Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2018 год

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2018 год

28 декабря 2018 года

В уходящем году владельцам мобильных устройств под управлением ОС Android вновь угрожало большое число вредоносных и нежелательных программ, многие из которых распространялись через официальный каталог приложений Google Play. При этом заметно усилилась начавшаяся в 2017 году тенденция использования различных приемов маскировки и сокрытия троянцев для снижения вероятности их обнаружения.

Одной из главных угроз для пользователей смартфонов и планшетов за последние 12 месяцев стали Android-банкеры, атаковавшие клиентов кредитных организаций по всему миру. Кроме того, серьезную опасность представляли вредоносные программы, способные скачивать из Интернета и запускать произвольный код.

Вирусописатели активно распространяли троянцев, применявшихся в мошеннических схемах, а также задействовали другие вредоносные приложения, с помощью которых получали незаконный доход. Кроме того, злоумышленники снова пытались заработать «мобильной» добычей криптовалют и даже использовали троянцев-клиперов для подмены номеров электронных кошельков в буфере обмена Android-устройств.

Актуальной осталась проблема заражения прошивок смартфонов и планшетов на этапе их производства. Один из случаев внедрения троянца в образ операционной системы Android вирусные аналитики компании «Доктор Веб» выявили весной — тогда были скомпрометированы свыше 40 моделей мобильных устройств.

Также в течение года пользователям угрожали вредоносные приложения, использовавшиеся для кибершпионажа.

Главные тенденции года

- Очередные случаи проникновения троянских и нежелательных программ в каталог Google Play
- Попытки вирусописателей усложнить обнаружение вредоносных программ
- Атаки Android-банкеров на клиентов кредитных организаций по всему миру
- Использование троянцами специальных возможностей ОС Android для автоматического выполнения вредоносных действий
- Распространение троянцев-клиперов, подменяющих номера электронных кошельков в буфере обмена

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2018 год

Наиболее интересные события 2018 года

В начале года специалисты по информационной безопасности зафиксировали распространение троянца-майнера Android.CoinMine.15, заражавшего «умные» телевизоры, роутеры, телеприставки и другие устройства под управлением ОС Android. Он проникал на оборудование с использованием отладчика ADB (Android Device Bridge). Для этого Android.CoinMine.15 случайным образом генерировал IP-адреса и пытался подключиться к открытому порту 5555. В случае успеха троянец устанавливал на доступное устройство свою копию вместе со вспомогательными файлами, среди которых были и приложения-майнеры для добычи криптовалюты Monero (XMR).

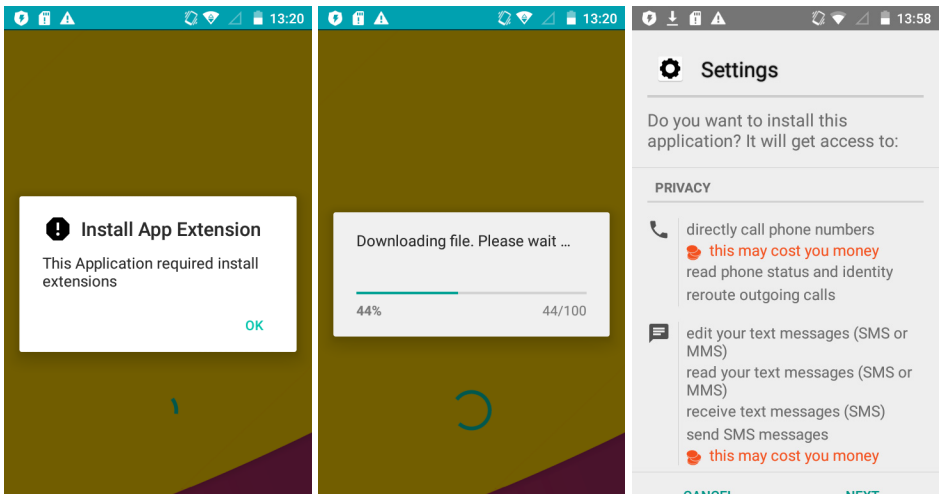
В марте компания «Доктор Веб» рассказала о новом случае обнаружения троянца Android.Triada.231 в прошивках более 40 моделей Android-смартфонов и планшетов. Неустановленные злоумышленники встроили Android.Triada.231 в одну из системных библиотек на уровне исходного кода, тогда как другие представители семейства Android.Triada обычно распространяются как отдельные приложения. Троянец внедряется в системный процесс Zygote, ответственный за старт программ. В результате Android.Triada.231 заражает остальные процессы и может скрыто выполнять вредоносные действия – например, загружать, устанавливать и удалять ПО без участия пользователя. Более подробные сведения о проведенном специалистами «Доктор Веб» расследовании этого случая доступны в соответствующем информационном материале.

Злоумышленники все чаще используют разнообразные методы, позволяющие уменьшить вероятность обнаружения вредоносных и нежелательных программ. В 2018 году эта тенденция сохранилась. Один из популярных способов снизить заметность — применение приложений-загрузчиков. Благодаря им троянцы и другое опасное ПО дольше остаются вне поля зрения антивирусов и вызывают меньше подозрений у потенциальных жертв. С помощью таких загрузчиков киберпреступники могут распространять вредоносное ПО различного типа – например троянцев-шпионов.

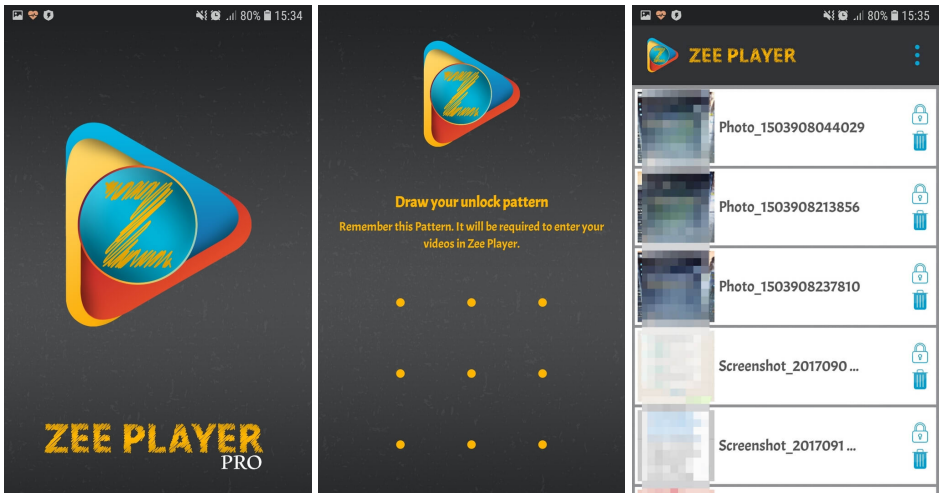
В апреле в каталоге Google Play был обнаружен загрузчик Android.DownLoader.3557, который скачивал на устройства и под видом важных плагинов предлагал пользователям установить вредоносные программы Android.Spy.443.origin и Android.Spy.444.origin. Они отслеживали местоположение зараженного смартфона или планшета, получали информацию обо всех доступных файлах, могли пересылать злоумышленникам документы жертвы, отправлять и красть СМС-сообщения, похищать данные из телефонной

Наиболее интересные события 2018 года

книги, записывать видео, прослушивать окружение при помощи встроенного в устройство микрофона, перехватывать телефонные звонки и совершать другие действия.



В августе в Google Play был найден загрузчик Android.DownLoader.784.origin, скачивавший троянца, предназначенного для кибершпионажа. Он получил имя Android.Spy.409.origin. Вирусописатели распространяли Android.DownLoader.784.origin под видом приложения Zee Player, которое позволяло скрывать хранящиеся в памяти мобильных устройств фотографии и видео. Программа была полностью работоспособной, поэтому у жертв злоумышленников не было причин заподозрить какой-либо подвох.

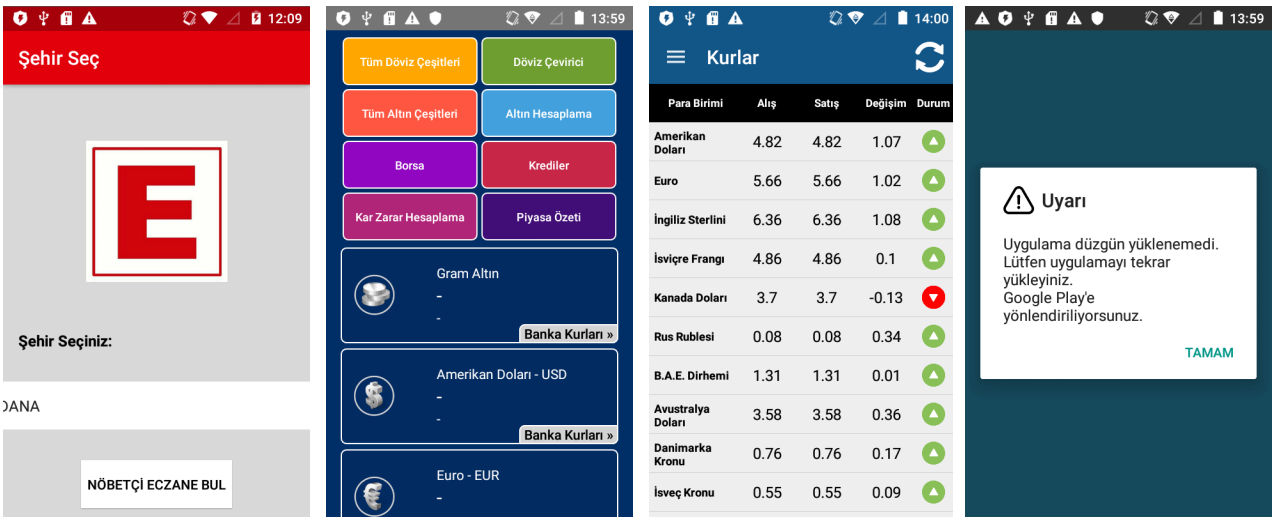


.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2018 год

Наиболее интересные события 2018 года

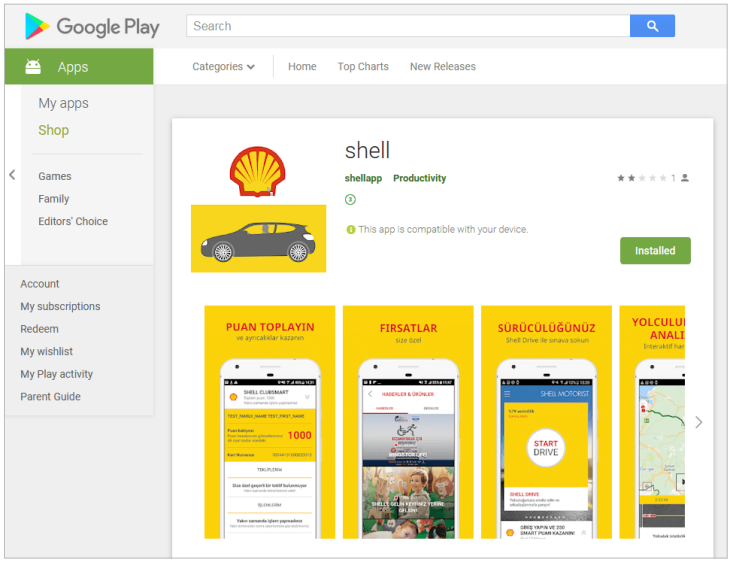
Однако все чаще троянцы-загрузчики используются для распространения Android-банкеров. В июле в Google Play был найден Android.DownLoader.753.origin, которого вирусописатели выдавали за финансовые приложения. Некоторые из них для большей убедительности действительно выполняли заявленные функции. Android.DownLoader.753.origin скачивал и пытался установить различных банковских троянцев, похищавших конфиденциальные данные.

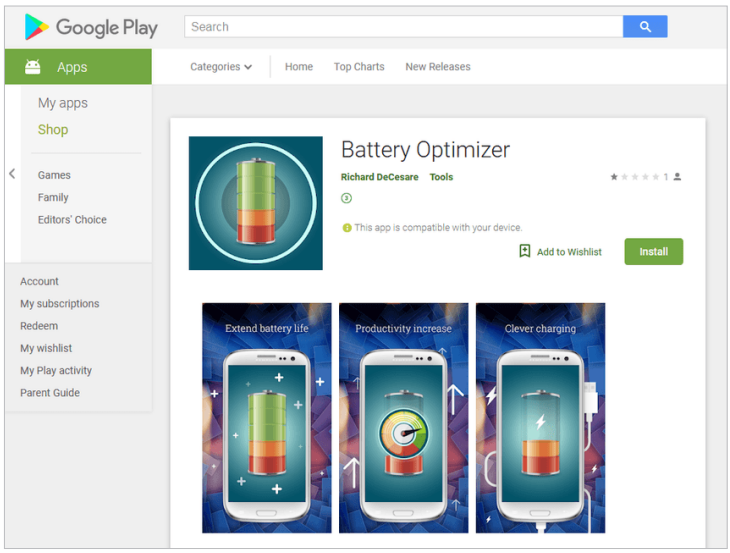


Позднее было выявлено несколько аналогичных вредоносных программ, которые также проникли в Google Play. Одна из них получила имя Android.DownLoader.768.origin — киберпреступники распространяли ее под видом официального ПО корпорации Shell. Другая, добавленная в вирусную базу Dr.Web как Android.DownLoader.772.origin, скрывалась под маской полезных утилит. Оба троянца также использовались для скачивания и установки Android-банкеров.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2018 год

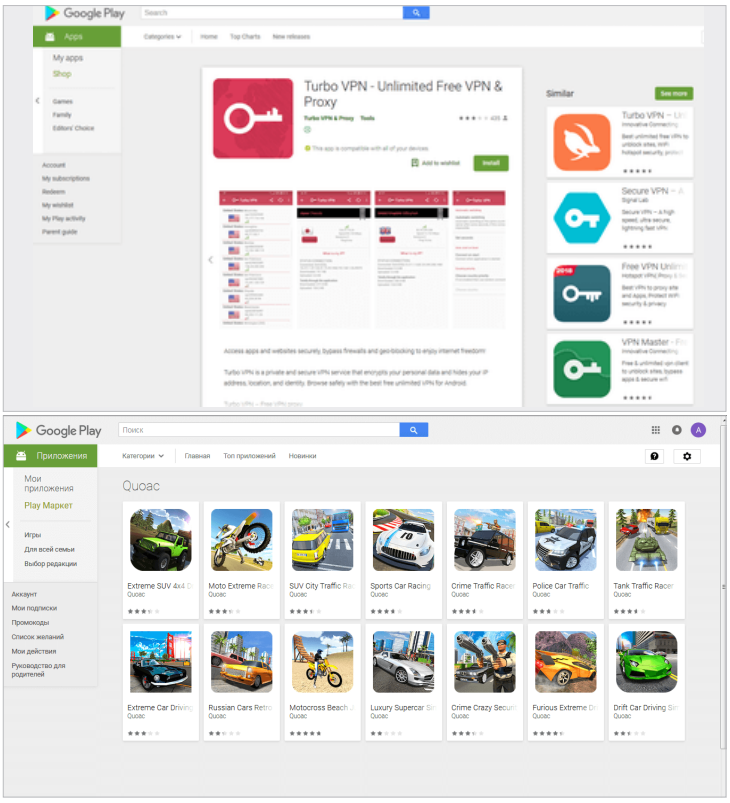
Наиболее интересные события 2018 года





Загрузчики применяются для заражения мобильных устройств и другим вредоносным ПО. В октябре вирусные аналитики обнаружили в каталоге Google Play троянца Android.DownLoader.818.origin, распространявшегося под видом VPN-клиента. Позже специалисты «Доктор Веб» выявили несколько его модификаций, которые скрывались в поддельных играх и получили имена Android.DownLoader.819.origin и Android.DownLoader.828.origin. Они предназначались для установки рекламных троянцев.

Наиболее интересные события 2018 года



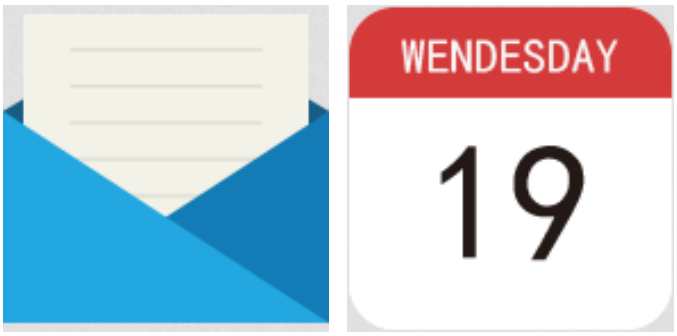
Все большее распространение получают многокомпонентные вредоносные приложения. Каждый из их модулей отвечает за выполнение определенных функций, что позволяет злоумышленникам при необходимости расширять возможности троянцев. Кроме того, такой механизм работы на зараженных мобильных устройствах снижает вероятность выявления угрозы. Вирусописатели способны оперативно обновлять эти плагины и добавлять к ним новые, оставляя основного троянца с минимальным набором функций и делая его менее заметным.

Подобный «комбайн» специалисты «Доктор Веб» обнаружили в феврале — он получил имя Android.RemoteCode.127.origin. Троянец, которого установили свыше 4 500 000 пользователей, незаметно скачивал и запускал вредоносные модули, выполнявшие разнообразные действия. Один из исследованных плагинов Android.RemoteCode.127.origin загружал собственное обновление, скрытое в обычном, на первый взгляд, изображении. Такой способ маскировки вредоносных объектов известен как стеганография. Он знаком специалистам по информационной безопасности уже давно, однако применяется вирусописателями редко.

После расшифровки и запуска модуль скачивал еще одно изображение, в котором скрывался другой плагин, загружавший и запускавший троянца Android.Click.221.origin. Тот незаметно открывал веб-сайты и нажимал на расположенные на них элементы —

Наиболее интересные события 2018 года

ссылки и баннеры, — накручивая счетчики посещений и зарабатывая деньги за рекламные «клики».
Примеры изображений с зашифрованными в них модулями Android.RemoteCode.127.origin:



Подробнее об этом троянце рассказано в новостном материале на нашем сайте.

Android.RemoteCode.152.origin — еще один многокомпонентный троянец, способный загружать и выполнять произвольный код. Его установили более 6 500 000 пользователей. Эта вредоносная программа незаметно скачивала и запускала вспомогательные модули, среди которых были рекламные плагины. С их помощью троянец создавал невидимые баннеры с объявлениями и нажимал на них, принося вирусописателям прибыль.

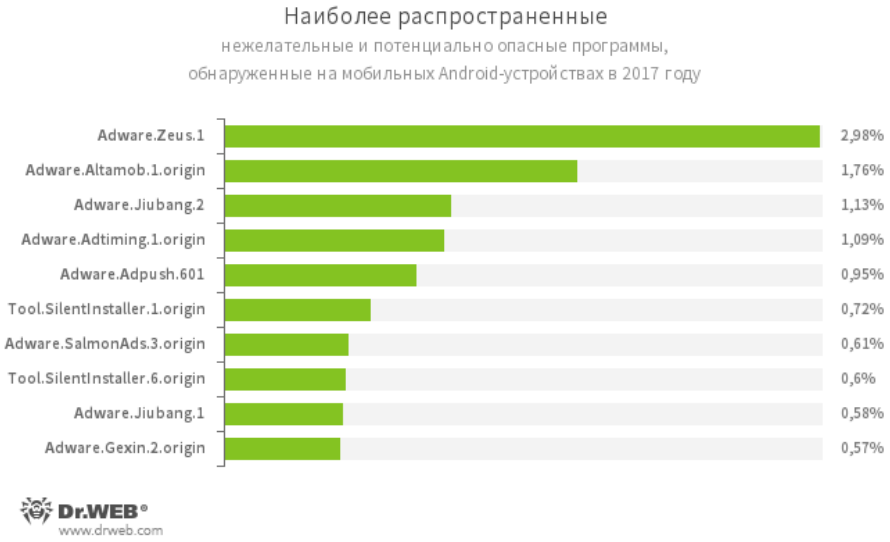
В августе аналитики «Доктор Веб» исследовали троянца-клипера Android.Clipper.1.origin, а также его модификацию Android.Clipper.2.origin. Эта вредоносная программа подменяла в буфере обмена номера электронных кошельков платежных систем «Яндекс.Деньги», Qiwi и Webmoney (R и Z), а также криптовалют Bitcoin, Litecoin, Etherium, Monero, zCash, DOGE, DASH и Blackcoin. Вирусописатели распространяли троянца под видом известных и безобидных приложений.

При копировании номера электронного кошелька в буфер обмена Android.Clipper.1.origin перехватывал его и передавал на управляющий сервер. В ответ вредоносная программа получала информацию о номере кошелька злоумышленников, на который троянец заменял номер в буфере обмена. В результате, если пользователь не замечал подмену, он переводил деньги на счет киберпреступников. Подробная информация об Android.Clipper.1.origin доступна в новостной публикации на сайте компании «Доктор Веб».

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2018 год

Вирусная обстановка в сегменте мобильных устройств

Согласно статистике детектирований антивирусными продуктами Dr.Web для Android, в 2018 году на Android-устройствах чаще всего обнаруживались рекламные троянцы, вредоносные программы, скачивающие опасное и ненужное ПО, а также троянцы, выполняющие по команде злоумышленников различные действия.



Android.Backdoor.682.origin

Троянец, выполняющий по команде киберпреступников вредоносные действия.

Android.Mobifun.4

Представители семейства троянцев, предназначенных для показа навязчивой рекламы.

Android.HiddenAds

Представители семейства троянцев, предназначенных для показа навязчивой рекламы.

Android.DownLoader.573.origin

Вредоносная программа, выполняющая загрузку заданных вирусописателями приложений.

Android.Packed.15893

Детектирование троянцев, защищенных программным упаковщиком.

Android.Xiny.197

Троянец, основная задача которого — загрузка и удаление приложений.

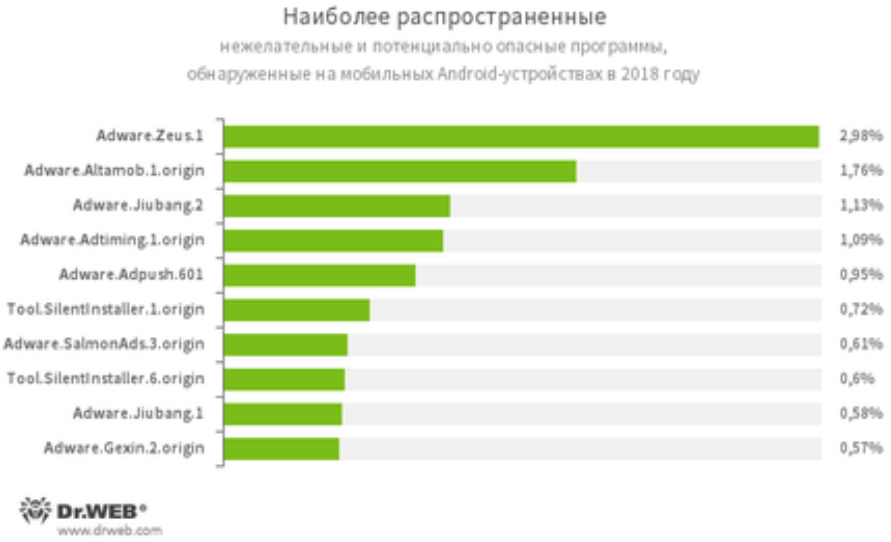
Android.Altamob.1.origin

Вредоносная программа, выполняющая загрузку заданных вирусописателями приложений.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2018 год

Вирусная обстановка в сегменте мобильных устройств

Среди нежелательных и потенциально опасных приложений, обнаруженных на Android-устройствах в течение года, самыми распространенными оказались модули, показывающие рекламу. Кроме того, на смартфонах и планшетах детектировались программы, предназначенные для загрузки и установки различного ПО.



Adware.Zeus.1
Adware.Altamob.1.origin
Adware.Jiubang
Adware.Adtiming.1.origin
Adware.Adpush.601
Adware.SalmonAds.3.origin
Adware.Gexin.2.origin

Нежелательные модули, которые разработчики ПО и вирусописатели встраивают в приложения для показа агрессивной рекламы.

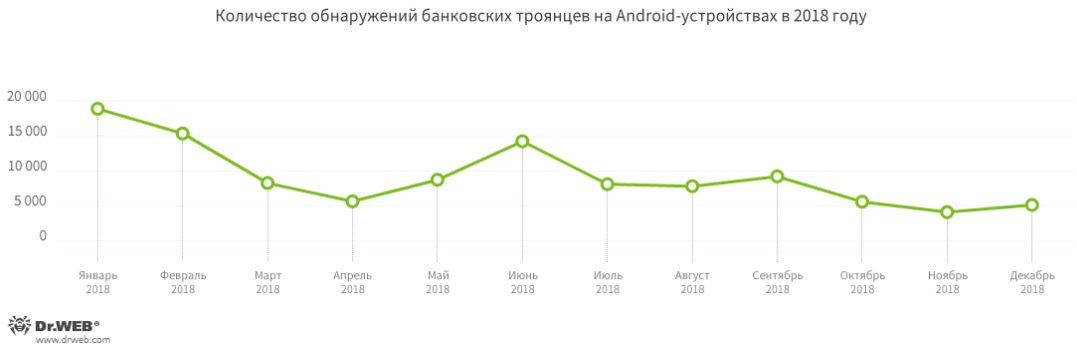
Tool.SilentInstaller.1.origin
Tool.SilentInstaller.6.origin

Потенциально опасные программы, предназначенные для загрузки и установки других приложений.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2018 год

Банковские троянцы

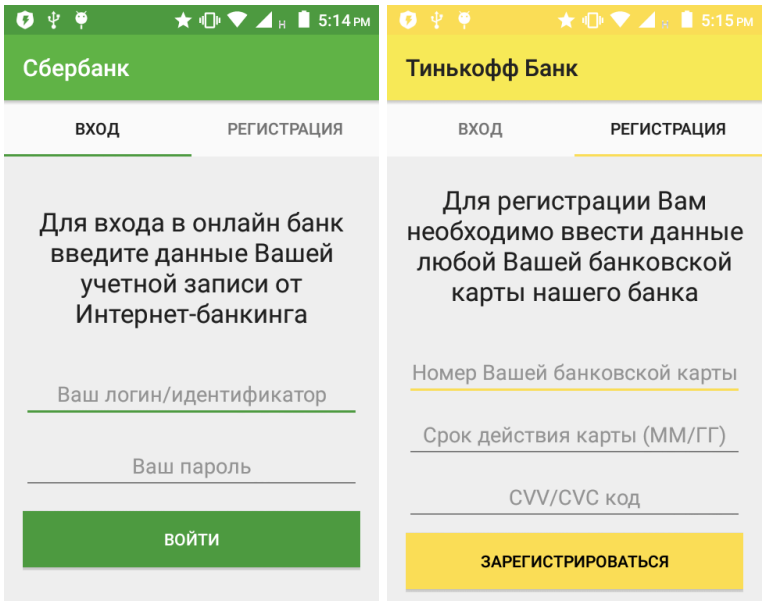
Банковские троянцы по-прежнему представляют серьезную опасность для владельцев мобильных устройств. Эти вредоносные приложения похищают логины и пароли доступа к учетным записям клиентов кредитных организаций, информацию о банковских картах и другие конфиденциальные данные, которые могут использоваться для кражи денег. В течение последних 12 месяцев антивирусные продукты Dr.Web для Android обнаруживали таких троянцев на смартфонах и планшетах свыше 110 000 раз. Динамика детектирования Android-банкеров показана на следующем графике:



Когда в конце 2016 года авторы банковского троянца Android.BankBot.149.origin опубликовали его исходный код, специалисты компании «Доктор Веб» спрогнозировали появление множества вредоносных программ, созданных на его основе. Это предположение оказалось верным: вирусописатели активно приступили к производству похожих банкеров, одновременно совершенствуя их и добавляя новые функции. Одним из таких троянцев, которые злоумышленники распространяли в 2018 году, был Android.BankBot.250.origin, а также его обновленная и еще более опасная версия Android.BankBot.325.origin. Этот банкер, известный под именем Anubis, является многофункциональным вредоносным приложением. Оно не только крадет конфиденциальные данные и деньги пользователей, но и способно выполнять множество команд. Кроме того, с его помощью киберпреступники могут получать дистанционный доступ к зараженным устройствам, применяя Android.BankBot.325.origin как утилиту удаленного администрирования. С деталями исследования этого троянца можно ознакомиться в соответствующем материале на нашем сайте.

В марте специалисты «Доктор Веб» обнаружили в Google Play троянца Android.BankBot.344.origin, скрывавшегося в приложении под названием «ВСЕБАНКИ – Все банки в одном месте». Злоумышленники выдавали его за универсальное приложение для работы с системами онлайн-банкинга нескольких российских кредитных организаций.

Банковские троянцы

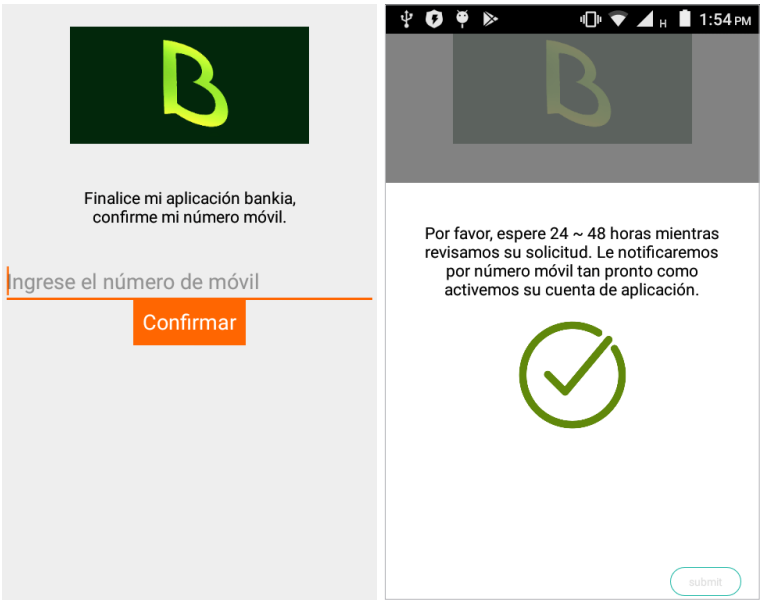


При запуске Android.BankBot.344.origin предлагал потенциальной жертве войти в уже существующую банковскую учетную запись, указав логин и пароль, либо зарегистрироваться, предоставив сведения о банковской карте. Вводимая информация передавалась кибержуликам, после чего те могли украсть деньги со скомпрометированного счета.

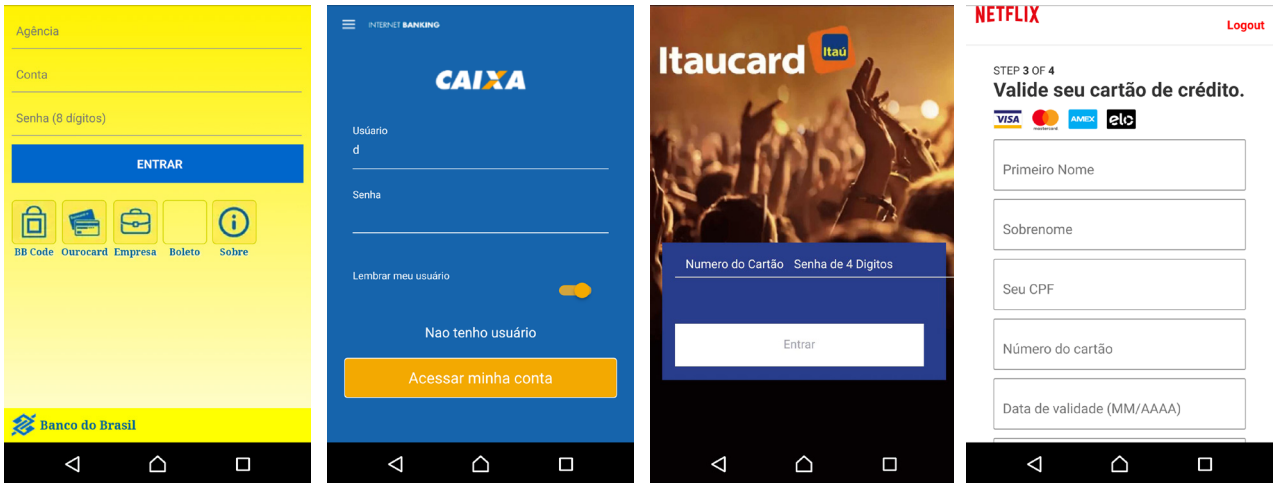
Осенью вирусные аналитики исследовали банкера Android.Banker.2876, который также распространялся через каталог Google Play и атаковал клиентов кредитных учреждений Испании, Франции и Германии. Он отображал фишинговое окно и предлагал потенциальной жертве указать ее номер телефона, после чего передавал его вирусописателям. Затем Android.Banker.2876 начинал перехватывать СМС-сообщения и отправлял их содержимое злоумышленникам. Благодаря этому те могли получать одноразовые коды подтверждения финансовых операций и красть деньги пользователей.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2018 год

Банковские троянцы



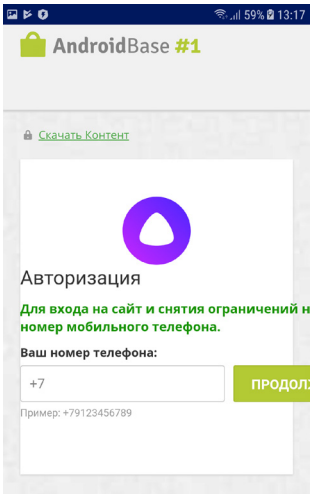
Вскоре наши специалисты выявили в Google Play троянца Android.BankBot.495.origin, предназначенного для пользователей из Бразилии. Android.BankBot.495.origin задействовал специальные возможности ОС Android. С их помощью он считывал содержимое окон работающих приложений, передавал злоумышленникам конфиденциальные данные, а также самостоятельно нажимал на кнопки и управлял атакованными программами. Кроме того, троянец показывал мошеннические окна, в которых запрашивал логины, пароли, номера кредитных карт и другую секретную информацию.

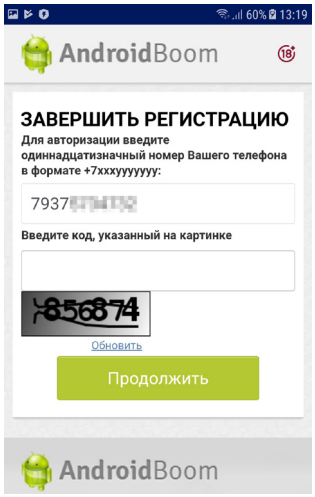


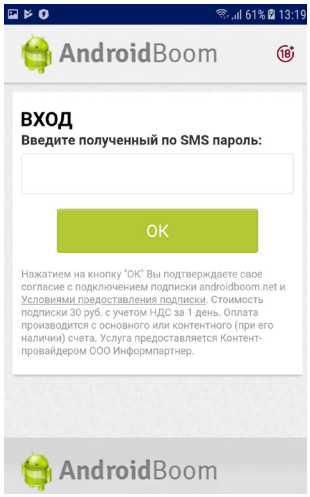
«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2018 год

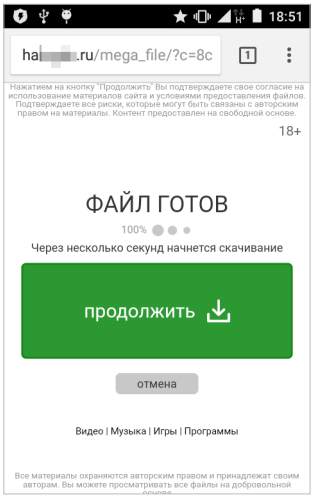
Мошенничество

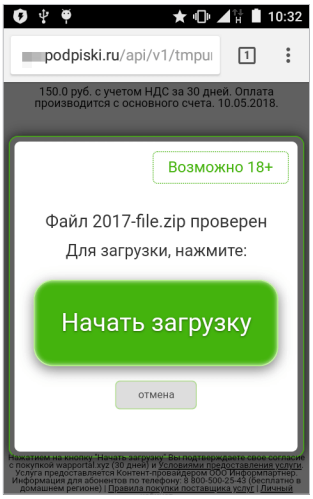
Проводя мошеннические кампании, киберпреступники все чаще используют вредоносные программы для мобильных Android-устройств. В 2018 году было выявлено множество таких троянцев. Об одном из них — Android.Click.245.origin — компания «Доктор Веб» рассказывала в апреле. Он распространялся под видом известных приложений, однако занимался лишь загрузкой мошеннических веб-страниц. На них потенциальным жертвам предлагалось скачать то или иное ПО, указав для этого номер мобильного телефона. После ввода номера жертве приходило СМС-сообщение с кодом подтверждения, который был якобы необходим для завершения загрузки приложения. Однако вводя полученный код на сайте, пользователь подписывался на платную услугу. Если же владелец зараженного устройства был подключен к Интернету через мобильную сеть, при нажатии на поддельную кнопку загрузки оформление дорогостоящей услуги происходило автоматически с использованием технологии Wap-Click. Пример таких веб-сайтов показан ниже:







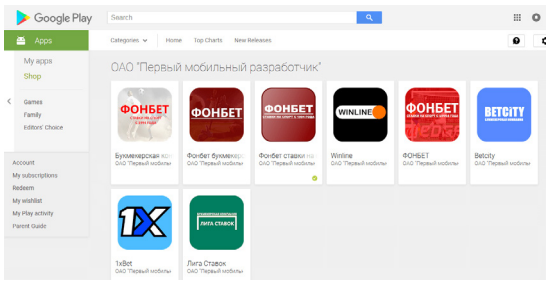


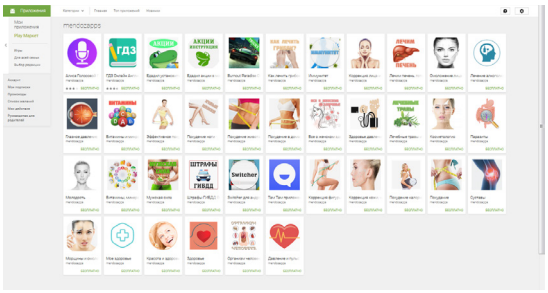


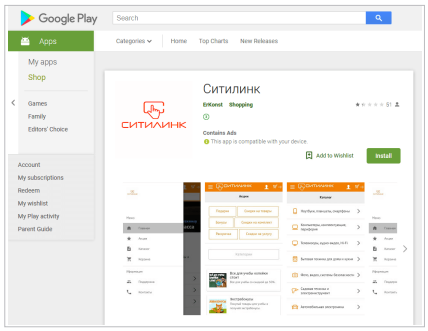
«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2018 год

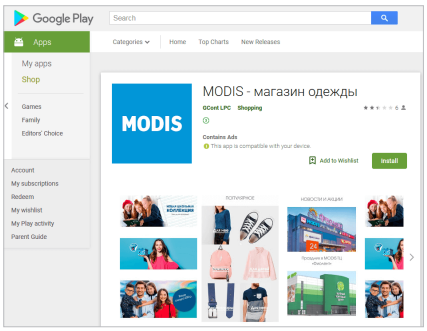
Мошенничество

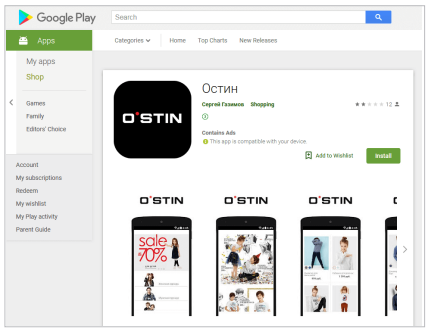
На протяжении года наши специалисты находили в Google Play и других троянцев, способных по команде управляющего сервера загружать любые веб-страницы. Среди них были Android.Click.415, Android.Click.416, Android.Click.417, Android.Click.246.origin, Android.Click.248.origin, Android.Click.458 и ряд других. Они также распространялись под видом полезных программ — сборников рецептов, различных пособий, голосовых помощников, игр и даже букмекерских приложений.











Кроме того, злоумышленники активно распространяли Android-троянцев семейства Android.FakeApp, которые загружали мошеннические сайты с размещенными на них поддельными опросами. Пользователям предлагалось ответить на несколько простых вопросов, за что киберзулики обещали солидное денежное вознаграждение. Для получения оплаты от потенциальной жертвы требовалось выполнить некий проверочный или иной платеж. Однако после перевода средств мошенникам владелец зараженного устройства не получал никаких денег.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2018 год

Мошенничество

В течение года вирусные аналитики обнаружили десятки мошеннических приложений Android.FakeApp и Android.Click, которые в общей сложности установили не менее 85 000 владельцев Android-смартфонов и планшетов. Более детально о некоторых из этих троянцев компания «Доктор Веб» рассказывала в отдельном информационном материале.

Перспективы и тенденции

В следующем году пользователи мобильных устройств вновь столкнутся с атаками банковских троянцев, а вирусописатели продолжат улучшать их функционал. Вполне вероятно, что все большее число Android-банкеров будет становиться универсальными вредоносными программами, способными выполнять широкий спектр задач.

Возрастет число мошеннических приложений и рекламных троянцев. Также вирусописатели не оставят попыток заработать на добыче криптовалют, используя вычислительные мощности Android-устройств. Нельзя исключать очередных случаев заражения прошивок.

Киберпреступники будут совершенствовать способы обхода антивирусов, встроенных в операционную систему Android новых ограничений и защитных механизмов. Не исключено появление руткитов и троянцев, способных обходить эти барьеры. Возможно возникновение вредоносных программ с новыми принципами работы и способами получения конфиденциальной информации. Например, использование датчиков мобильного устройства и слежение за движениями глаз для получения информации о набираемом тексте. Кроме того, в новых вредоносных приложениях злоумышленники могут применять алгоритмы машинного обучения и другие методы искусственного интеллекта.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2018 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.антивирус.рф | www.drweb.ru | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах

© ООО «Доктор Веб»,
2003-2018

Узнайте больше
Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека