Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2019 год

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2019 год

Главное

28 января 2020 года

В ушедшем году продолжилась тенденция к появлению многокомпонентных угроз для устройств под управлением ОС Android. Вирусописатели все чаще переносят основные функции троянцев в отдельные модули, которые загружаются и запускаются уже после установки вредоносных приложений. Это не только снижает вероятность их обнаружения, но и позволяет создавать универсальные вредоносные программы, способные выполнять самый широкий спектр задач.

Google Play вновь стал источником распространения различных угроз. Несмотря на попытки компании Google защитить официальный каталог Android-приложений, злоумышленникам по-прежнему удается размещать в нем вредоносное, нежелательное и другое опасное ПО.

Высокую активность проявили троянцы-кликеры, которые приносили доход киберпреступникам как за счет автоматических переходов по ссылкам и рекламным баннерам, так и благодаря подписке жертв на дорогостоящие мобильные услуги. Появились новые рекламные троянцы, а также нежелательные рекламные модули, которые показывали агрессивную рекламу и мешали нормальной работе с Android-устройствами. Кроме того, широкое распространение вновь получили троянцы, которые скачивают и пытаются установить другие вредоносные приложения, а также ненужное ПО.

В течение года пользователи сталкивались с очередными Android-банкерами. Также владельцам Android-устройств угрожало ПО для кибершпионажа и всевозможные бэкдоры — троянцы, позволяющие контролировать зараженные устройства и по команде выполняющие различные действия.

Актуальной осталась проблема мошенничества. Почти каждый месяц специалисты компании «Доктор Веб» фиксировали появление новых приложений, созданных для обмана и кражи денег у пользователей Android-устройств. Одна из популярных схем на вооружении злоумышленников — создание веб-сайтов с поддельными опросами, поучаствовать в которых потенциальным жертвам предлагается за «вознаграждение».

Были обнаружены и новые вредоносные приложения, которые эксплуатировали критические уязвимости ОС Android.

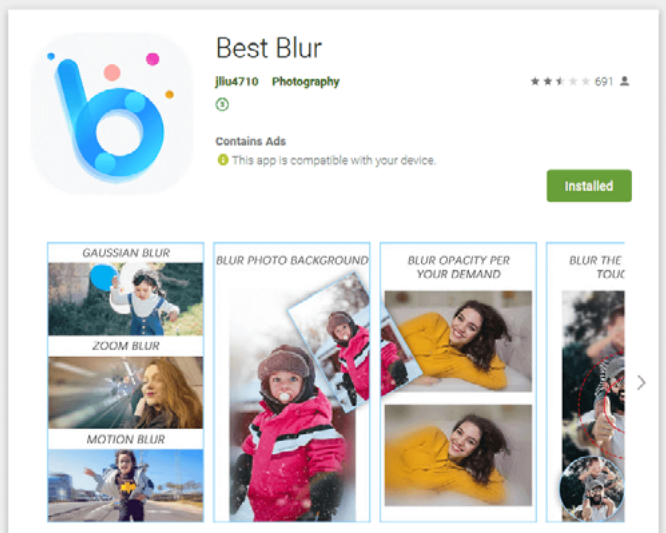
Тенденции прошедшего года

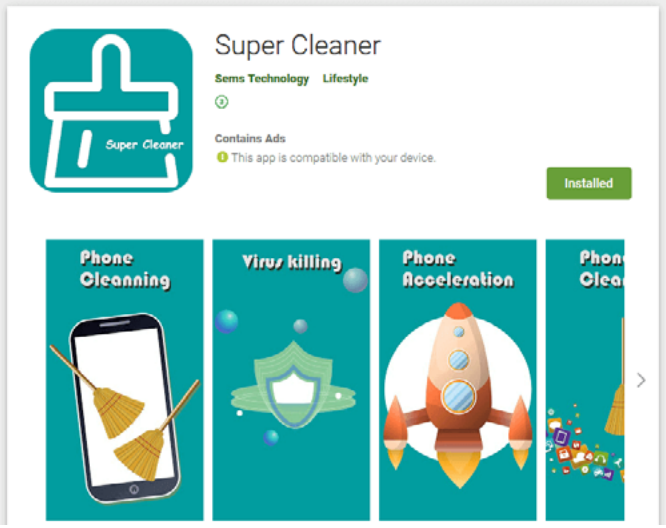
- Распространение угроз через каталог Google Play.
- Активность банковских троянцев.
- Появление новых вредоносных программ, помогающих злоумышленникам похищать деньги пользователей Android-устройств.
- Рост числа троянцев с модульной архитектурой, позволяющей им дольше оставаться незаметными.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2019 год

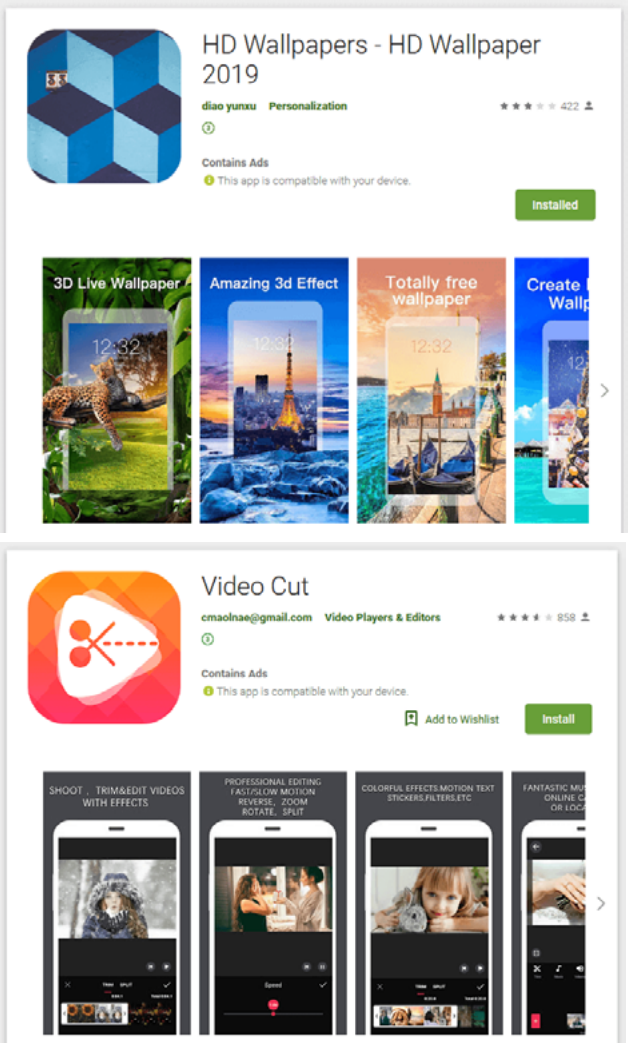
Наиболее интересные события 2019 года

В феврале вирусные аналитики «Доктор Веб» выявили в Google Play несколько десятков рекламных троянцев семейства Android.HiddenAds, которые злоумышленники выдавали за программы для фотосъемки, редакторы изображений и видео, полезные утилиты, сборники обоев рабочего стола, игры и другое безобидное ПО. После установки те скрывали значки из списка программ на главном экране и создавали вместо них ярлыки. При удалении таких ярлыков у пользователей создавалось ложное впечатление, что и сами троянцы удалялись с устройств, однако на самом деле они продолжали скрытно работать и практически непрерывно показывали надоедливую рекламу.





Наиболее интересные события 2019 года



Для более успешного распространения троянцев мошенники рекламировали их в популярных онлайн-сервисах Instagram и YouTube. В результате вредоносные программы загрузили почти 10 000 000 пользователей. В течение года злоумышленники активно применяли этот метод для распространения и других троянцев этого семейства.

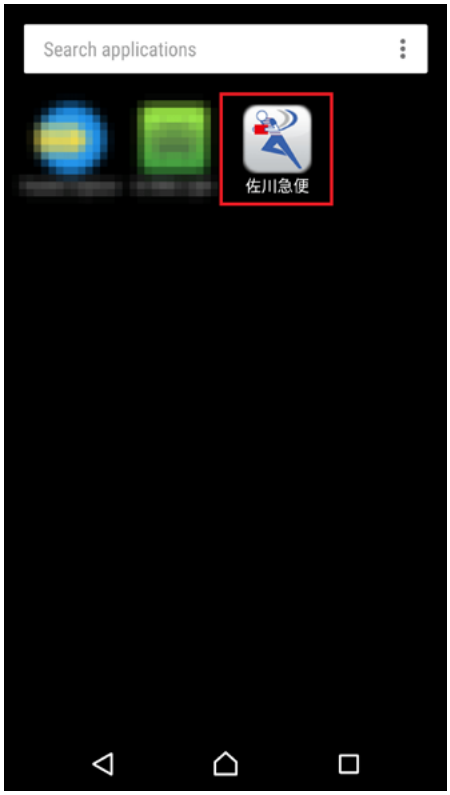
В марте вирусные аналитики обнаружили скрытую функцию загрузки и запуска непроверенных модулей в популярных браузерах UC Browser и UC Browser Mini. Программы могли скачивать дополнительные плагины в обход Google Play, делая свыше 500 000 000 пользователей уязвимыми для потенциальных атак злоумышленников.

В апреле компания «Доктор Веб» опубликовала исследование опасного троянца Android.InfectionAds.1, который эксплуатировал критические уязвимости Janus

Наиболее интересные события 2019 года

2017-13156) и EvilParcel (CVE-2017-13315) в ОС Android для заражения и автоматической установки других приложений. Вирусописатели распространяли Android.InfectionAds.1 через сторонние каталоги приложений, откуда его успели скачать несколько тысяч владельцев Android-устройств. Главная функция этого троянца — показ рекламных баннеров и подмена идентификаторов популярных рекламных платформ таким образом, что вся прибыль от демонстрации легальной рекламы в зараженных приложениях поступала не их разработчикам, а авторам Android.InfectionAds.1.

В этом же месяце наши вирусные аналитики обнаружили модификацию банкера Android.Banker.180.origin, атаковавшего японских пользователей. Троянец распространялся под видом приложения для отслеживания почтовых отправлений и после запуска скрывал свой значок.

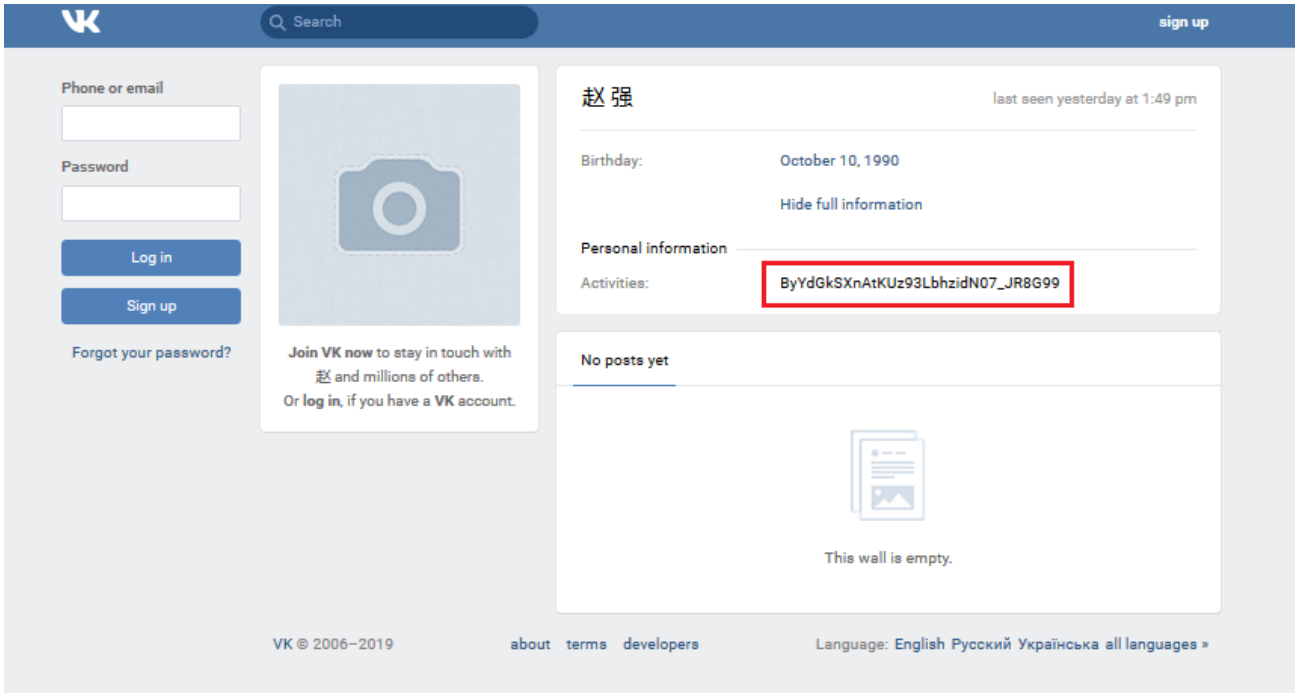


Вирусописатели контролировали банкера через специально созданные страницы в социальной сети «ВКонтакте», на которых в поле «Деятельность» («Activities») в зашифрованном виде располагался адрес одного из управляющих серверов. Android.Banker.180.origin искал это поле с помощью регулярного выражения, расшифровывал адрес и подключался к серверу, ожидая дальнейших команд.

Троянец по команде злоумышленников перехватывал и отправлял СМС-сообщения, по-

Наиболее интересные события 2019 года

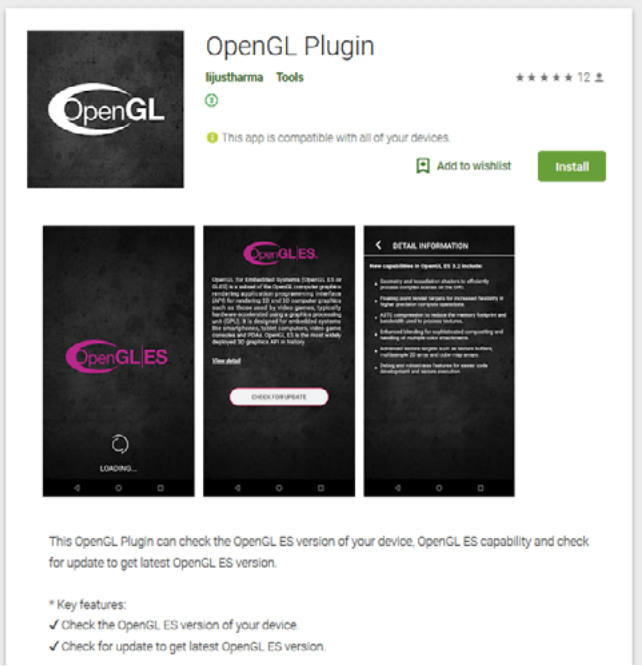
казывал фишинговые окна, выполнял телефонные звонки и прослушивал окружение с использованием микрофона зараженного устройства. Также он мог управлять зараженными устройствами – например, самостоятельно включал Wi-Fi-модуль, устанавливал интернет-соединение через мобильную сеть и блокировал экран.

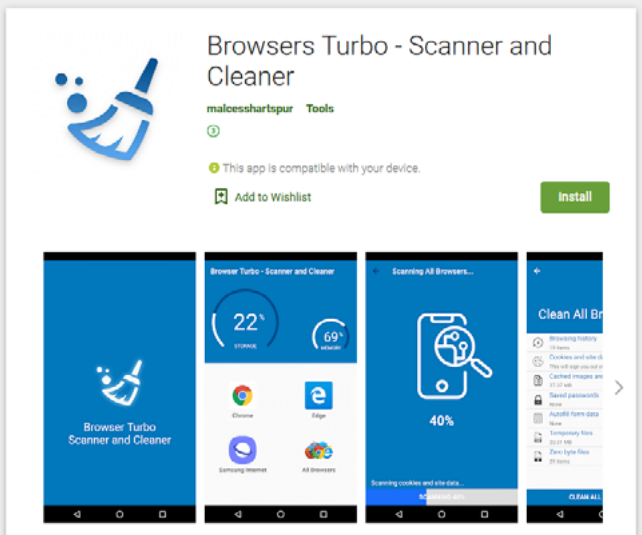


В июле вирусные аналитики обнаружили и исследовали опасного бэкдора Android.Backdoor.736.origin, который распространялся через Google Play под видом программы для обновления графического интерфейса OpenGL ES. Этот троянец, также известный под именем PWNDROID1, выполнял команды злоумышленников и шпионил за пользователями — собирал информацию о местоположении устройств, телефонных вызовах, контактах из телефонной книги, пересылал на сервер хранящиеся на устройствах файлы. Кроме того, он мог загружать и устанавливать приложения и показывать фишинговые окна, чтобы украсть логины, пароли и другие конфиденциальные данные.

Уже в ноябре наши специалисты выявили новую модификацию этого бэкдора. Она тоже распространялась через официальный каталог программ ОС Android, но на этот раз злоумышленники выдавали троянца за утилиту для настройки и ускорения работы браузера.

Наиболее интересные события 2019 года

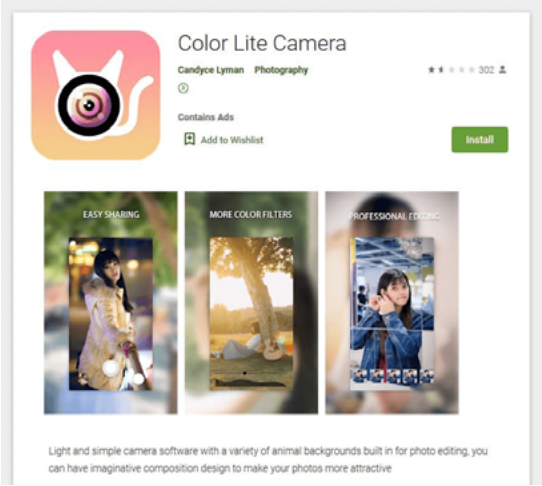




В конце лета вирусные аналитики «Доктор Веб» обнаружили троянца-кликера Android.Click.312.origin, которого загрузили порядка 102 000 000 пользователей. Кликер был встроен в самые разнообразные приложения — аудиоплееры, словари, сканеры штрих-кодов, онлайн-карты и другие, в общей сложности более чем в 30 программ. По команде управляющего сервера Android.Click.312.origin загружал сайты с рекламой и другим сомнительным содержимым.

Наиболее интересные события 2019 года

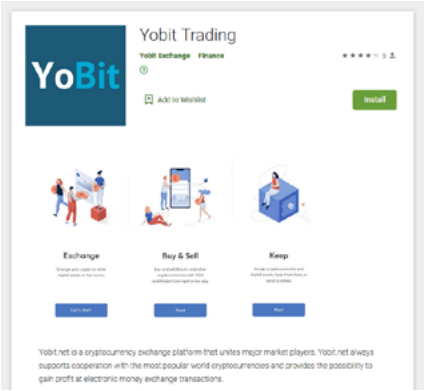
Осенью наши специалисты выявили других троянцев семейства Android.Click — Android.Click.322.origin, Android.Click.323.origin и Android.Click.324.origin. Они не только загружали сайты с рекламой, но и подписывали жертв на дорогостоящие мобильные услуги. Эти троянцы действовали избирательно и выполняли вредоносные функции лишь на устройствах пользователей из определенных стран. Программы, в которые были встроены кликеры, злоумышленники защитили специальным упаковщиком, а сами троянцы «притворялись» известными рекламно-аналитическими платформами, чтобы снизить вероятность своего обнаружения.



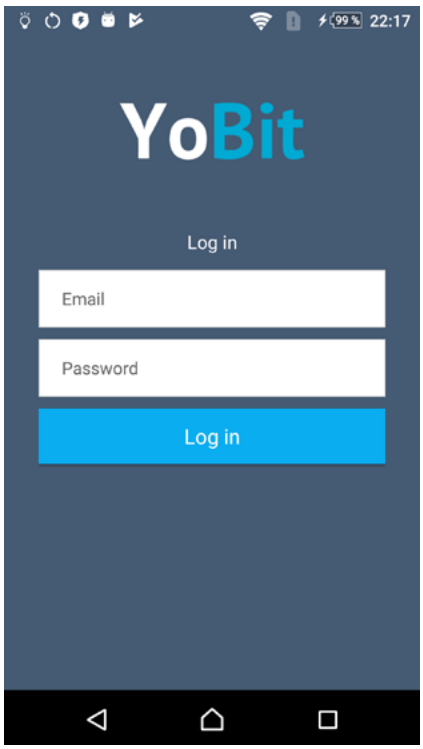
В октябре в Google Play был найден банковский троянец Android.Banker.352.origin, который распространялся под видом официального приложения криптобиржи YoBit. При

Наиболее интересные события 2019 года

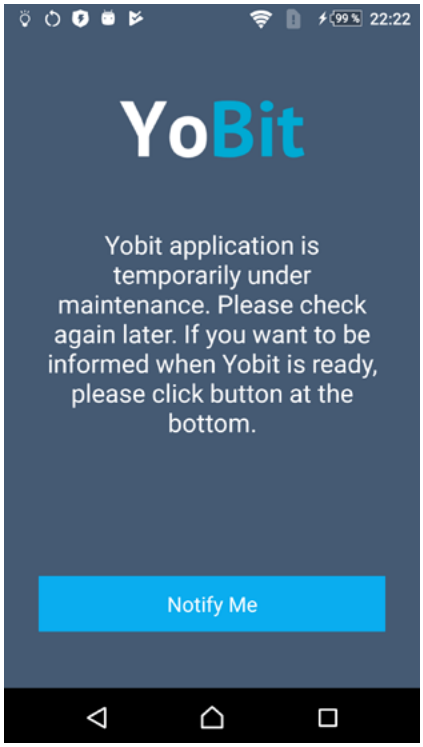
запуске он показывал поддельное окно авторизации и похищал вводимые логины и пароли клиентов биржи. Затем банкер демонстрировал сообщение о временной недоступности сервиса.



Android.Banker.352.origin перехватывал коды двухфакторной аутентификации из СМС, а также коды доступа из email-сообщений. Кроме того, он перехватывал и блокировал уведомления от различных мессенджеров и программ-клиентов электронной почты. Все украденные данные троянец сохранял в базу Firebase Database.



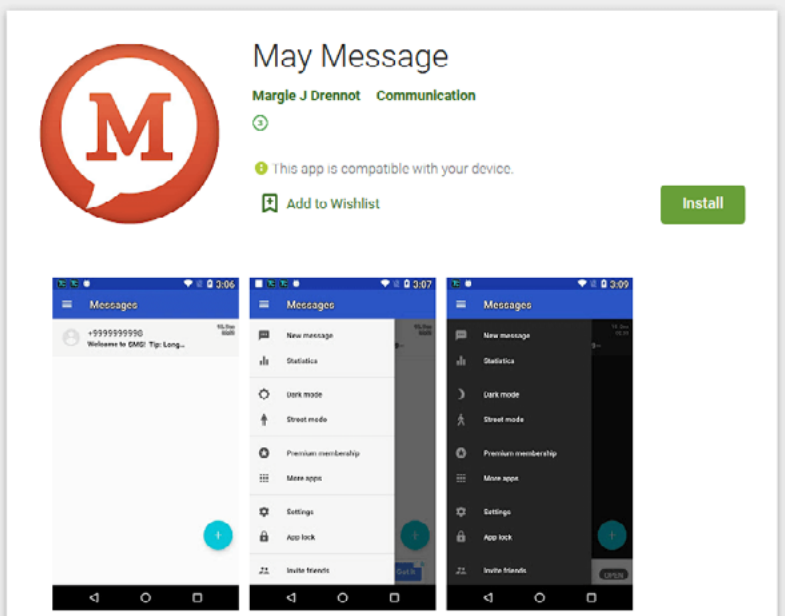
Наиболее интересные события 2019 года

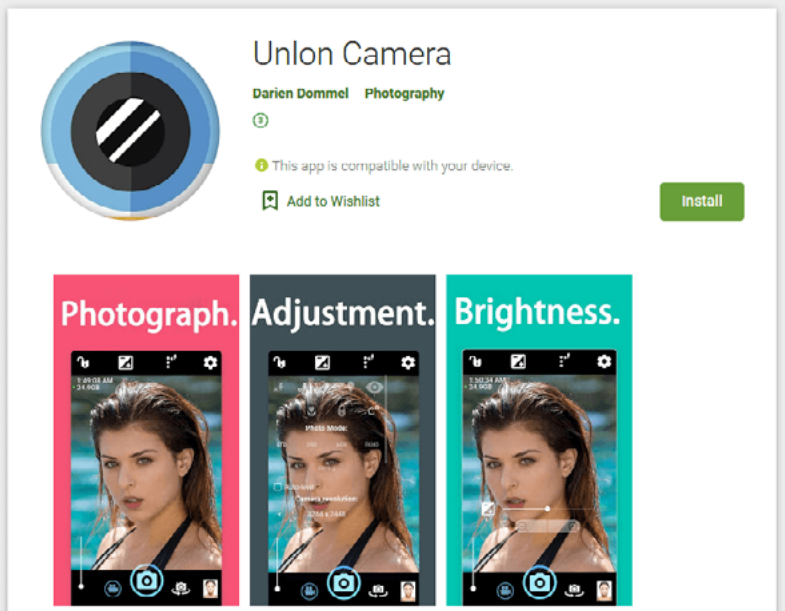


В ушедшем году возросла активность троянцев семейства Android.RemoteCode. Эти вредоносные приложения по команде злоумышленников загружают дополнительные модули и произвольный код, которые затем запускают на исполнение. По сравнению с 2018 годом они обнаруживались на устройствах пользователей на 5,31% чаще.

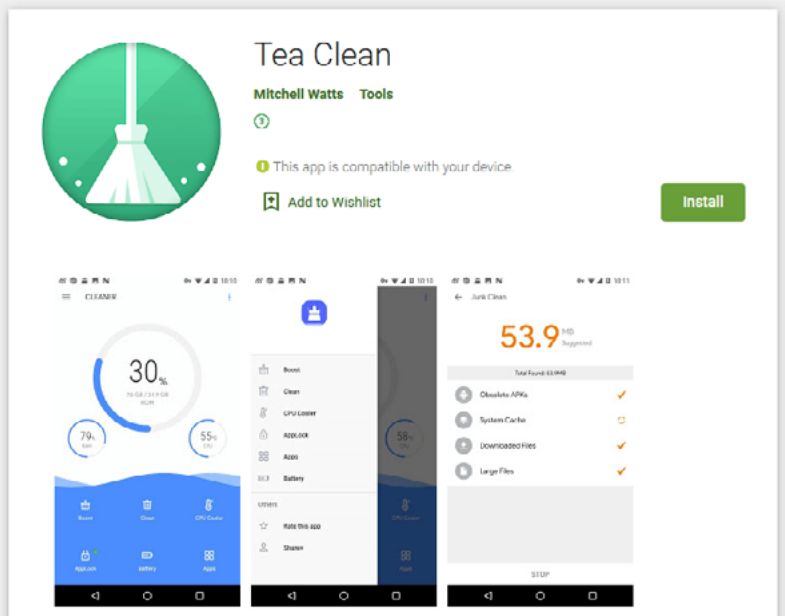
Кроме того, в сентябре стало известно о новом семействе троянцев Android.Joker. Они тоже могли скачивать и запускать произвольный код, а также загружали веб-сайты и подписывали жертв на платные услуги. Чаще всего эти троянцы распространялись под видом приложений для фотосъемки, редактирования фото и видео, мессенджеров, игр, сборников изображений и полезных утилит для оптимизации работы Android-устройств. За несколько месяцев вирусные аналитики «Доктор Веб» выявили множество различных модификаций этих вредоносных программ.

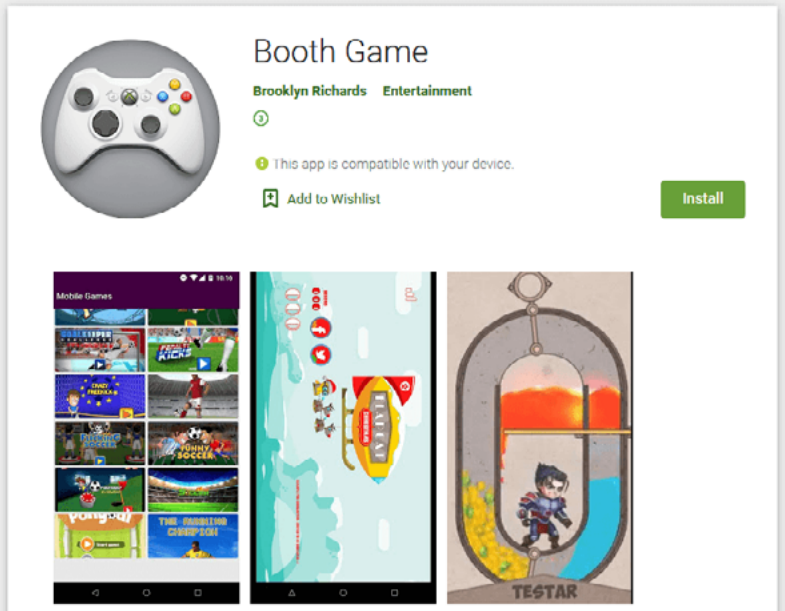
Наиболее интересные события 2019 года





Наиболее интересные события 2019 года





«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2019 год

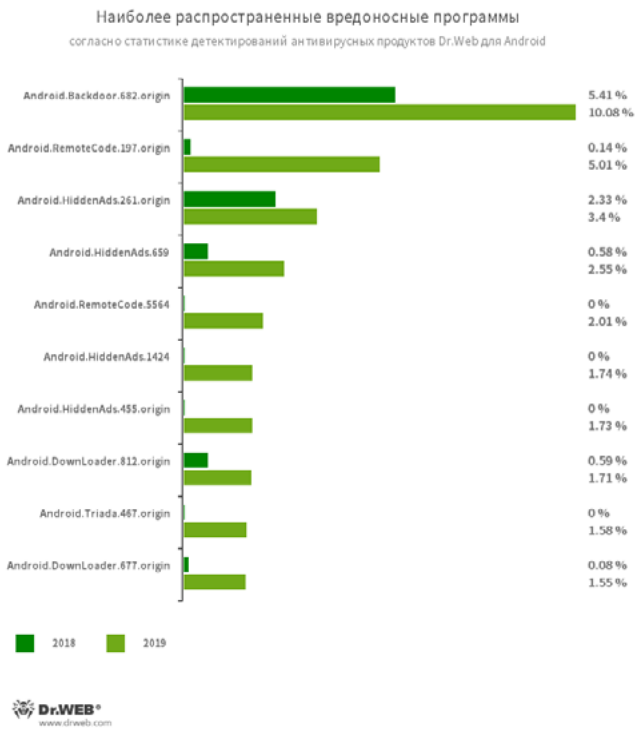
Статистика

В 2019 году антивирусные продукты Dr.Web Для Android обнаружили на устройствах пользователей 19 367 317 угроз — на 40,9% меньше, чем годом ранее. Пик распространения троянцев, нежелательных и потенциально опасных программ, а также рекламного ПО, пришелся на январь. До середины лета их активность снижалась, однако в июле и августе опять возросла. Затем число детектирований вновь стало уменьшаться и достигло минимума в декабре.

Подавляющее большинство угроз составили всевозможные троянцы. На втором месте расположились рекламные программы и плагины. На третьем и четвертом местах со значительным отставанием оказалось потенциально опасное и нежелательное ПО.

Согласно статистике детектирований, наиболее распространенными вредоносными программами стали рекламные троянцы и троянцы, которые скачивали и запускали или устанавливали другие вредоносные приложения, а также выполняли произвольный код. Кроме того, широкое распространение получили бэкдоры, позволяющие злоумышленникам дистанционно управлять зараженными устройствами и шпионить за пользователями.

Статистика

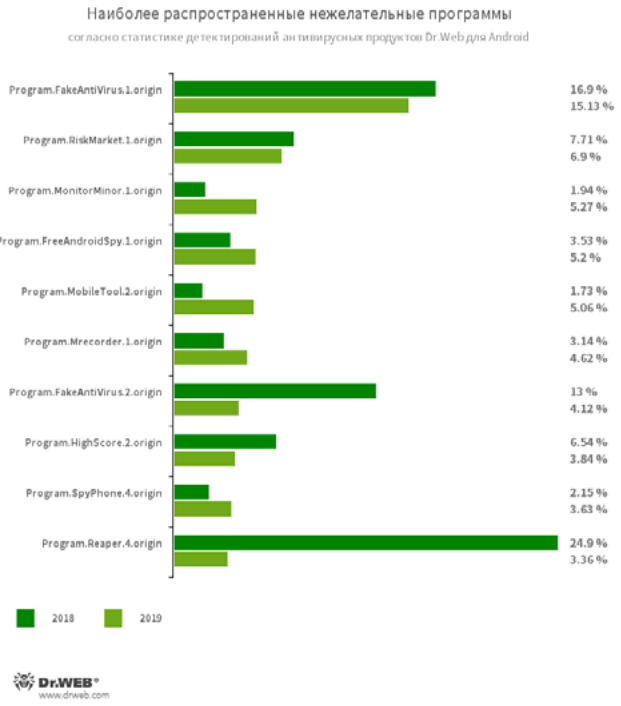


Android.Backdoor.682.origin
Бэкдор, который выполняет команды злоумышленников и позволяет им контролировать зараженные мобильные устройства.
Android.RemoteCode.197.origin
Android.RemoteCode.5564
Троянцы, которые загружают и выполняют произвольный код. Распространяются под видом игр и полезных программ.
Android.HiddenAds.261.origin
Android.HiddenAds.659
Android.HiddenAds.1424
Android.HiddenAds.455.origin
Троянцы, показывающие навязчивую рекламу. Чтобы их было сложнее удалить, после установки скрывают свой значок из списка приложений в меню главного экрана Android.
Android.Triada.467.origin
Многофункциональный троянец, выполняющий разнообразные вредоносные действия.
Android.DownLoader.677.origin
Троянец-загрузчик, скачивающий на Android-устройства другие вредоносные приложения.

Статистика

Одними из самых распространенных нежелательных программ стали приложения, предназначенные для слежки за пользователями. Такое ПО незаметно собирает конфиденциальные сведения — СМС-переписку, информацию о телефонных разговорах, сообщениях из социальных сетей, местоположении устройств, посещаемых сайтах, хранимых на устройствах файлах и т. п. и может использоваться для кибершпионажа.

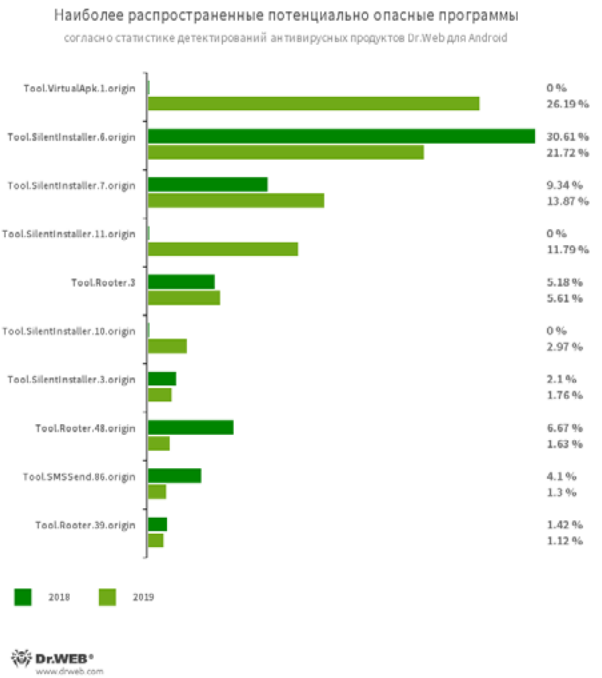
Кроме того, пользователи сталкивались с программами, имитирующими работу антивирусов, а также сомнительными каталогами приложений, через которые распространялись троянцы и пиратские копии бесплатного ПО, продаваемого злоумышленниками за деньги.



Program.FakeAntiVirus.1.origin
Program.FakeAntiVirus.2.origin
Детектирование рекламных приложений, которые имитируют работу антивирусного ПО.
Program.MonitorMinor1.origin
Program.MobileTool.2.origin
Program.FreeAndroidSpy.1.origin
Program.MobileTool.2.origin
Program.SpyPhone.4.origin
Программы, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа.

Статистика

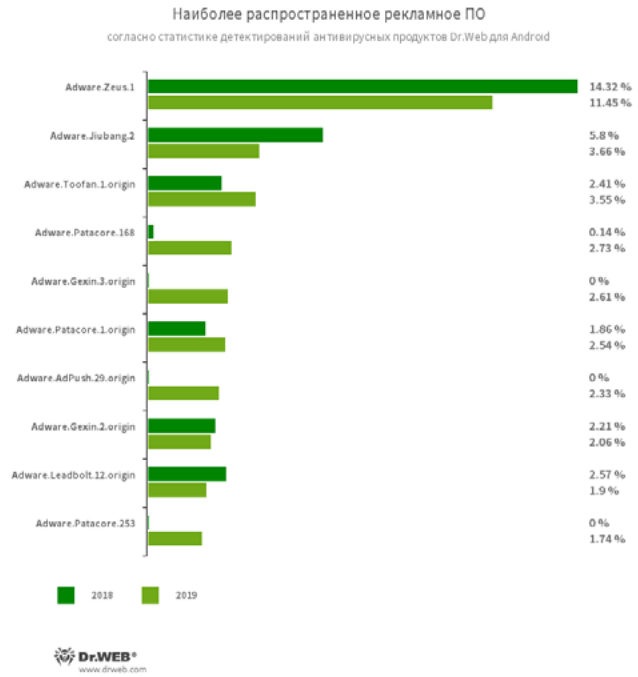
Program.RiskMarket.1.origin
Магазин приложений, который содержит троянские программы и рекомендует пользователям их установку.
Program.HighScore.2.origin
Каталог приложений, в котором через отправку дорогостоящих СМС предлагается оплатить установку доступных в Google Play бесплатных программ.
Program.Reaper.4.origin
Программа, предустанавливаемая на некоторые модели Android-смартфонов. Она без ведома пользователей собирает и передает на удаленный сервер технические сведения об устройствах и данные об их местоположении.
Наиболее часто детектируемыми потенциально опасными приложениями стали утилиты, позволяющие запускать программы без их предварительной установки, а также ПО для получения root-полномочий.



Tool.VirtualApk.1.origin
Tool.SilentInstaller.6.origin
Tool.SilentInstaller.7.origin
Tool.SilentInstaller.11.origin
Tool.SilentInstaller.10.origin
Tool.SilentInstaller.3.origin

Статистика

Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки.
Tool.Rooter.3
Tool.Rooter.48.origin
Tool.Rooter.39.origin
Утилиты для получения root-полномочий на Android-устройствах. Их могут использовать как злоумышленники, так и вредоносные программы.
Tool.SMSSend.86.origin
Приложение для рассылки СМС-сообщений.
Среди рекламного ПО наибольшее распространение получили программные модули, которые показывали баннеры и видеорекламу поверх интерфейса других программ и операционной системы. Они мешали нормальной работе с Android-устройствами и могли привести к значительным расходам, если у пользователей были ограниченные тарифные планы на передачу данных в Интернете.



Adware.Zeus.1
Adware.Jiubang.2
Adware.Toofan.1.origin

Статистика

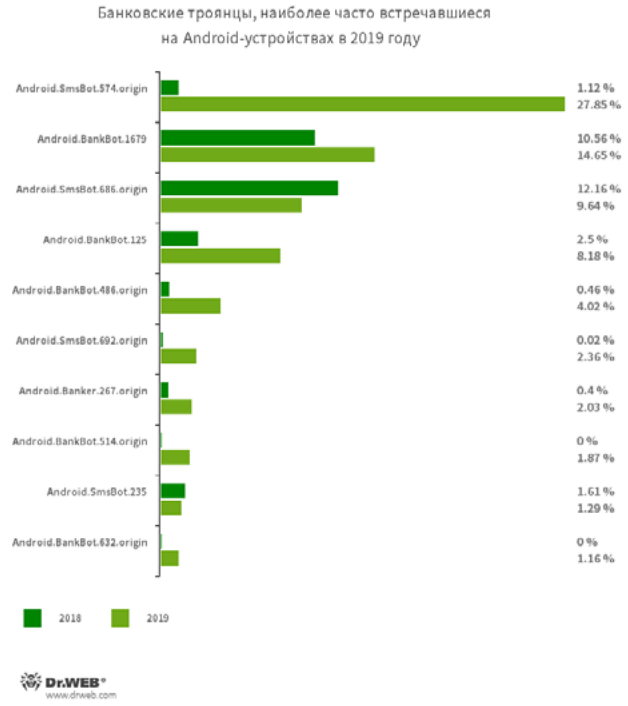
Adware.Patacore.168
Adware.Gexin.3.origin
Adware.Patacore.1.origin
Adware.AdPush.29.origin
Adware.Gexin.2.origin
Adware.Leadbolt.12.origin
Adware.Patacore.253

Рекламные модули, встраиваемые разработчиками ПО в приложения для их монетизации. Такие модули показывают надоедливые уведомления с объявлениями, баннеры и видеорекламу, которые мешают работе с устройствами. Кроме того, они могут собирать конфиденциальную информацию и передавать ее на удаленный сервер.

Банковские троянцы

Согласно статистике детектирований антивирусными продуктами Dr.Web для Android, за последние 12 месяцев банковские троянцы обнаруживались на Android-устройствах свыше 428 000 раз. Пик распространения этих вредоносных программ пришелся на первое полугодие, после чего их активность постепенно снижалась.

Чаще всего пользователям угрожали банкеры семейств Android.BankBot, Android.SmsBot и Android.Banker. Десять наиболее распространенных в прошедшем году Android-банкеров представлены на следующей диаграмме:



Android.SmsBot.574.origin
Android.SmsBot.686.origin
Android.SmsBot.692.origin

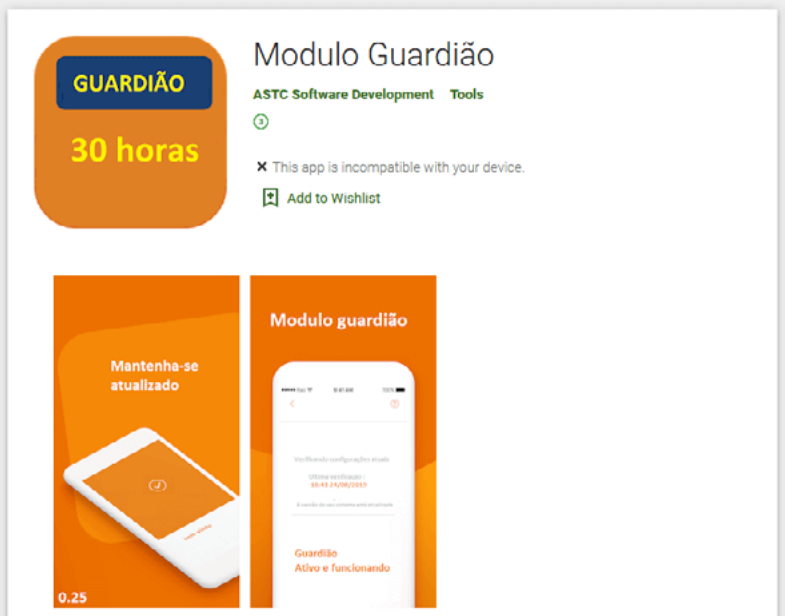
Банковские троянцы

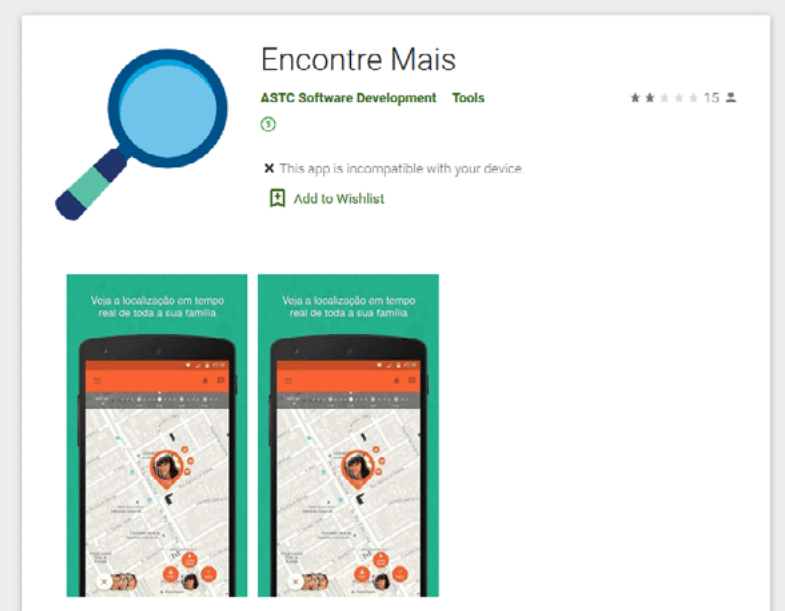
Android.SmsBot.235
Троянские программы, которые выполняют команды злоумышленников. Способны перехватывать и отправлять СМС-сообщения, демонстрировать мошеннические окна и уведомления, а также выполнять другие вредоносные действия. Многие из них используются для кражи денег с банковских карт.
Android.BankBot.1679
Android.BankBot.125
Android.BankBot.486.origin
Android.BankBot.514.origin
Android.BankBot.632.origin
Представители семейства многофункциональных банковских троянцев, способных выполнять широкий спектр вредоносных действий. Их основная задача — похищение логинов, паролей и другой ценной информации, необходимой для доступа к счетам пользователей.
Android.Banker.267.origin
Банкер, который показывает фишинговые окна и крадет конфиденциальные сведения.
Уже на протяжении нескольких лет пользователей атакуют различные модификации банковского троянца Flexnet, который по классификации Dr.Web относится к семейству Android.ZBot. Эта опасная вредоносная программа угрожала владельцам Android-устройств и в 2019 году. Вирусописатели распространяют ее при помощи СМС-спама, предлагая потенциальным жертвам загрузить и установить популярные игры и программы.
Попадая на устройства, Flexnet крадет деньги как с банковских счетов, так и со счетов мобильных телефонов. Для этого троянец проверяет баланс доступных счетов и отправляет несколько СМС-сообщений с командами на перевод денег. Таким образом злоумышленники могут не только выводить средства с карт жертв на свои карты, но и оплачивать различные услуги (например, хостинг-провайдеров) и совершать внутриигровые покупки в популярных играх. Подробнее об этом банкере рассказано в публикации нашей компании.
За последние 12 месяцев банковские троянцы атаковали жителей многих стран. Например, пользователям из Японии вновь угрожали многочисленные модификации троянцев семейства Android.Banker, которые киберпреступники распространяют через поддельные сайты почтовых компаний и курьерских служб доставки.

Банковские троянцы

В августе и октябре специалисты «Доктор Веб» выявили в Google Play банкеров Android.Banker.346.origin и Android.Banker.347.origin, предназначенных для владельцев Android-устройств из Бразилии. Эти опасные вредоносные приложения, представлявшие собой модификации обнаруженных в 2018 году троянцев, использовали специальные возможности (Accessibility Service) ОС Android. С их помощью они похищали информацию из СМС-сообщений, в которых могли быть одноразовые коды и другие конфиденциальные данные. Кроме того, по команде злоумышленников троянцы открывали фишинговые страницы.

Банковские троянцы

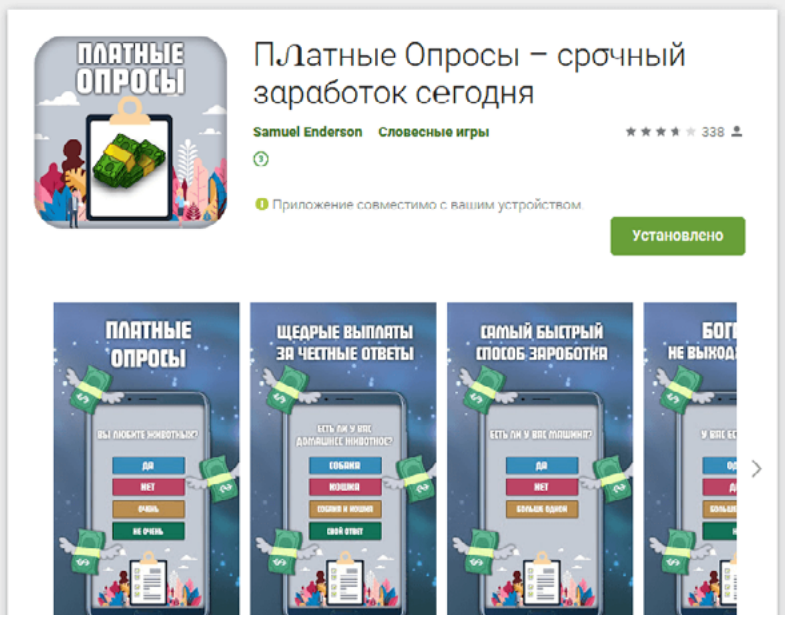




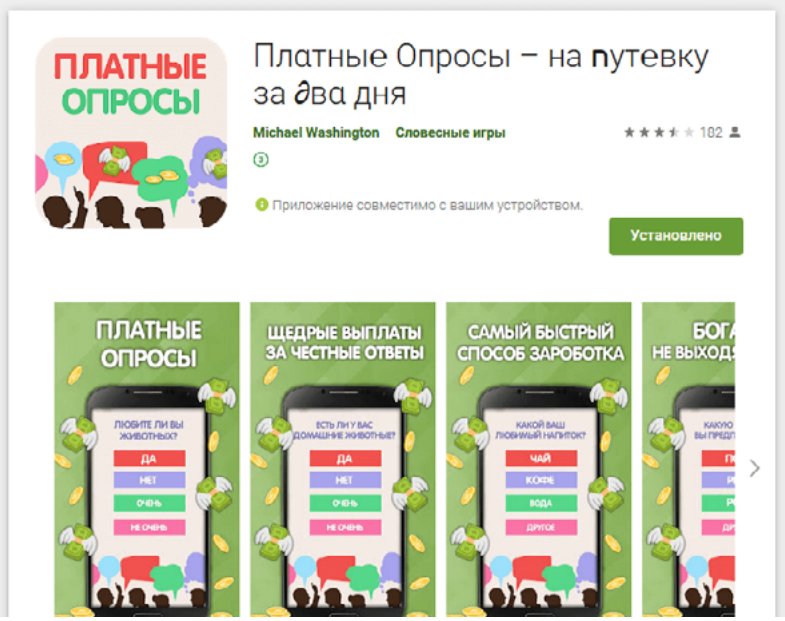
Мошенничество

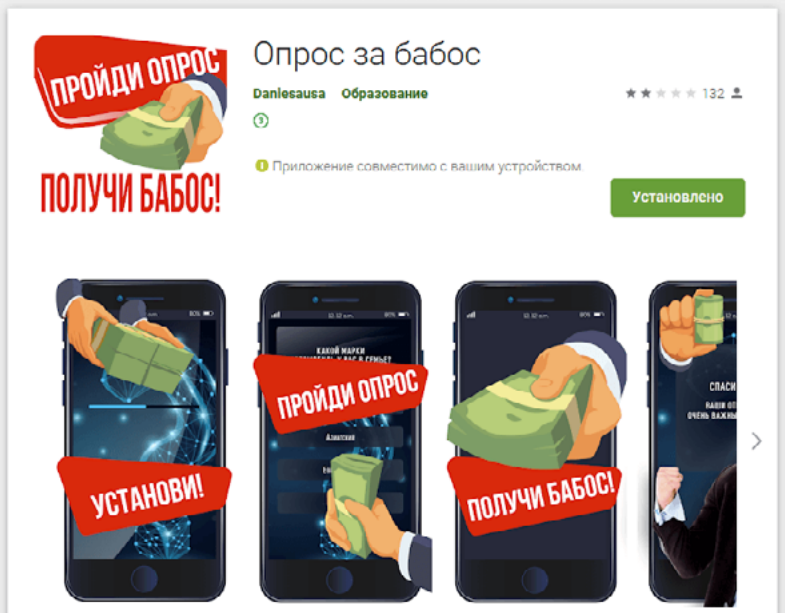
Киберпреступники продолжают использовать вредоносные программы в различных мошеннических схемах. Например, они создают троянцев, которые загружают веб-сайты, где потенциальным жертвам предлагается пройти тесты или принять участие в опросах, ответив на несколько простых вопросов. За это мошенники обещают пользователям денежное вознаграждение. Однако чтобы получить его, те якобы должны выполнить проверочный или иной платеж – например, для «подтверждения личности» или оплаты «комиссии» за перевод. На самом деле эти деньги поступают киберпреступникам, и жертвы не получают никакого вознаграждения.

Android-троянцы семейства Android.FakeApp, которые используются в этой схеме, получили широкое распространение еще в 2018 году, и за последние 12 месяцев наши вирусные аналитики вновь фиксировали их активность, которая выросла на 96,27%. Злоумышленники размещают большинство таких вредоносных приложений в каталоге Google Play, которому многие пользователи доверяют. Поэтому владельцы Android-устройств, которые ищут способы быстро и легко заработать, не догадываются, что устанавливают не безопасные программы, а троянцев.

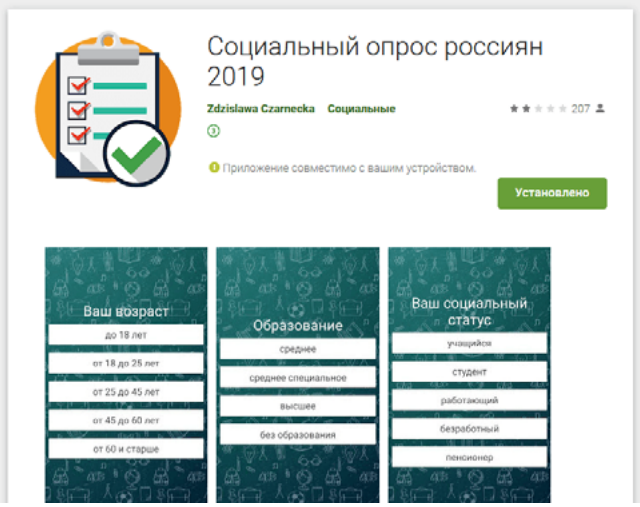


Мошенничество



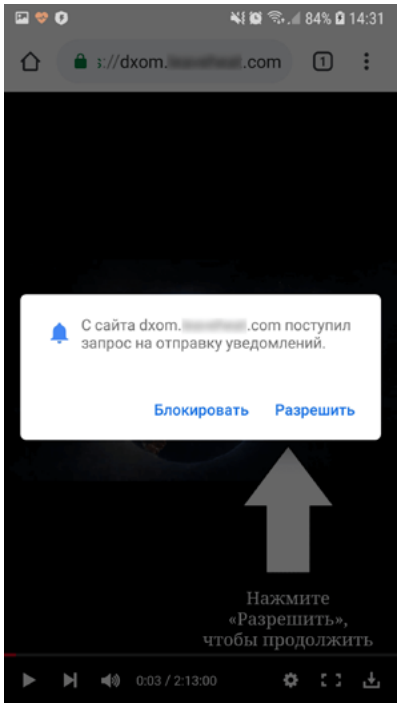


Мошенничество

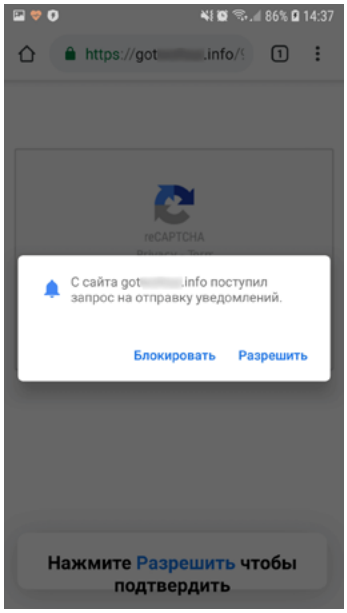


В начале лета специалисты компании «Доктор Веб» обнаружили другую вредоносную программу этого семейства, которая получила имя Android.FakeApp.174. Она распространялась под видом официальных приложений популярных магазинов.

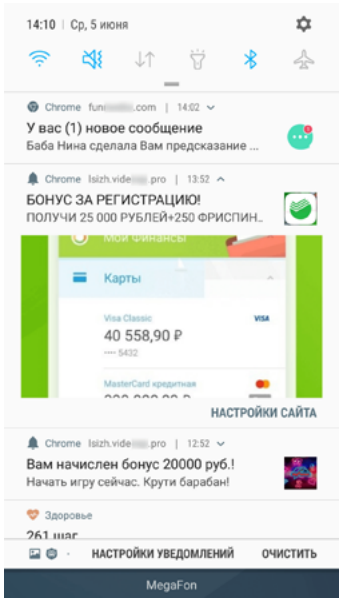
Android.FakeApp.174 загружал в браузере Google Chrome веб-сайты, с которых выполнялись перенаправления на страницы партнерских программ. Там под видом неких проверок пользователям предлагалось разрешить получать уведомления с этих сайтов.



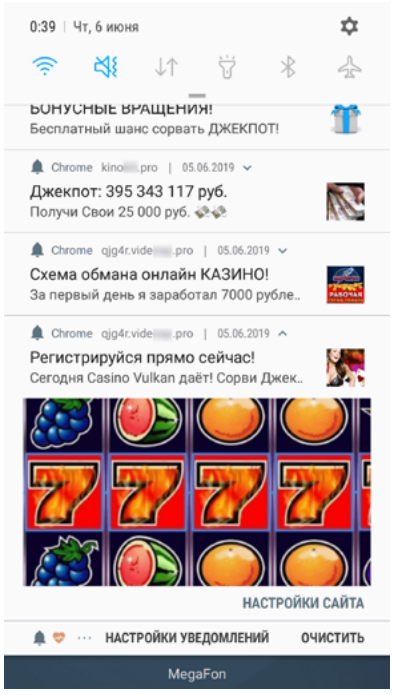
Мошенничество

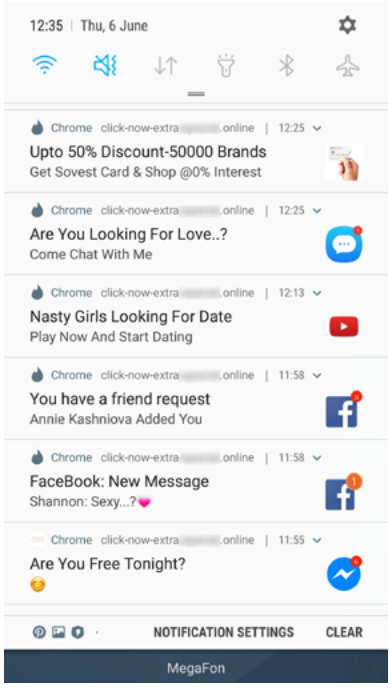


В случае согласия (и фактической подписки на веб-уведомления) жертвам начинали приходить многочисленные сообщения, часто похожие на уведомления от известных и надежных приложений или онлайн-сервисов, – например, банковских программ, социальных сетей и мессенджеров. При нажатии на такие сообщения владельцы устройств перенаправлялись на веб-сайты с сомнительным содержимым — онлайн-казино, мошенническими опросами, «розыгрышами призов» и т. п.

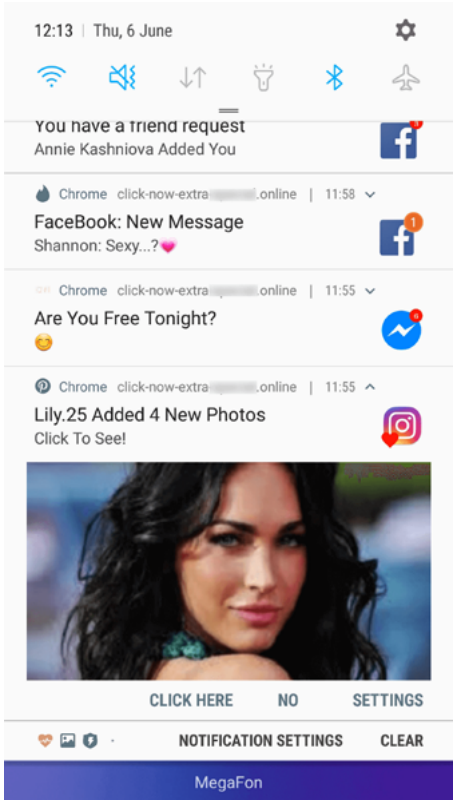


Мошенничество





Мошенничество



Перспективы и тенденции

В наступившем году одной из главных угроз для владельцев Android-устройств по-прежнему останутся банковские троянцы. Продолжится их эволюция и тенденция к трансформации многих из них в универсальные вредоносные программы, которые в зависимости от нужд киберпреступников будут решать самые разные вредоносные задачи. Дальнейшее развитие получат механизмы защиты троянцев и сокрытия вредоносного кода.

Злоумышленники продолжат организовывать таргетированные атаки, а пользователи вновь столкнутся с угрозой кибершпионажа и утечками конфиденциальных данных. Актуальной останется и проблема агрессивной рекламы. Появится больше вредоносных и нежелательных приложений, которые будут демонстрировать надоедливые баннеры и уведомления, а также троянцев, которые будут без спроса скачивать и пытаться установить рекламируемые приложения.

Возможно появление новых троянцев-майнеров и выявление новых случаев внедрения вредоносных программ в прошивки Android-устройств. Кроме того, пока в ОС Android не будут внесены изменения, продолжат появляться троянцы, эксплуатирующие специальные возможности (Accessibility Service) во вред пользователям.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2019 год

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.drweb.ru | www.антивирус.рф | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах