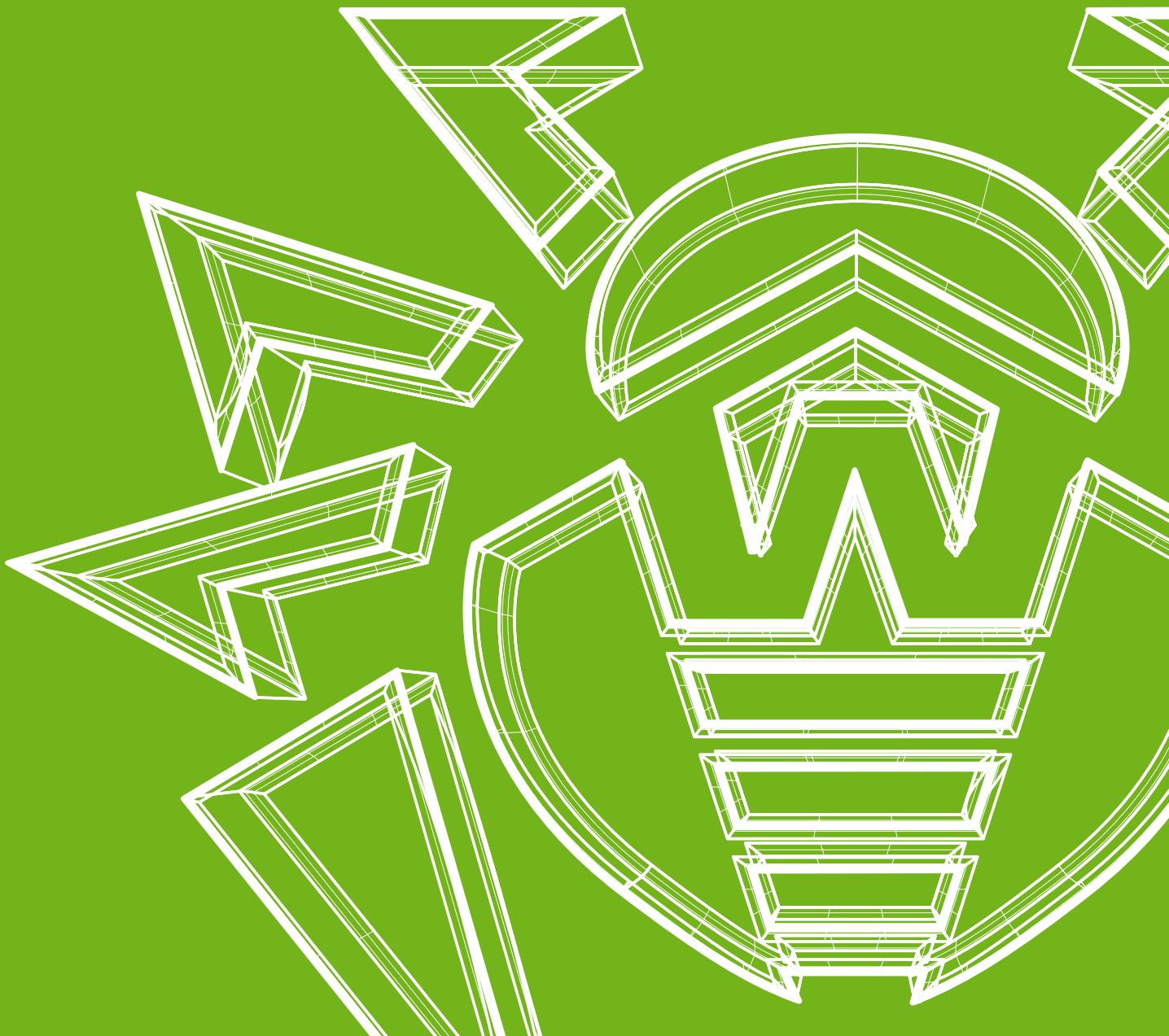
Dr.WEB®
с 1992 года

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



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

15 октября 2021 года

В сентябре антивирусные продукты Dr.Web для Android чаще всего выявляли на защищаемых устройствах рекламные трояны, а также вредоносные программы, загружающие другое ПО и выполняющие произвольный код. Кроме того, среди наиболее активных угроз вновь оказались различные нежелательные рекламные модули, которые разработчики встраивают в приложения с целью монетизации.

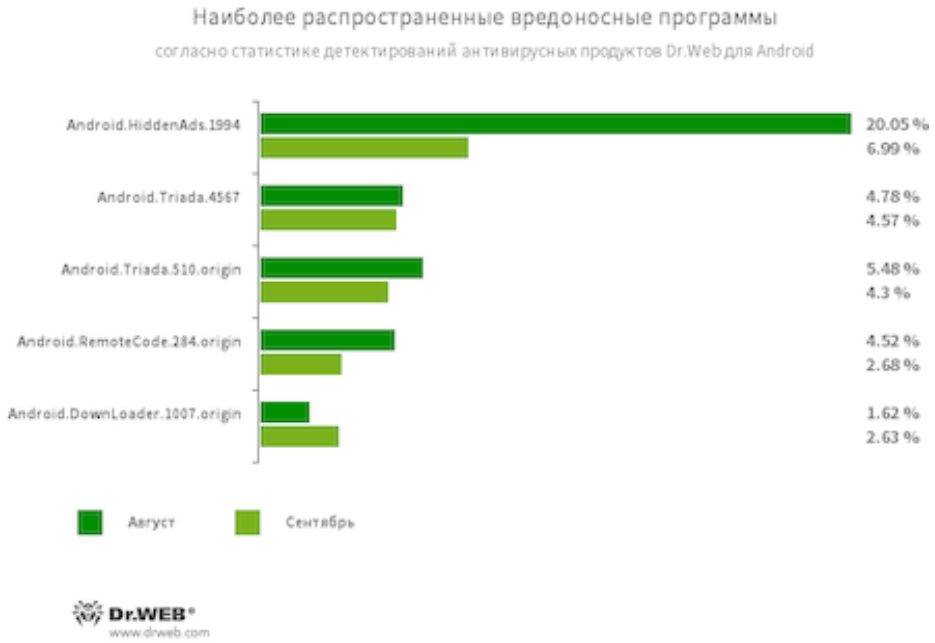
В течение предыдущего месяца вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play десятки новых программ-подделок семейства Android.FakeApp, используемых злоумышленниками в различных мошеннических схемах.

ГЛАВНЫЕ ТЕНДЕНЦИИ СЕНТЯБРЯ

- Высокая активность приложений-подделок, распространяемых через каталог Google Play
- Трояны, загружающие приложения и выполняющие произвольный код, а также рекламные вредоносные приложения остаются одной из наиболее актуальных угроз

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

По данным антивирусных продуктов Dr.Web для Android



Android.HiddenAds.1994

Троян, предназначенный для показа навязчивой рекламы. Трояны этого семейства часто распространяются под видом безобидных приложений и в некоторых случаях устанавливаются в системный каталог другими вредоносными программами.

Android.Triada.4567

Android.Triada.510.origin

Многофункциональные трояны, выполняющие разнообразные вредоносные действия. Относятся 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.RemoteCode.284.origin

Вредоносная программа, которая загружает и выполняет произвольный код. В зависимости от модификации трояны этого семейства также могут загружать различные веб-сайты, переходить по ссылкам, нажимать на рекламные баннеры, подписывать пользователей на платные услуги и выполнять другие действия.

Android.DownLoader.1007.origin

Троян, загружающий другие вредоносные программы и ненужное ПО. Подобные трояны могут скрываться во внешне безобидных приложениях, которые распространяются через каталог Google Play или вредоносные сайты.

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

По данным антивирусных продуктов Dr.Web для Android

Program.FakeAntiVirus.1

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.WapSniff.1.origin

Программа для перехвата сообщений в мессенджере WhatsApp.

Program.FreeAndroidSpy.1.origin

Program.Reptilicus.7.origin

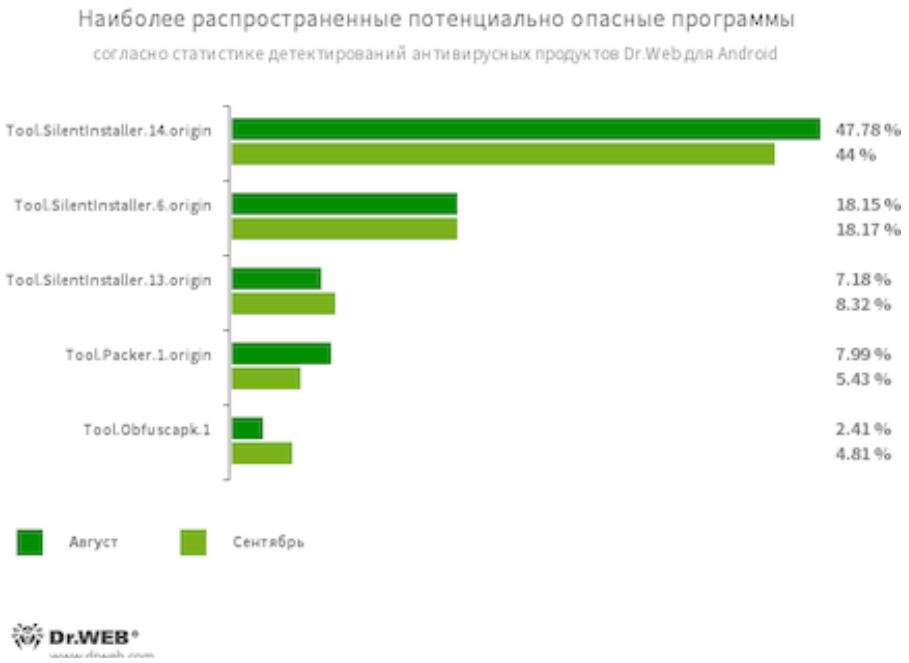
Приложения, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа. Они способны контролировать местоположение устройств, собирать данные об СМС-переписке, беседах в социальных сетях, копировать документы, фотографии и видео, прослушивать телефонные звонки и окружение и т. п.

Program.SecretVideoRecorder.1.origin

Приложение, предназначенное для фоновой фото- и видеосъемки через встроенные камеры Android-устройств. Оно может работать незаметно, позволяя отключить уведомления о записи, а также изменять значок и описание приложения на фальшивые. Такая функциональность делает данную программу потенциально опасной.

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

По данным антивирусных продуктов Dr.Web для Android



Tool.SilentInstaller.14.origin

Tool.SilentInstaller.6.origin

Tool.SilentInstaller.13.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

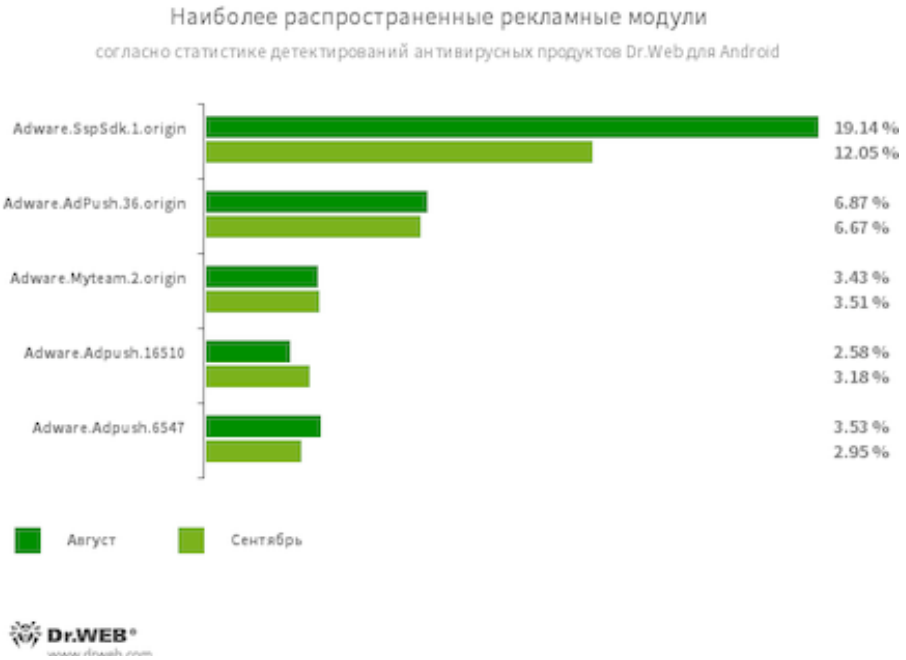
Специализированная утилита-упаковщик, предназначенная для защиты Android-приложений от модификации и обратного инжиниринга. Она не является вредоносной, но может использоваться для защиты как безобидных, так и троянских программ.

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 сентябре 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

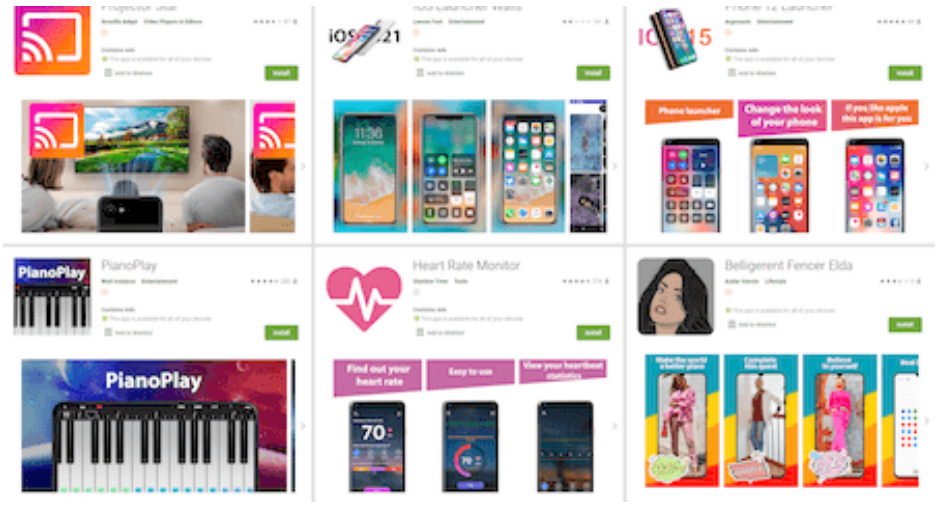
Adware.AdPush.36.origin

Adware.Adpush.16510

Adware.Adpush.6547

Adware.Myteam.2.origin

Угрозы в Google Play



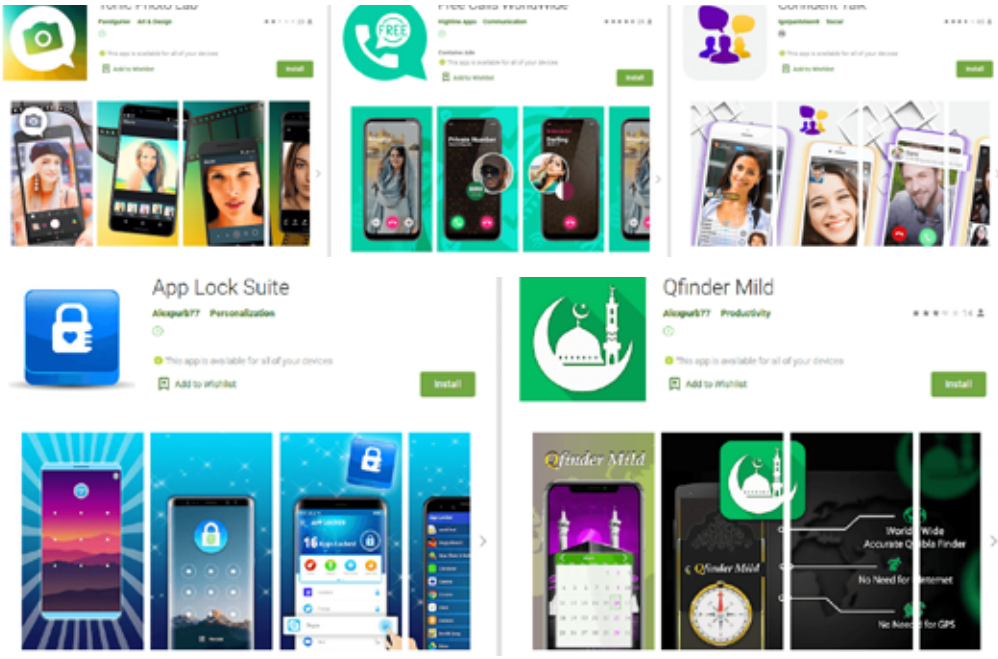
В сентябре специалисты компании «Доктор Веб» обнаружили в Google Play несколько десятков новых приложений-подделок, которые помогали злоумышленникам реализовывать различные мошеннические схемы. В их числе был троян Android.FakeApp.344, несколько модификаций которого распространялись под видом самых разнообразных программ — графических оболочек (лончеров), сборников изображений, самоучителя игры на пианино, приложения для контроля пульса и других.

Его основная функция — загрузка веб-сайтов по команде вирусописателей. При этом троян может использоваться в самых разных вредоносных сценариях: выполнять фишинг-атаки, подписывать жертв на платные мобильные услуги, продвигать интересующие злоумышленников сайты или же загружать сайты с рекламой.

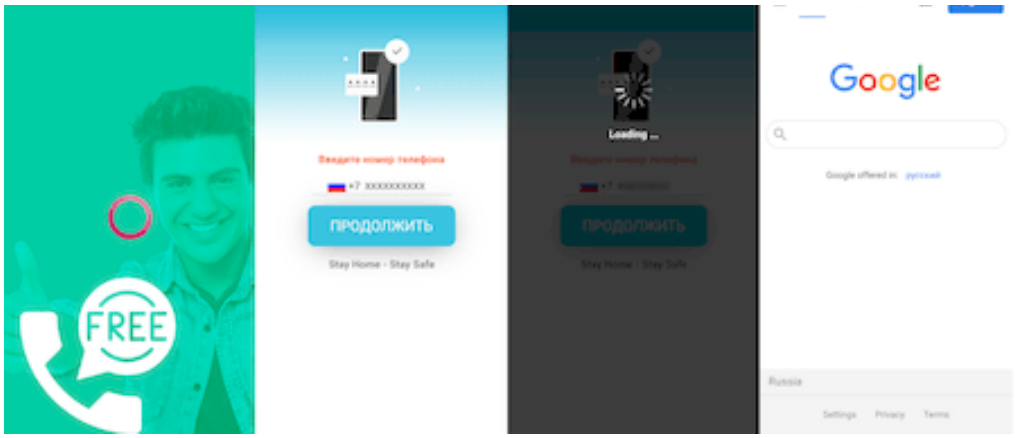
Android.FakeApp.344 управляется через одну из учетных записей GitHub, репозитории которых содержат конфигурационные файлы. При запуске троян получает необходимые настройки. Если в них есть соответствующее задание, он загружает целевой сайт. Если же задания нет или трояну не удалось получить конфигурацию, он работает в обычном режиме, и пользователи могут даже не подозревать, что с программой что-то не так.

Другие обнаруженные вредоносные приложения-подделки получили имена Android.FakeApp.347, Android.FakeApp.364 и Android.FakeApp.385. Они также распространялись под видом безобидных и полезных программ — приложений для осуществления бесплатных звонков, фоторедактора, программы религиозной тематики и ПО для защиты установленных приложений от несанкционированного использования.

Угрозы в Google Play



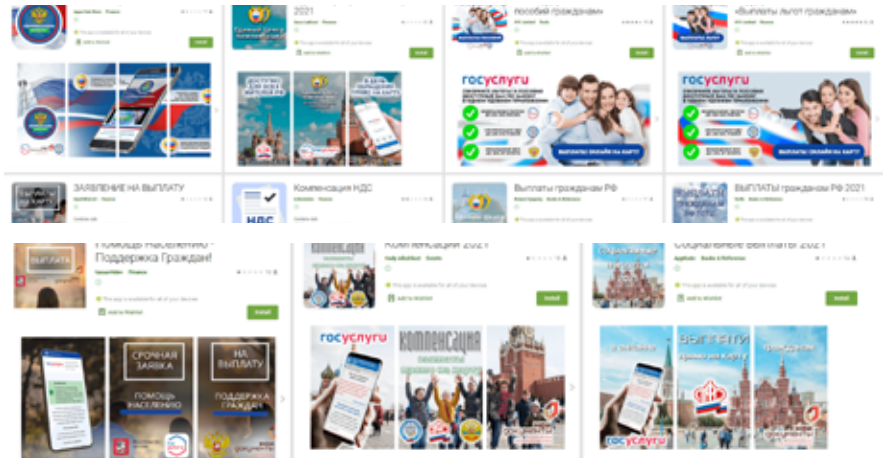
Однако заявленных функций они не выполняли — трояны лишь загружали различные сайты, в том числе те, на которых у пользователей запрашивался номер мобильного телефона. После его ввода владельцы Android-устройств перенаправлялись на страницу поисковой системы, и на этом работа подделок заканчивалась.



Троянские приложения Android.FakeApp.354, Android.FakeApp.355, Android.FakeApp.356, Android.FakeApp.357, Android.FakeApp.358, Android.FakeApp.366, Android.FakeApp.377, Android.FakeApp.378, Android.FakeApp.380, Android.FakeApp.383 и Android.FakeApp.388 якобы должны были помочь российским пользователям найти информацию о государственной социальной поддержке — выплатах льгот, пособий, «компенсации НДС», а также непосредственно получить «полагающиеся по закону» деньги. Однако эти программы лишь заманивали

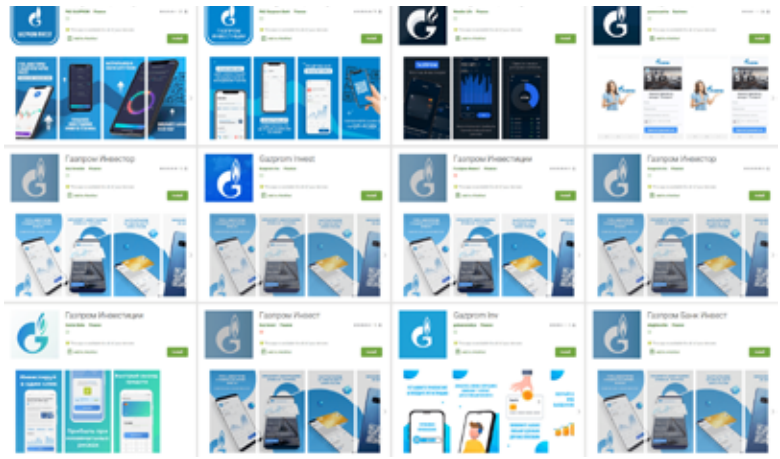
Угрозы в Google Play

владельцев мобильных устройств на мошеннические сайты, где абсолютно любому посетителю сулились многотысячные выплаты. За «начисление» обещанных средств от пользователей требовалось оплатить «государственную пошлину» или «комиссию банка» в размере от нескольких сотен до нескольких тысяч рублей. Никаких выплат жертвы этой обманной схемы на самом деле не получали — вместо этого они переводили собственные средства мошенникам.



Другие программы-подделки, добавленные в вирусную базу Dr.Web как Android.FakeApp.348, Android.FakeApp.349, Android.FakeApp.350, Android.FakeApp.351, Android.FakeApp.352, Android.FakeApp.353, Android.FakeApp.365, Android.FakeApp.367, Android.FakeApp.368, Android.FakeApp.369, Android.FakeApp.370, Android.FakeApp.382, Android.FakeApp.384, Android.FakeApp.387 и Android.FakeApp.389, мошенники выдавали за официальные инвестиционные приложения компании «Газпром». С их помощью пользователи якобы могли получать значительный пассивный доход от инвестиций, не имея ни опыта, ни специальных экономических знаний. Всю работу за них якобы должен был выполнять менеджер или некий уникальный алгоритм.

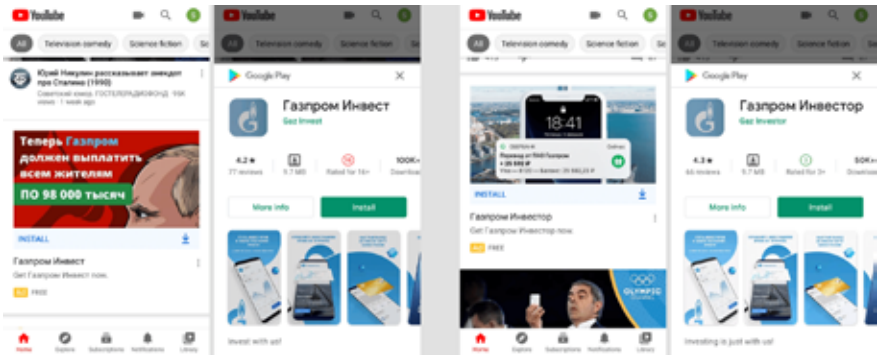
Примеры страниц таких программ в Google Play:



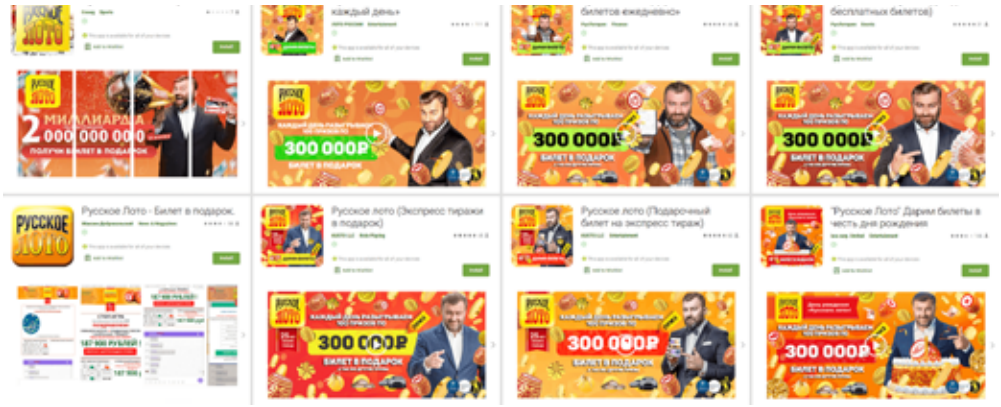
Угрозы в Google Play

В действительности эти троянские приложения не имели никакого отношения к известным компаниям и инвестициям. Они загружали мошеннические сайты, на которых владельцам Android-устройств предлагалось зарегистрировать учетную запись, указав персональную информацию, и дождаться звонка «оператора». Предоставленные при регистрации данные — имена, фамилии, адреса электронной почты и номера телефонов — злоумышленники могли самостоятельно использовать для дальнейшего обмана пользователей или же продать на черном рынке.

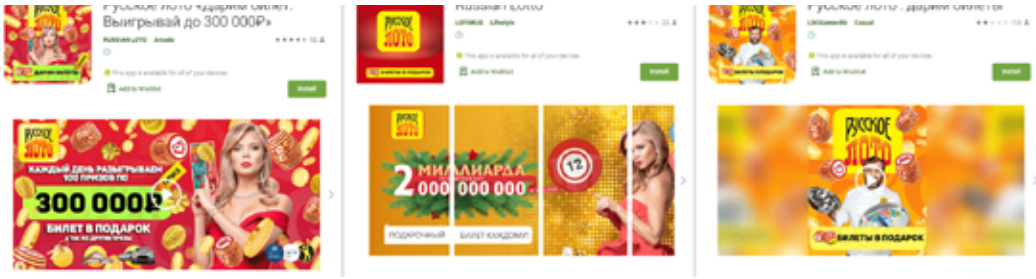
При этом для привлечения внимания и увеличения числа установок таких троянов злоумышленники активно рекламируют их, например, через видеосервис YouTube. Пример подобной рекламы:



Были выявлены и очередные подделки, выдаваемые за официальные приложения популярных российских лотерей. Они были добавлены в вирусную базу Dr.Web как Android.FakeApp.359, Android.FakeApp.360, Android.FakeApp.361, Android.FakeApp.362, Android.FakeApp.363, Android.FakeApp.371, Android.FakeApp.372, Android.FakeApp.373, Android.FakeApp.374, Android.FakeApp.379 и Android.FakeApp.381. С их помощью пользователи якобы могли получить бесплатные лотерейные билеты и принять участие в розыгрышах. Эти программы также загружали мошеннические сайты, где для получения несуществующих билетов и выигрышей требовалось оплатить «комиссию».

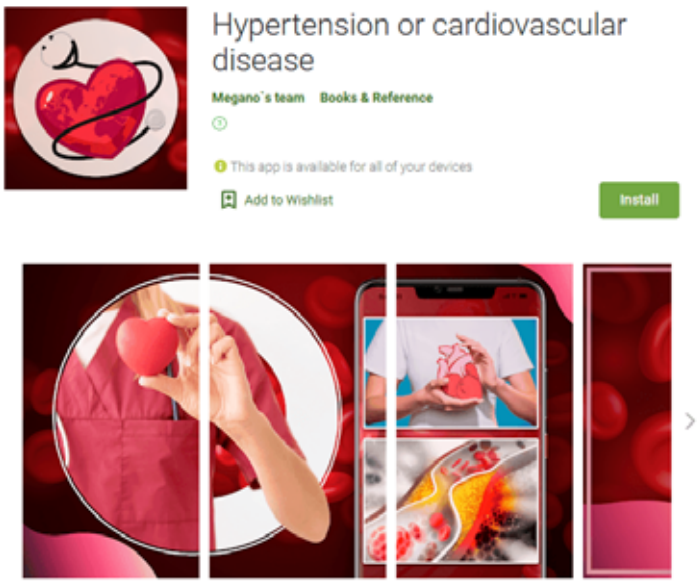


Угрозы в Google Play



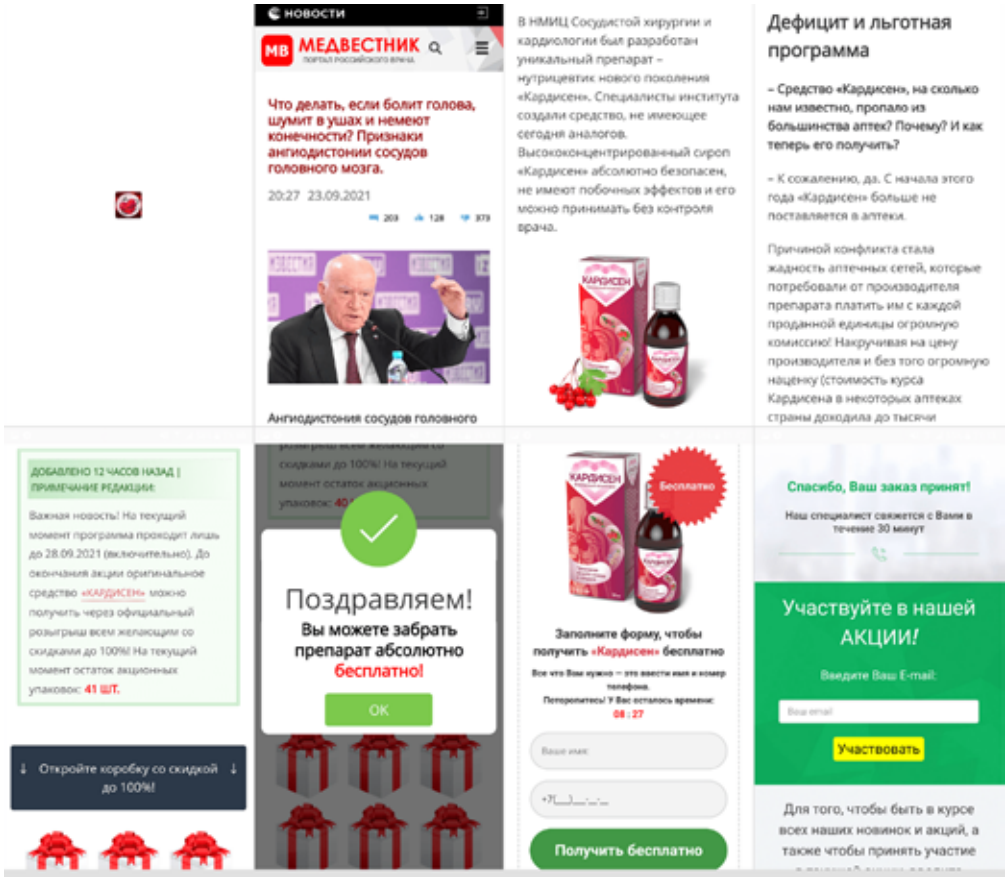
Кроме того, наши специалисты обнаружили несколько модификаций трояна Android.FakeApp.386, который распространялся под видом программ-справочников — с их помощью пользователи якобы могли почерпнуть знания о здоровье и ознакомиться с возможными способами лечения тех или иных недугов. На самом деле это были обычные подделки. Они не выполняли заявленных функций и только загружали веб-сайты, которые зачастую имитировали популярные информационные ресурсы. На таких сайтах от лица известных врачей и медийных персон рекламировались всевозможные препараты сомнительного качества. Потенциальные «клиенты» также завлекались предложениями получить препараты якобы бесплатно или с большой скидкой, если укажут имя и номер телефона, а затем дождутся звонка «менеджера».

Пример одного из таких приложений:



Угрозы в Google Play

Пример его работы:



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 сентябре 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