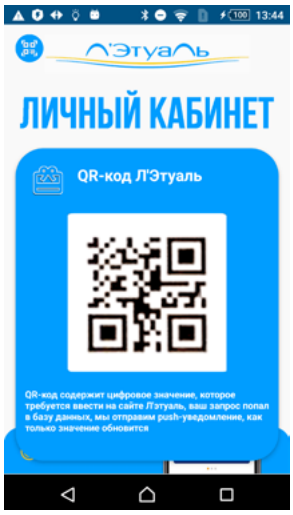


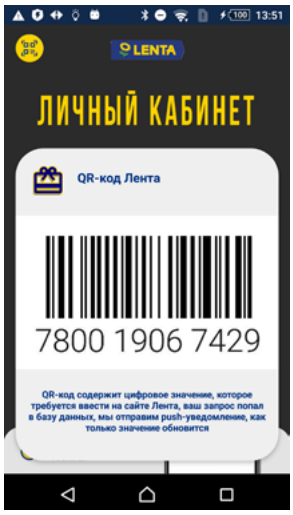


«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2021 года

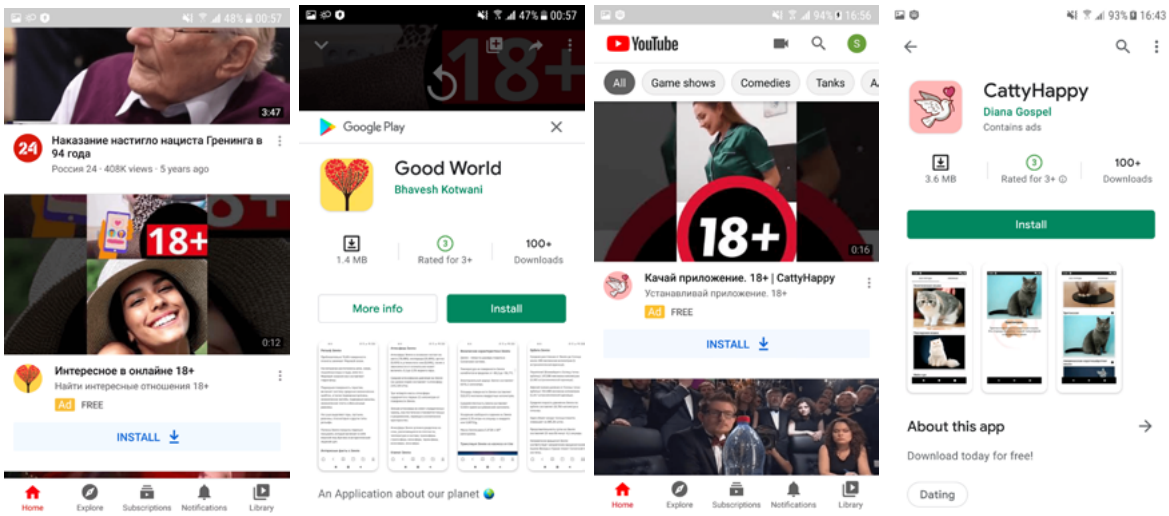
Угрозы в Google Play

Сообщения и примеры кодов, которые трояны демонстрировали после успешной подписки на дорогостоящую услугу:



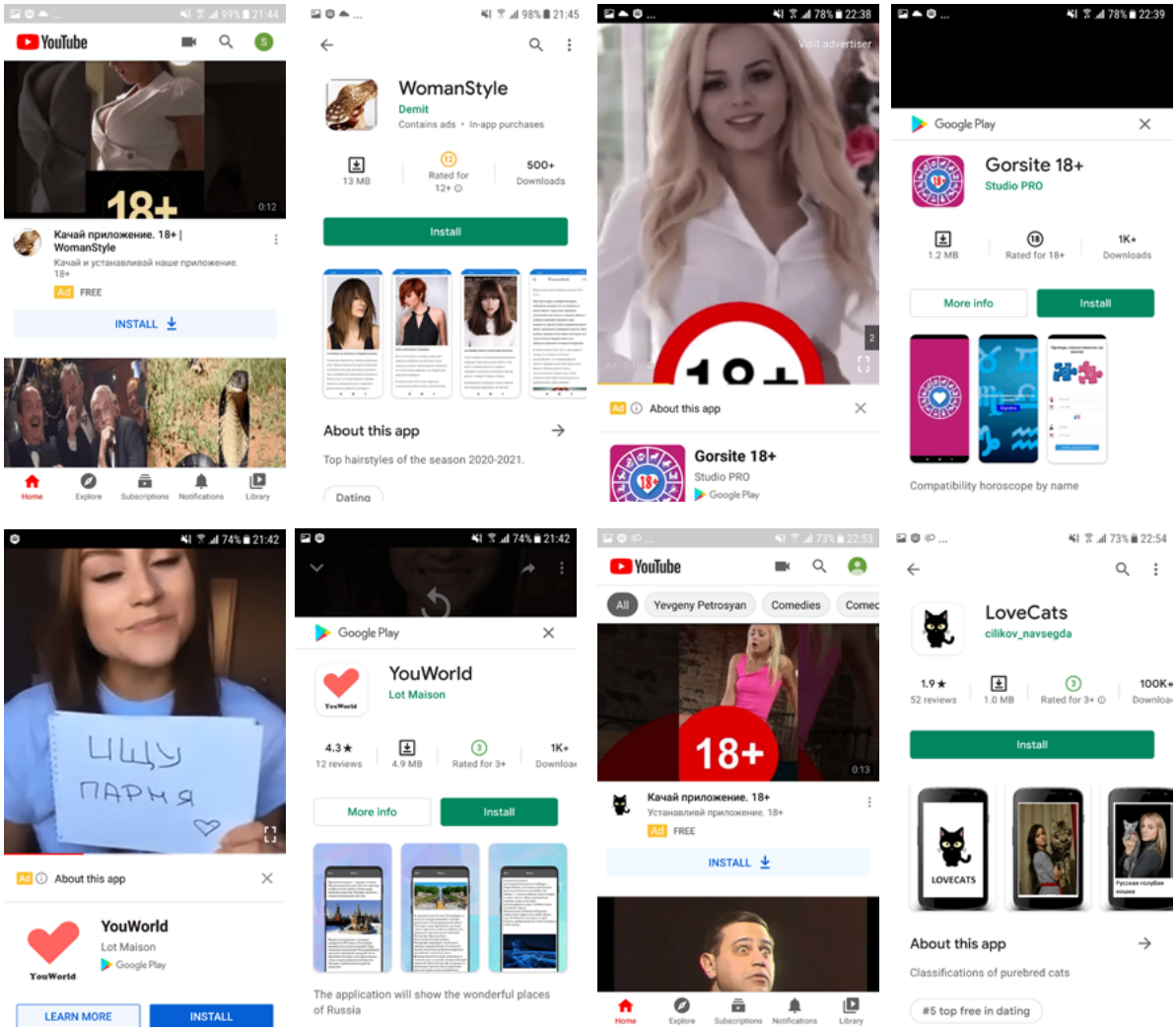


Во вторую группу программ-подделок семейства Android.FakeApp вошли приложения, которые злоумышленники выдавали за безобидные программы разнообразной тематики. Среди них были справочники о моде, животных, природе, различные гороскопы. Их функциональность не соответствовала заявленной, и они лишь загружали всевозможные сайты знакомств, а также откровенно мошеннические сайты. Данные программы активно продвигались через рекламную сеть видеосервиса YouTube, при этом в роликах и баннерах агрессивно использовалась тематика категории «для взрослых», а также знакомств и свиданий. В общей сложности специалисты «Доктор Веб» выявили свыше 20 вариантов таких поддельных программ.
Примеры расположенных в каталоге Google Play троянских приложений Android.FakeApp и ведущей на них вредоносной рекламы представлены ниже:



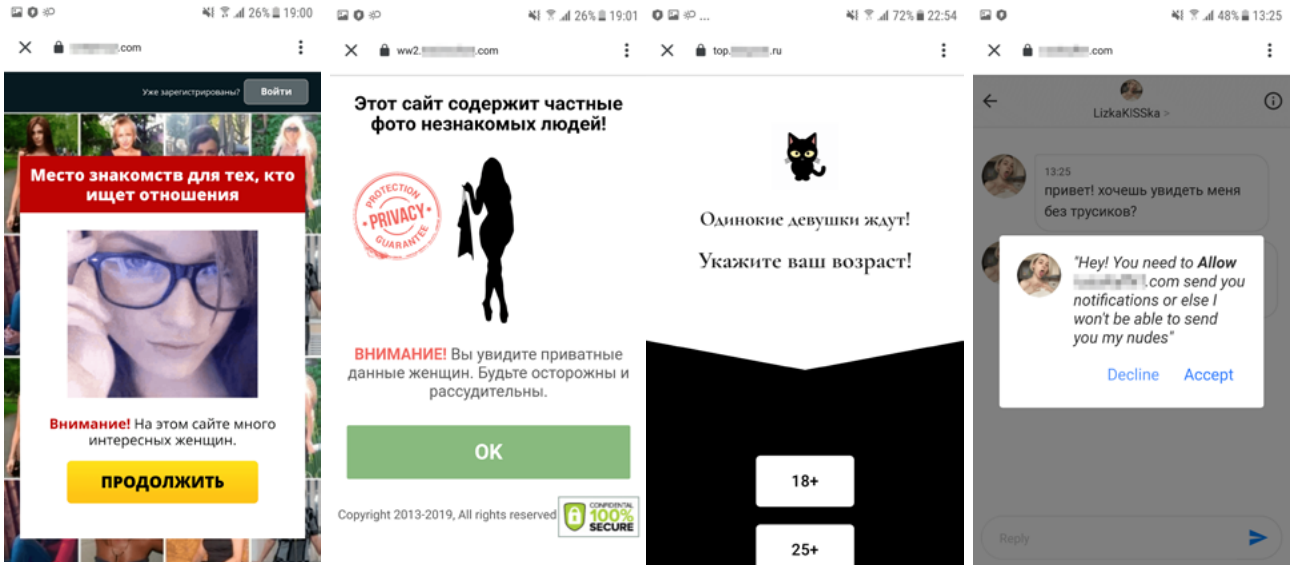
«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2021 года

По данным антивирусных продуктов Dr.Web для Android

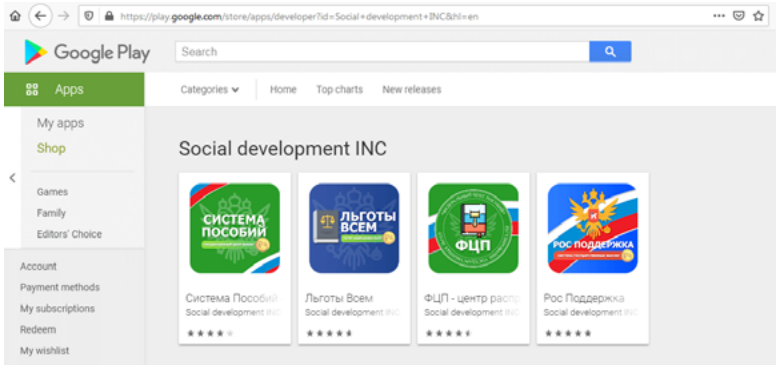


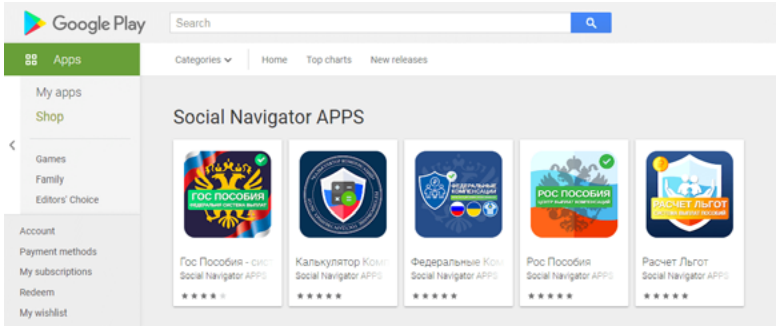
По данным антивирусных продуктов Dr.Web для Android

Примеры сайтов, которые загружали эти программы:



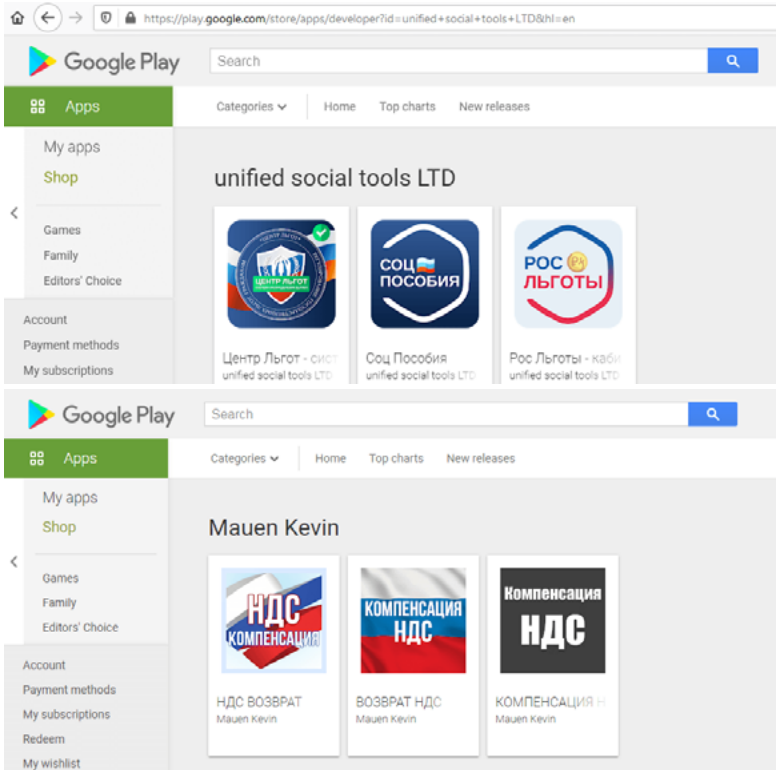
Третью группу вредоносных программ семейства Android.FakeApp представляли очередные вариации мошеннических троянов, которые распространялись под видом ПО с информацией о различных денежных компенсациях, льготах и социальных выплатах. Ими оказались новые модификации известных вредоносных приложений Android.FakeApp.219 и Android.FakeApp.227.



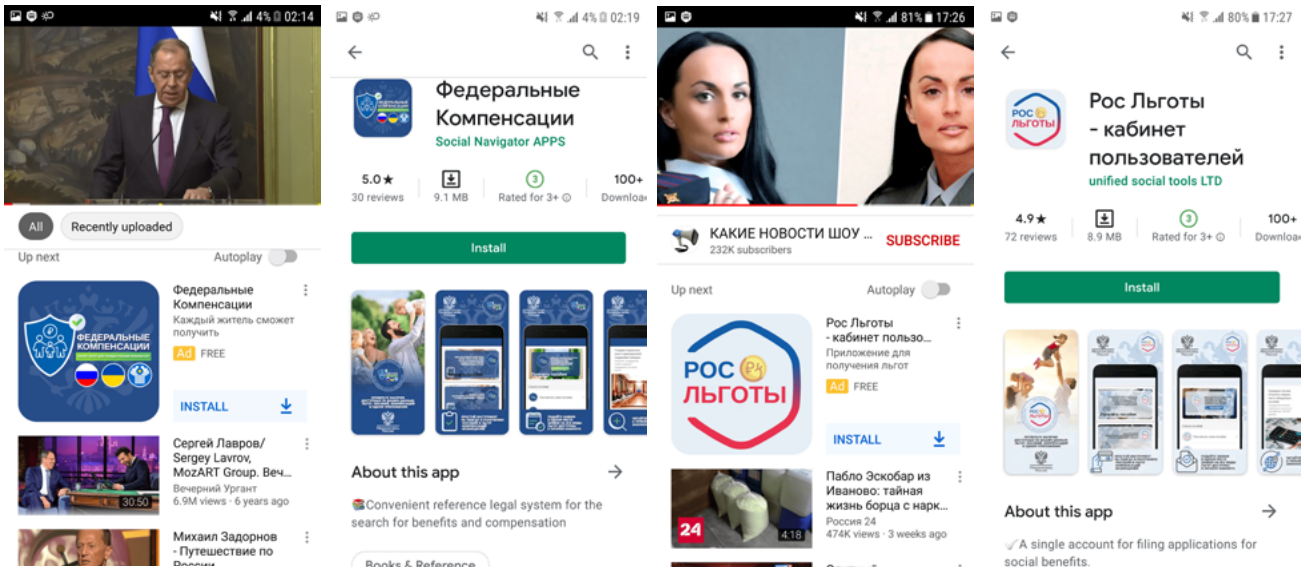


«Доктор Веб»: обзор вирусной активности для мобильных устройств в феврале 2021 года

По данным антивирусных продуктов Dr.Web для Android



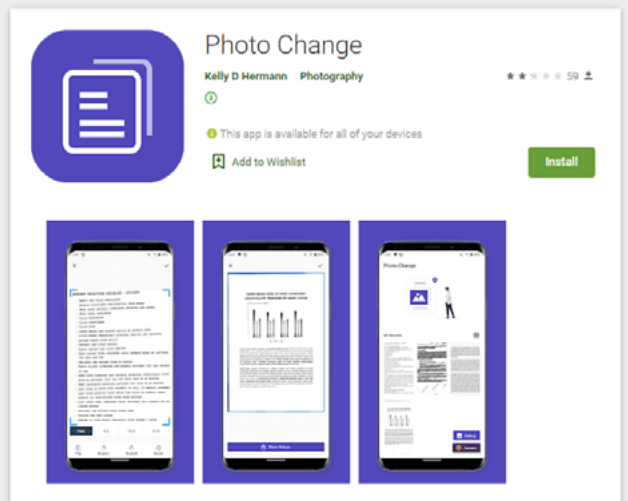
Как и ряд других вредоносных программ-подделок этого семейства, они также рекламировались через YouTube:

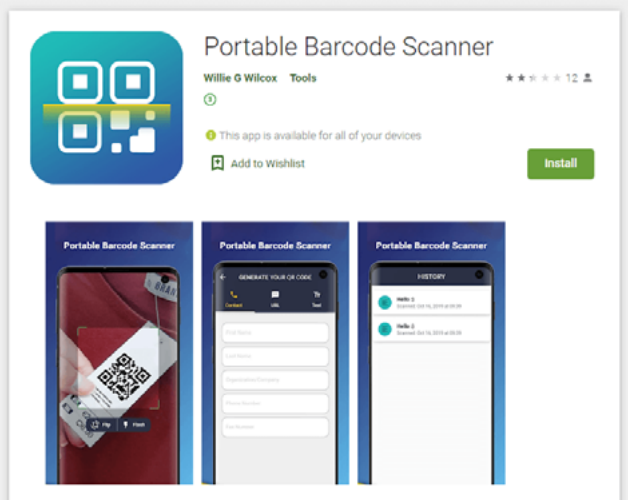


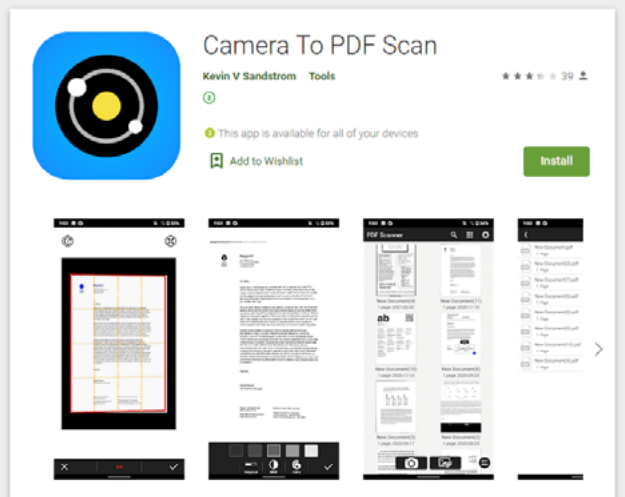
Угрозы в Google Play

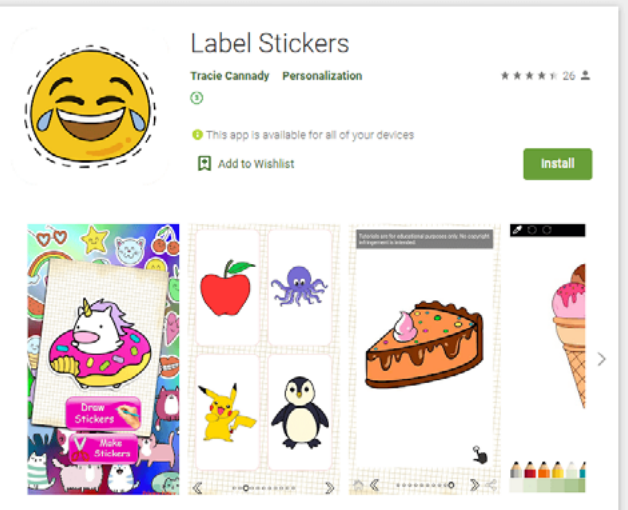
При запуске трояны загружали мошеннические сайты, на которых потенциальные жертвы якобы могли найти сведения о доступных для них выплатах. Там пользователей вводили в заблуждение, предлагая указать конфиденциальную информацию и оплатить либо комиссию за «перевод» денег на их банковский счет, либо «госпошлину». Никаких компенсаций они на самом деле не получали и лишь передавали мошенникам свои деньги и персональные данные.

Также вирусные аналитики компании «Доктор Веб» выявили несколько новых многофункциональных троянов семейства Android.Joker. Как и другие вредоносные приложения этого семейства, они распространялись под видом полезных программ — редактора изображений, сканера штрих-кодов, программы для создания PDF-документов, сборника стикеров для мессенджеров, анимированных обоев для рабочего стола и других приложений. Трояны были добавлены в вирусную базу Dr.Web как Android.Joker.580, Android.Joker.585, Android.Joker.586, Android.Joker.592, Android.Joker.595, Android.Joker.598 и Android.Joker.604.

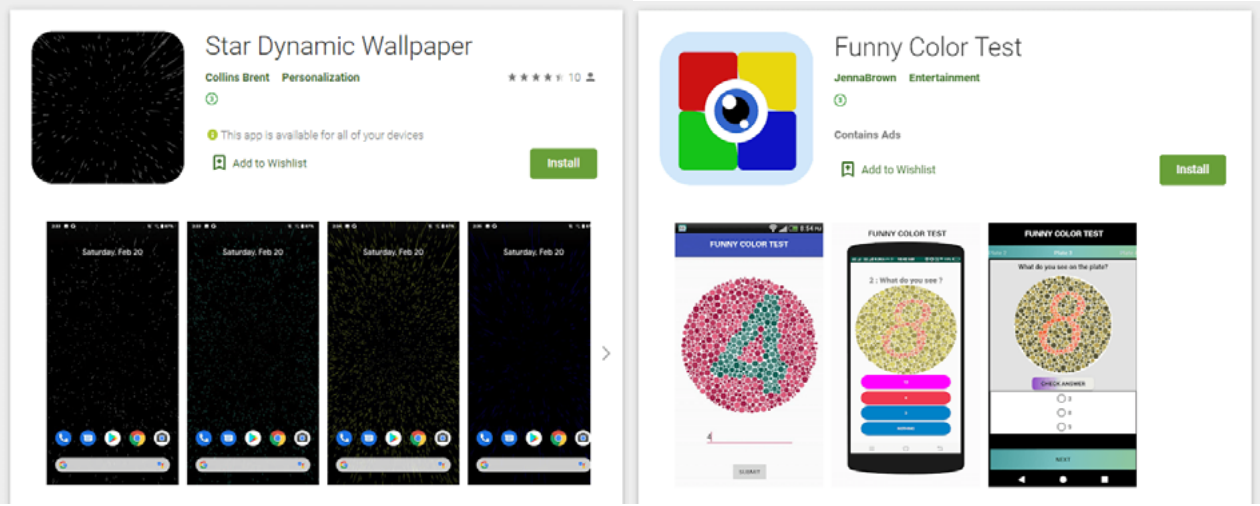






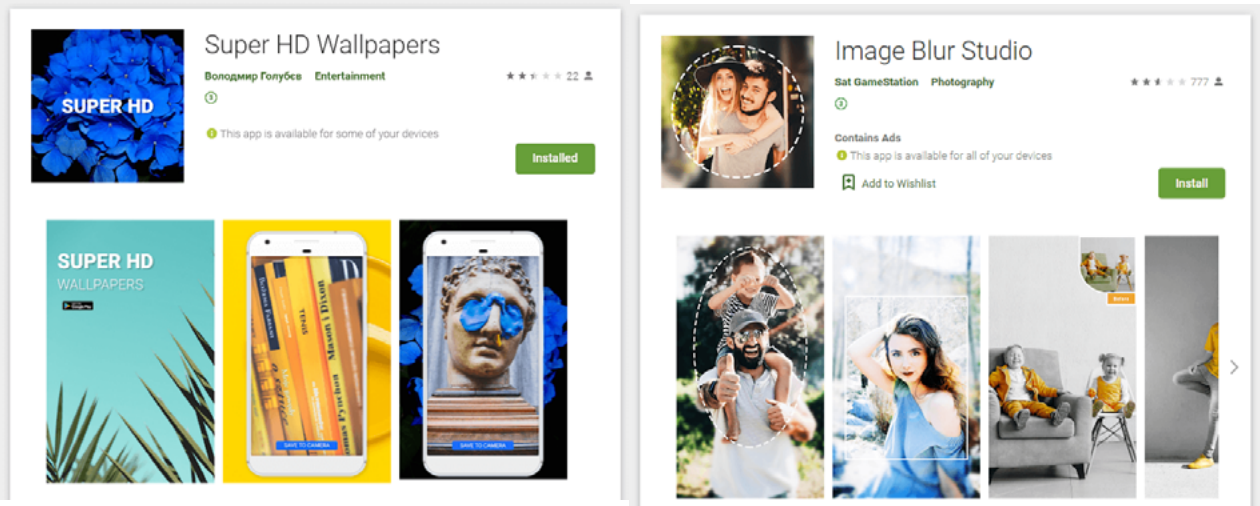


Угрозы в Google Play



Их главные функции — загрузка и запуск произвольного кода, а также автоматическая подписка пользователей на дорогостоящие мобильные услуги.

Кроме того, в Google Play были обнаружены очередные рекламные трояны из семейства Android.HiddenAds, получившие имена Android.HiddenAds.610.origin и Android.HiddenAds.2357. Первый распространялся под видом программы с коллекцией изображений, второй — программы для редактирования фотографий.



При запуске они скрывали свои значки из списка установленных программ в меню главного экра-

Угрозы в Google Play

на Android-устройств и начинали демонстрировать рекламу. При этом Android.HiddenAds.610.origin получал команды через облачный сервис Firebase и мог показывать уведомления с объявлениями, а также загружать различные веб-сайты. Среди них были как сайты с рекламой, так и сомнительные и даже мошеннические веб-ресурсы.

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 феврале 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

© ООО «Доктор Веб»,
2003-2021