Dr.WEB®
с 1992 года

Обзор вирусной активности для мобильных устройств за 2016 год

Обзор вирусной активности для мобильных устройств за 2016 год

29 декабря 2016 года

В 2016 году пользователи ОС Android вновь столкнулись с большим числом угроз. На протяжении последних 12 месяцев злоумышленники распространяли банковских троянцев, один из которых сумел заразить почти 40 000 смартфонов и планшетов по всему миру. Были выявлены новые вредоносные приложения, встроенные киберпреступниками в прошивку десятков моделей Android-устройств. Появились Android-троянцы, способные заражать запущенные процессы и системные библиотеки. Кроме того, в каталог Google Play попало множество новых вредоносных приложений. Также в 2016 году вирусописатели распространяли троянцев, которые показывали агрессивную рекламу, пытались получить root-полномочия и незаметно устанавливали ПО. Были обнаружены и новые вредоносные программы для iOS.

Главные тенденции года

- Рост числа вредоносных и нежелательных программ, которые показывали рекламу, а также незаметно скачивали и устанавливали ненужные приложения
- Появление Android-троянцев, заражающих процессы и системные библиотеки ОС Android
- Обнаружение новых троянцев, предустановленных на мобильные устройства
- Развитие Android-банкеров и увеличение количества атак на клиентов кредитных организаций из множества стран
- Появление новых троянцев в каталоге Google Play
- Обнаружение новых вредоносных и нежелательных программ для iOS

Обзор вирусной активности для мобильных устройств за 2016 год

«Мобильная» угроза месяца

Операционная система Android по-прежнему остается самой популярной платформой, на которой работает множество современных мобильных устройств. Поэтому в 2016 году киберпреступники вновь сконцентрировали атаки именно на пользователях Android-смартфонов и планшетов. Большинство вредоносных и нежелательных программ, с помощью которых вирусописатели заражали Android-устройства, применялись для получения незаконной прибыли. При этом интерес злоумышленников к популярным ранее СМС-троянцам продолжил снижаться, и основным источником их заработка все чаще становились вредоносные программы с другой моделью монетизации. Эта тенденция начала прослеживаться еще в 2015 году.

Широкое распространение получили троянцы, показывающие агрессивную рекламу. Они отображают баннеры поверх работающих приложений, помещают сообщения в панель уведомлений, создают ярлыки на главном экране операционной системы, загружают заданные вирусописателями веб-страницы и открывают определенные разделы в каталоге Google Play.

Другой популярный способ обогащения киберпреступников заключается в загрузке и установке троянцами программ без разрешения владельцев зараженных устройств, когда за каждую успешную установку вирусописатели получают оплату. Для незаметной работы многие такие вредоносные приложения пытаются получить root-полномочия и копируют себя в системные каталоги. А некоторые из них злоумышленники встраивают непосредственно в прошивку мобильных устройств. Кроме того, появились троянцы, которые заражают процессы системных приложений, после чего обретают расширенные полномочия и могут скрытно устанавливать ПО. Такие вредоносные программы были обнаружены в феврале 2016 года. А в декабре вирусные аналитики «Доктор Веб» исследовали новые версии этих троянцев, научившиеся заражать не только процессы приложений, но и системные библиотеки.

Согласно статистике детектирований антивирусными продуктами Dr.Web для Android, в 2016 году на Android-смартфонах и планшетах чаще всего обнаруживался троянец Android.Xiny.26.origin, который при помощи эксплойтов пытался получить на заражаемом мобильном устройстве root-доступ и без разрешения пользователя скачивал и устанавливал программы. Кроме того, он показывал рекламу. На второй строчке расположился троянец Android.Callpay.1.origin. Он предоставлял владельцам Android-устройств доступ к эротическим материалам, но в качестве оплаты этой услуги незаметно совершал звонки на премиум-номера. На третьем месте по числу детектирований оказались троянцы, которые антивирусные продукты Dr.Web для Android определяют с использованием вирусной записи Android.Packed.1. Такие приложения защищены программными упаковщиками и могут совершать самые разные вредоносные действия.

Обзор вирусной активности для мобильных устройств за 2016 год

- **Android.Sprovider.1**
  Троянец, который загружает на мобильные Android-устройства различные приложения и пытается их установить. Кроме того, он может показывать рекламу.
- **Android.Backdoor.279.origin**
  Многофункциональный троянец-бэкдор для ОС Android, который получает команды от злоумышленников и выполняет широкий спектр задач.
- **Android.Banker.70.origin**
  Представитель семейства банковских троянцев, которые крадут конфиденциальную информацию и похищают деньги со счетов пользователей.
- **Android.DownLoader**
  Семейство троянцев, которые загружают и пытаются установить на мобильные Android-устройства другие вредоносные приложения.
- **Android.BankBot.75.origin**
  Представитель семейства банковских троянцев, предназначенных для кражи конфиденциальной информации и похищения денег.

Эта статистика говорит о том, что среди выявленных на Android-смартфонах и планшетах вредоносных программ наибольшее распространение в 2016 году получили рекламные троянцы, а также троянцы, которые загружали на мобильные устройства и пытались установить ненужные приложения.

Аналогичная ситуация наблюдается и согласно статистике обнаружений нежелательно-

го и потенциально опасного ПО. В 2016 году на Android-устройствах чаще всего детектировались нежелательные приложения и программные модули, предназначенные для показа агрессивной рекламы. Первую строчку среди них занял рекламный модуль Adware.WalkFree.1.origin, на втором месте расположился Adware.Leadbolt.12.origin, а на третьем — Adware.Airpush.31.origin. Десять наиболее распространенных нежелательных приложений, обнаруженных в 2016 году на Android-смартфонах и планшетах, показаны на следующей диаграмме:

- **Adware.AdMogo.2.origin**
- **Adware.Cosiloon.1**
- **Adware.DuMobove.1**
- **Adware.Revmob.1.origin**

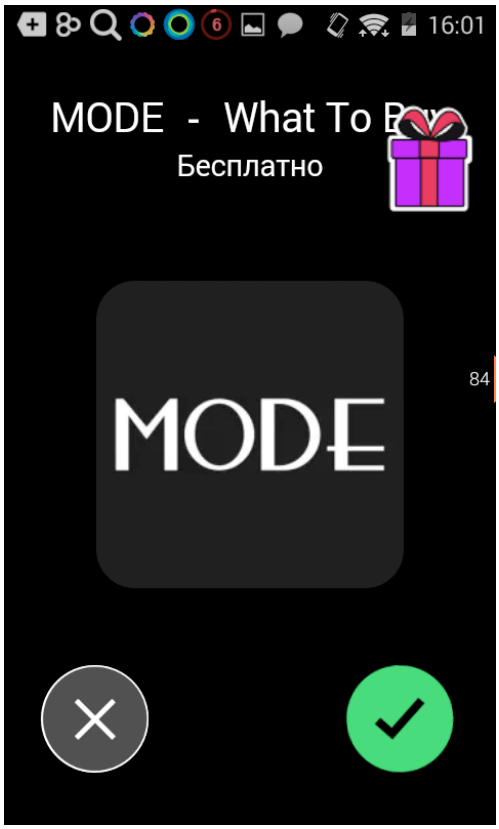
  Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

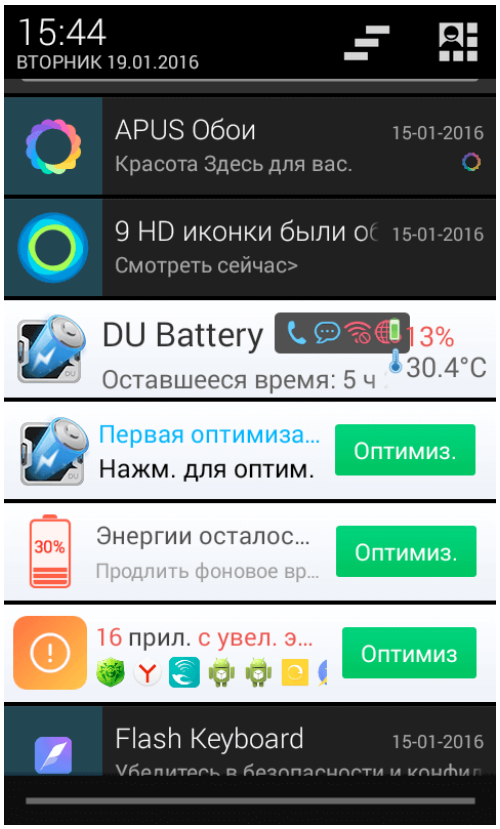
Большинство рекламных модулей для ОС Android показывают баннеры, всплывающие окна и сообщения в панели уведомлений мобильных устройств. Однако многие из них могут также загружать приложения и предлагать пользователям их установить.

Судя по всему, в следующем году популярность троянцев и нежелательных программ, которые показывают рекламу и без разрешения загружают на устройства программы, продолжит расти.

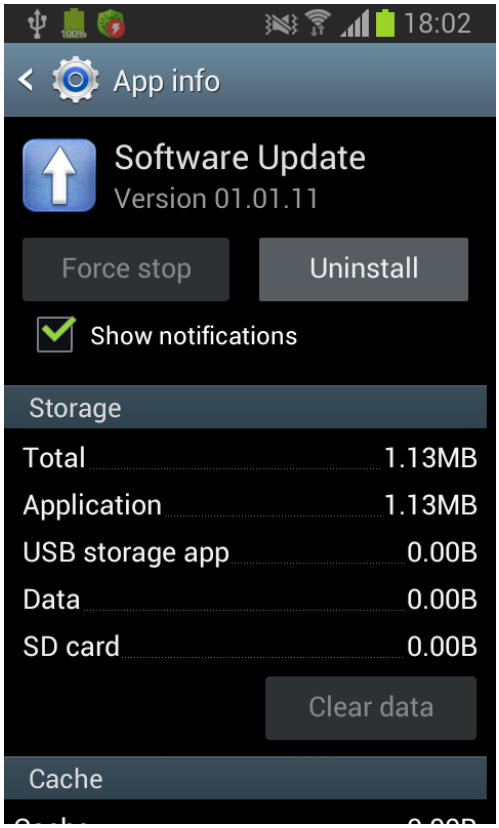
Предустановленные троянцы

Вредоносные программы, которые киберпреступники внедряют в прошивку мобильных устройств под управлением ОС Android, обладают системными полномочиями и могут без разрешения пользователей выполнять множество действий – например, они способны незаметно скачивать, устанавливать и удалять приложения. В 2016 году вирусные аналитики компании «Доктор Веб» зафиксировали сразу несколько новых случаев предустановки Android-троянцев на смартфоны и планшеты. Так, в середине января на одной из популярных моделей Android-устройств был выявлен троянец Android.Cooee.1. Он представлял собой созданную вирусописателями графическую оболочку со встроенным в нее рекламным модулем. Android.Cooee.1 показывал рекламу, незаметно загружал и запускал дополнительные рекламные плагины, а также приложения, среди которых были и вредоносные.





Уже в марте специалисты «Доктор Веб» обнаружили троянца Android.Gmobi.1. Он был предустановлен на нескольких десятках моделей мобильных устройств, а также распространялся в составе приложений TrendMicro Dr.Safety, TrendMicro Dr.Booster и Asus WebStorage, размещенных в катале Google Play. Троянец представлял собой программную платформу (SDK), которую использовали производители смартфонов и планшетов, а также разработчики ПО.



Эта платформа позволяла выполнять дистанционное обновление операционной системы, собирала аналитические данные, показывала различные уведомления, а также использовалась для мобильных платежей. Однако помимо безобидных функций она имела и вредоносные. Например, Android.Gmobi.1 показывал рекламу, создавал ярлыки на главном экране ОС, открывал различные страницы в веб-браузере и в приложении Google Play, а также мог загружать, устанавливать и запускать ПО. Кроме того, этот троянец передавал конфиденциальную информацию на управляющий сервер.

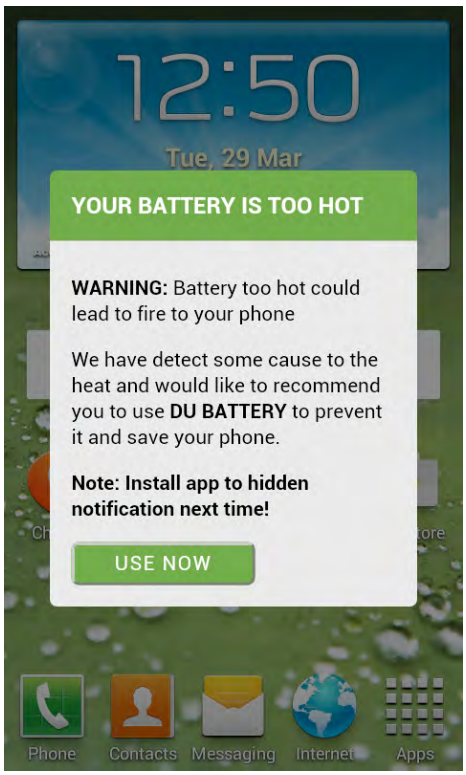
В ноябре был обнаружен троянец Android.Spy.332.origin, который изначально представлял собой системное ПО для обновления прошивки и ранее не был вредоносным приложением. Однако в новой версии в нем появился троянский функционал. Android.Spy.332.origin мог незаметно скачивать, устанавливать и удалять программы, выполнять shell-команды, а также передавал на управляющий сервер конфиденциальную информацию, в том числе сведения об СМС-сообщениях, телефонных звонках и ряд технических данных о зараженном мобильном устройстве. После того как этот случай получил широкую огласку в СМИ, некоторые производители выпустили обновление операционной системы, в котором этот троянец уже отсутствовал.

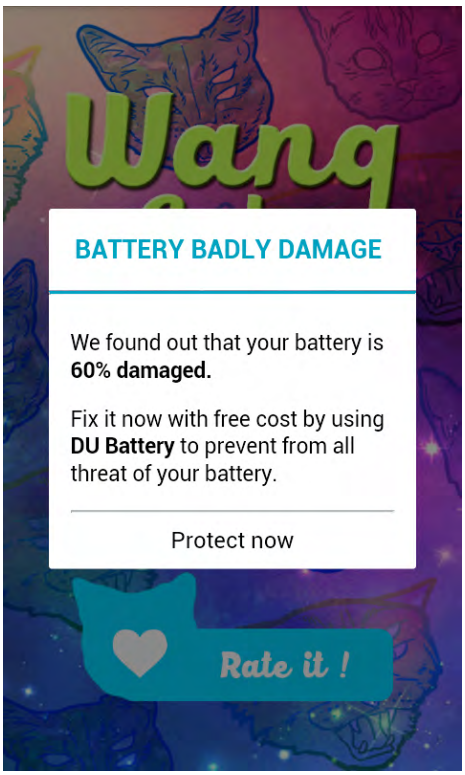
Поскольку внедрение троянцев и других нежелательных приложений в системный каталог Android-смартфонов и планшетов позволяет злоумышленникам незаметно выполнять любые действия, в будущем году, вероятно, снова обнаружатся мобильные устройства, на которых будут предустановлены троянцы.

Троянцы в Google Play

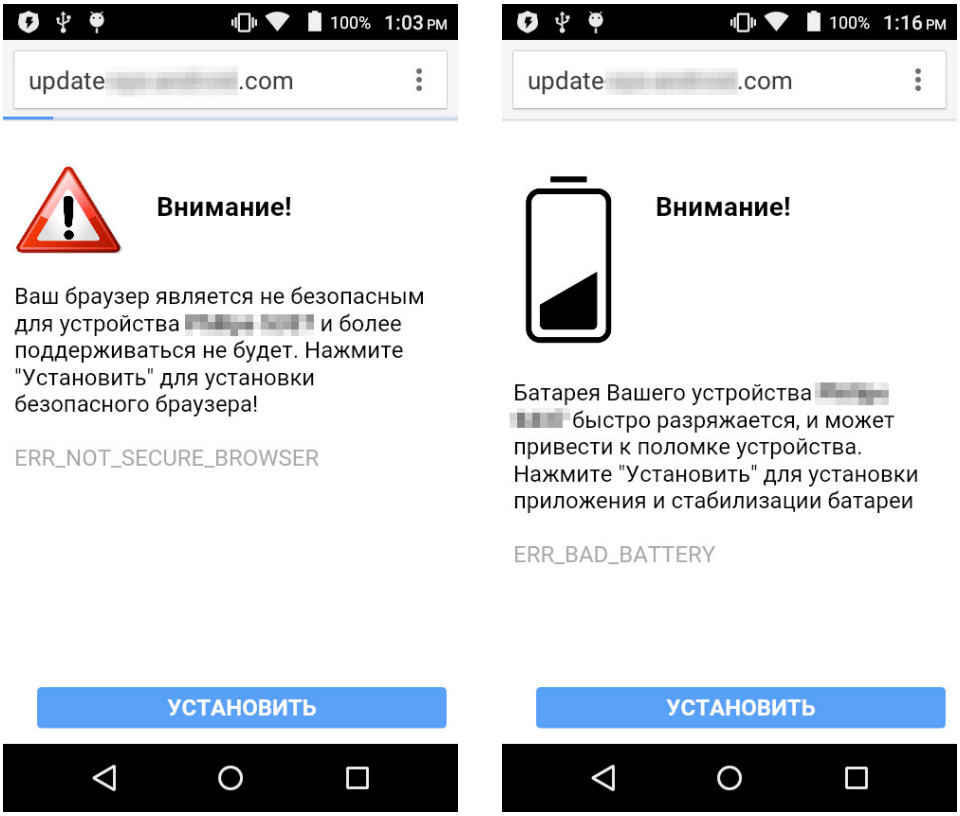
Каталог цифрового контента Google Play является самым надежным источником программ и игр для мобильных устройств под управлением ОС Android. Однако вирусописатели по-прежнему обходят его защитные механизмы и распространяют через него троянцев. В 2016 году было зафиксировано множество таких случаев. Например, еще в начале января в Google Play был найден троянец Android.Click.47.origin, встроенный, на первый взгляд, в безобидные приложения. При запуске Android.Click.47.origin скачивал с управляющего сервера список веб-страниц, которые он незаметно открывал. Затем троянец автоматически переходил по всем доступным на этих страницах рекламным ссылкам, нажимал на баннеры и другие интерактивные элементы, принося прибыль вирусописателям.

В марте вирусные аналитики компании «Доктор Веб» обнаружили в Google Play трояна Android.Spy.277.origin, которого злоумышленники встроили в более чем 100 программ. Это вредоносное приложение передавало вирусописателям подробную информацию о зараженном мобильном устройстве и показывало различную рекламу. Например, троянец отображал баннеры, в которых пугал пользователя тем, что аккумулятор его устройства поврежден, и для восстановления его работоспособности предлагал загрузить некие программы. Кроме того, Android.Spy.277.origin помещал рекламные сообщения в панель уведомлений и создавал на главном экране ярлыки, ведущие на страницы приложений в каталоге Google Play.

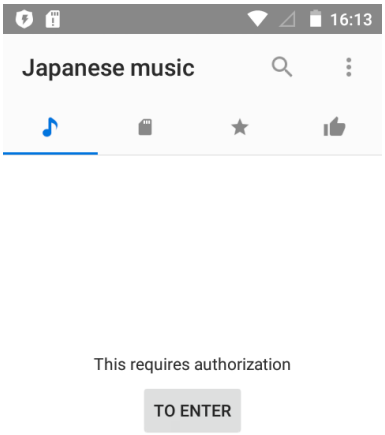


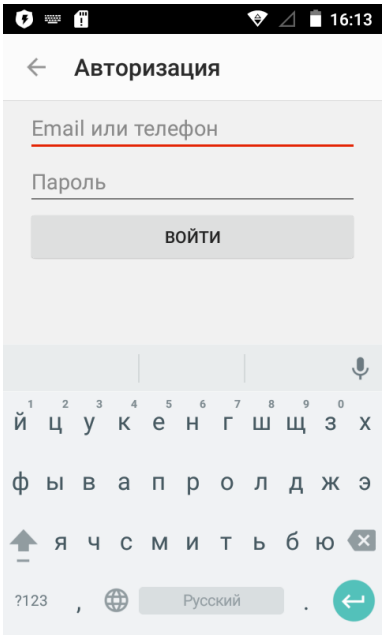


Уже в апреле специалисты «Доктор Веб» обнаружили похожего троянца, который был встроен в более чем 190 программ и получил имя Android.Click.95. После заражения мобильного устройства троянец проверял, установлено ли на нем одно из заданных вирусописателями приложений. Если оно не обнаруживалось, Android.Click.95 открывал в веб-браузере страницу мошеннического сайта с заранее приготовленным сообщением о якобы имеющейся проблеме. В нем владельца смартфона или планшета пугали старой и небезопасной версией используемого браузера или неисправностью аккумулятора. А для решения «проблемы» опять же предлагалось установить некое приложение.

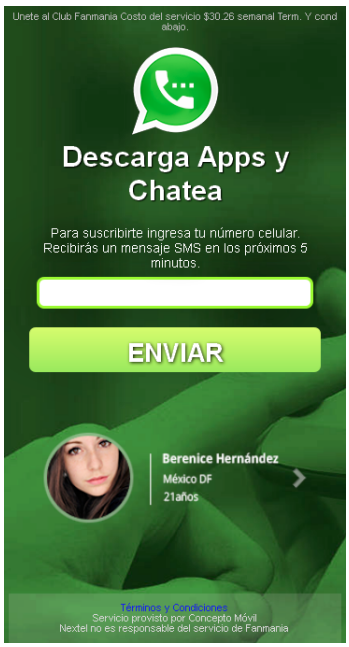


Android.PWS.Vk.3 — еще один троянец, который в 2016 году распространялся через каталог Google Play. О нем компания «Доктор Веб» сообщала в июне. Android.PWS.Vk.3 представлял собой аудиоплеер и позволял воспроизводить хранящуюся на серверах «ВКонтакте» музыку. Для этого троянец запрашивал логин и пароль от учетной записи пользователя социальной сети. Однако помимо заявленной функции он незаметно для жертвы передавал полученные данные злоумышленникам.

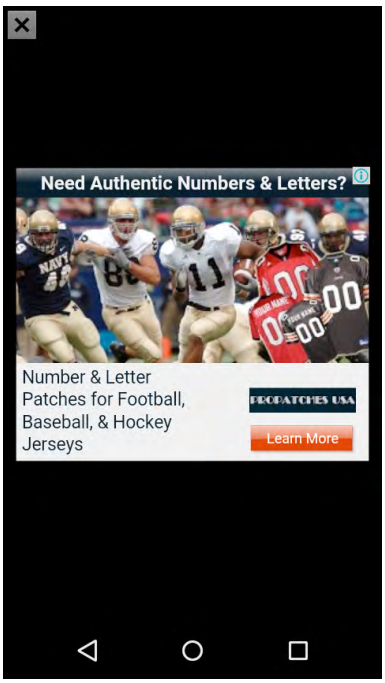


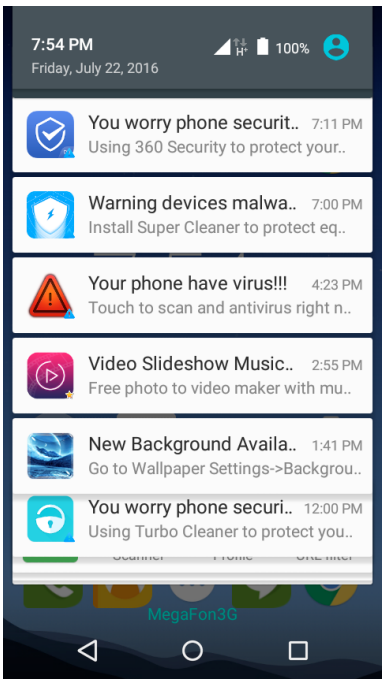


Также в июне в каталоге Google Play был найден троянец Android.Valeriy.1.origin, встроенный в безобидные программы. Android.Valeriy.1.origin показывал всплывающие окна, в которых предлагалось ввести номер мобильного телефона для загрузки того или иного приложения. После того как владелец зараженного мобильного устройства указывал свой телефон, ему приходило СМС-уведомление о подписке на платный сервис, однако троянец перехватывал и скрывал такие сообщения. Кроме того, Android.Valeriy.1.origin мог незаметно нажимать на рекламные баннеры и переходить по ссылкам, а также скачивал другие программы, в том числе вредоносные.



Другой троянец из каталога Google Play, обнаруженный уже в июле, получил имя Android.Spy.305.origin. Злоумышленники встроили его в более чем 150 приложений. Основное предназначение этой вредоносной программы — показ рекламы. Однако помимо этого Android.Spy.305.origin передавал на управляющий сервер конфиденциальную информацию.

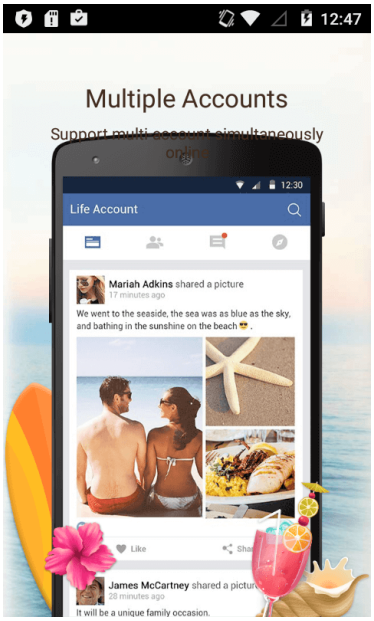


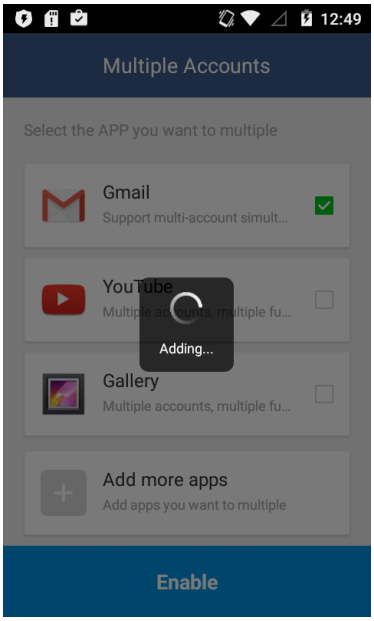


В сентябре в каталоге Google Play был найден троянец Android.SockBot.1. Эта вредоносная программа превращала зараженное устройство в прокси-сервер и позволяла злоумышленникам анонимно соединяться с удаленными компьютерами и другими устройствами, подключенными к сети, не раскрывая своего истинного местоположения. Кроме того, с его помощью вирусописатели могли перехватывать и перенаправлять сетевой трафик, похищать конфиденциальную информацию и организовывать DDoS-атаки на интернет-серверы.

Еще один троянец, распространявшийся через каталог Google Play в 2016 году, получил имя Android.MulDrop.924. О нем компания «Доктор Веб» сообщала в ноябре. Эта вредоносная программа была встроена в приложение, которое позволяло владельцам мобильных устройств одновременно использовать в установленных программах несколько учетных записей.

Обзор вирусной активности для мобильных устройств за 2016 год





Часть функционала троянца располагалась во вспомогательных модулях, которые были зашифрованы и спрятаны внутри PNG-изображения, размещенного в каталоге ресурсов Android.MulDrop.924. Один из этих модулей содержал несколько рекламных плагинов, а также троянца-загрузчика Android.DownLoader.451.origin, который без разрешения пользователя скачивал игры и приложения и предлагал установить их. Кроме того, Android.DownLoader.451.origin показывал навязчивую рекламу в панели уведомлений мобильного устройства.

Несмотря на предпринимаемые компанией Google меры безопасности, каталог Google Play по-прежнему может содержать вредоносные приложения. Вирусописатели постоянно находят способы обхода защитных механизмов, поэтому в следующем году в этом каталоге могут снова появиться троянцы.

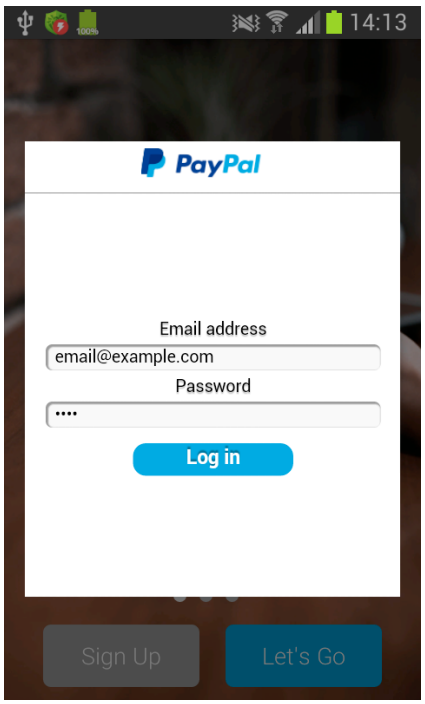
Банковские троянцы

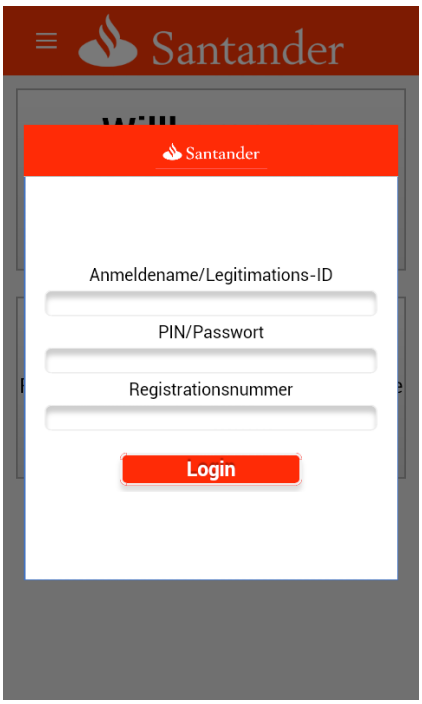
Все больше владельцев мобильных Android-устройств используют смартфоны и планшеты для доступа к услугам дистанционного банковского обслуживания. Поэтому киберпреступники продолжают совершенствовать мобильных банковских троянцев и наращивают число атак на клиентов кредитных организаций, пытаясь украсть деньги у пользователей из десятков стран. В 2016 году антивирусные продукты Dr.Web для Android обнаружили более 2 100 000 случаев проникновения таких вредоносных программ на Android-устройства, что на 138% больше, чем годом ранее.

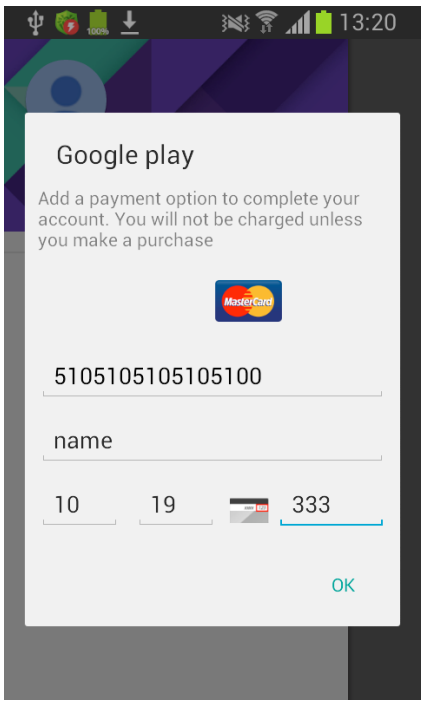
Обзор вирусной активности для мобильных устройств за 2016 год

Важным событием уходящего года стало распространение Android-банкеров при помощи рекламной платформы Google AdSence. Когда пользователи смартфонов или планшетов через браузер Chrome заходили на веб-сайты с рекламой, которую разместили злоумышленники, apk-файлы троянцев автоматически скачивались на устройства. С использованием этой уязвимости киберпреступники в течение нескольких месяцев активно распространяли таких банковских троянцев как Android.Banker.70.origin и Android.BankBot.75.origin. Позднее компания Google выпустила обновление Chrome, в котором ошибка была устранена.

Среди распространявшихся в 2016 году банковских троянцев отметился Android.SmsSpy.88.origin — о нем компания «Доктор Веб» сообщала в мае. Эта вредоносная программа известна с 2014 года, но вирусописатели до сих пор активно ее развивают. Android.SmsSpy.88.origin крадет логины и пароли от учетных записей мобильного банкинга, показывая поддельное окно аутентификации поверх запускаемых приложений «банк-клиент». Злоумышленники могут создать такое окно для любой программы, так что этот троянец способен атаковать клиентов кредитных организаций по всему миру. Android.SmsSpy.88.origin также похищает информацию о банковских картах, перехватывает входящие СМС, незаметно рассылает сообщения и даже может работать как троянец-вымогатель, блокируя экран мобильного устройства и требуя выкуп за разблокировку.

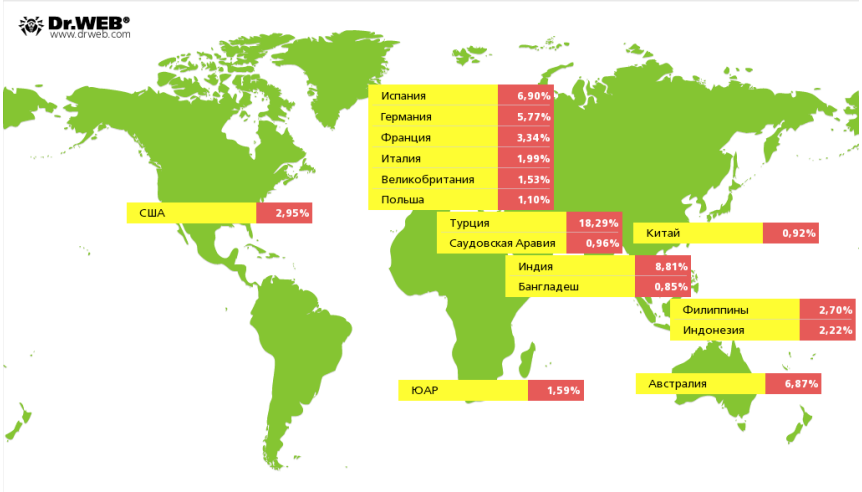






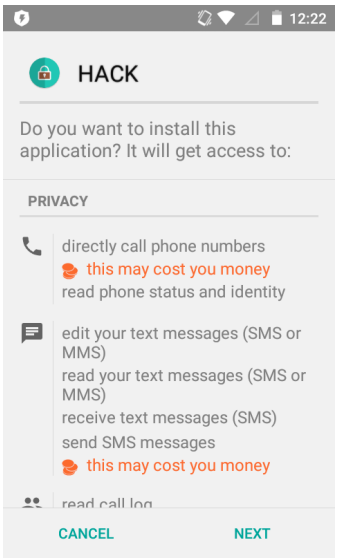
В результате проведенного исследования вирусные аналитики «Доктор Веб» установили, что с начала 2016 года с использованием Android.SmsSpy.88.origin вирусописатели атаковали пользователей из более 200 стран, а общее число зараженных устройств приблизилось к 40 000.

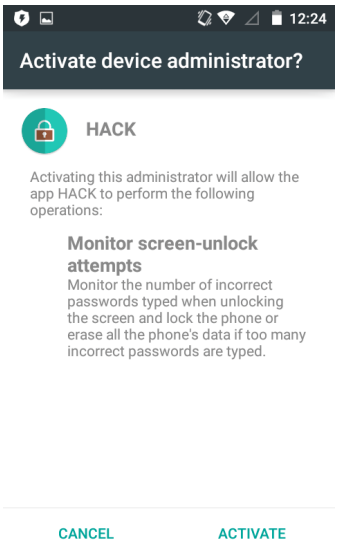
Обзор вирусной активности для мобильных устройств за 2016 год



В октябре появилась новая версия Android.SmsSpy.88.origin, которая получила имя Android.BankBot.136.origin. Здесь киберпреступники добавили поддержку современных версий ОС Android, в которых были улучшены защитные механизмы против вредоносных программ. В результате троянец научился показывать фишинговые окна и перехватывать СМС-сообщения на еще большем числе моделей мобильных устройств.

Также в 2016 году вирусные аналитики «Доктор Веб» обнаружили банкера Android.BankBot.104.origin. Он распространялся под видом приложений для взлома игр и программ для читерства. Попадая на мобильное устройство, Android.BankBot.104.origin определял, подключена ли услуга дистанционного банковского обслуживания, и проверял наличие средств на всех доступных счетах. Если троянец обнаруживал деньги, он пытался незаметно перевести их злоумышленникам.



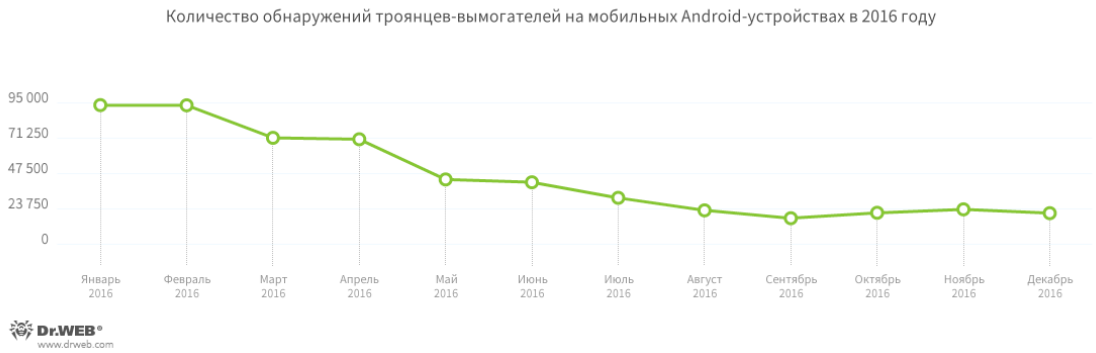


Кража денег с банковских счетов, а также похищение финансовых и других конфиденциальных данных владельцев Android-устройств приносит большую прибыль киберпреступникам. Можно с уверенностью сказать, что и в следующем году вирусописатели продолжат атаковать клиентов кредитных организаций.

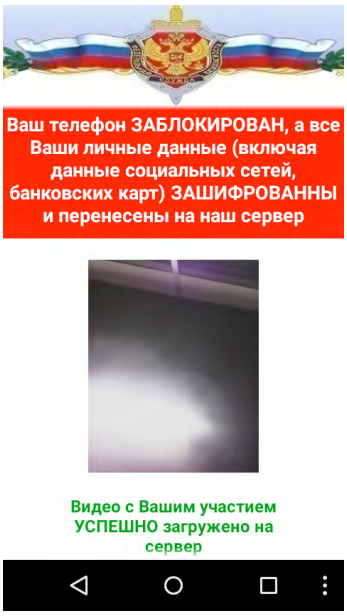
Обзор вирусной активности для мобильных устройств за 2016 год

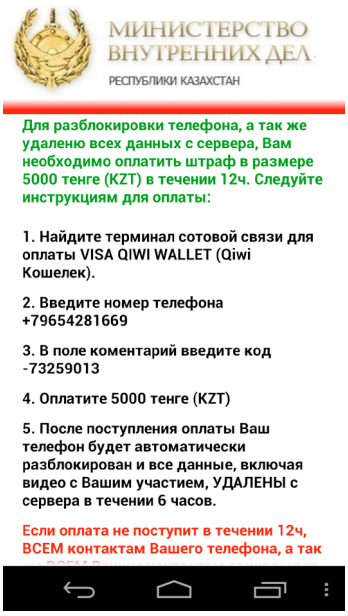
Троянцы-вымогатели

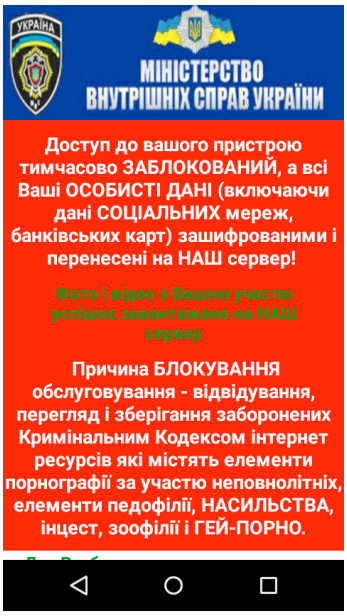
Android-троянцы, блокирующие мобильные устройства и требующие выкуп за их разблокировку, представляют серьезную опасность. В 2016 году злоумышленники вновь распространяли такие вредоносные приложения среди владельцев Android-смартфонов и планшетов. За последние 12 месяцев антивирусные продукты Dr.Web для Android зафиксировали более 540 000 случаев проникновения троянцев-вымогателей на Android-устройства. Это на 58% ниже, чем в 2015 году. Наиболее интенсивные атаки с использованием таких троянцев пришлись на первые месяцы уходящего года, после чего темп распространения этих вредоносных программ замедлился. Динамику выявлений Android-вымогателей на мобильных устройствах можно проследить на следующем графике:



Примеры сообщений, которые показывают такие вредоносные программы, представлены на следующих изображениях:







Обзор вирусной активности для мобильных устройств за 2016 год

Несмотря на некоторое снижение активности Android-блокировщиков в 2016 году, эти вредоносные программы по-прежнему являются серьезной угрозой для владельцев смартфонов и планшетов. Можно не сомневаться, что в будущем году киберпреступники сохранят Android-вымогателей в своем арсенале и продолжат с их помощью атаковать пользователей.

Для iOS

Киберпреступники, которые атакуют пользователей мобильных устройств, основное внимание уделяют смартфонам и планшетам под управлением ОС Android. Однако это не означает, что злоумышленников не интересуют другие платформы – например, iOS от компании Apple. Вредоносные и нежелательные программы для этой мобильной системы распространены еще не так широко, но их число год от года неуклонно растет. В 2016 году также появилось несколько новых угроз для iOS.

В феврале в официальном каталоге App Store была обнаружена потенциально опасная программа Program.IPhoneOS.Unwanted.ZergHelper.1, которая представляла собой каталог приложений для китайских пользователей. Ее опасность заключалась в том, что через нее распространялись любые программы, в том числе взломанные или не прошедшие проверку в компании Apple. Таким образом, пользователи рисковали скачать с помощью Program.IPhoneOS.Unwanted.ZergHelper.1 троянцев и другое опасное ПО. Кроме того, этот каталог мог устанавливать собственные обновления, минуя App Store, а также запрашивал идентификатор Apple ID и пароль, которые передавались на удаленный сервер.

Уже в марте в вирусную базу Dr.Web был добавлен троянец IPhoneOS.AceDeciever.6. Он входил в комплект созданного злоумышленниками приложения с именем 爱思助手, предназначенного для работы на Windows-компьютерах. Авторы этой программы позиционировали ее в качестве аналога утилиты iTunes, созданной для управления мобильными устройствами. Это приложение было добавлено в вирусную базу Dr.Web как Trojan.AceDeciever.2.

После того как при помощи USB-кабеля iOS-смартфон или планшет подключался к компьютеру с установленным на нем Trojan.AceDeciever.2, IPhoneOS.AceDeciever.6 автоматически устанавливался на устройство благодаря использованию уязвимости в DRM-протоколе FairPlay, созданном компанией Apple для защиты цифрового медиаконтента. Попав на мобильное устройство, IPhoneOS.AceDeciever.6 запрашивал у пользователя идентификатор Apple ID и пароль, после чего передавал их на сервер злоумышленников.

Смартфоны и планшеты под управлением iOS считаются более защищенными по сравнению с Android-устройствами. Однако киберпреступники все чаще проявляют интерес и к ним. Можно ожидать, что в будущем году появятся новые вредоносные программы, которые будут использоваться при атаках на пользователей мобильной операционной системы компании Apple.

Перспективы и тенденции

Большая часть современных мобильных устройств работает под управлением ОС Android, поэтому основная масса атак приходится именно на их владельцев. Одну из главных опасностей для пользователей Android-смартфонов и планшетов представляют банковские троянцы. Все больше таких вредоносных приложений отслеживают запуск программ «банк-клиент» и показывают поверх их окон поддельные формы ввода конфиденциальных данных. Безусловно, вирусописатели и дальше будут использовать этот механизм социальной инженерии. Кроме того, можно не сомневаться, что киберпреступники продолжат совершенствовать функционал Android-банкеров.

Актуальной для владельцев Android-смартфонов остается угроза со стороны троянцев, которые пытаются получить root-полномочия и незаметно загружают и устанавливают программы. Скорее всего, в 2017 году число таких вредоносных приложений увеличится. Кроме того, возможно появление троянцев, которые при атаках на мобильные устройства будут использовать новые механизмы заражения.

На протяжении нескольких лет киберпреступники не раз предустанавливали на Android-смартфоны и планшеты различных троянцев и нежелательные программы. С большой долей вероятности эта тенденция продолжится, поэтому в следующем году стоит ожидать новых случаев заражения прошивок мобильных устройств.

Несмотря на все усилия компании Google в обеспечении безопасности своего официального каталога приложений, вирусописатели по-прежнему размещают в нем различных троянцев, о чем красноречиво говорят наблюдавшиеся в 2016 году многочисленные случаи обнаружения вредоносных программ в Google Play. Скорее всего, в 2017 году владельцы Android-смартфонов и планшетов вновь столкнутся с появлением троянцев в официальном каталоге программ для ОС Android.

Серьезную опасность для пользователей по-прежнему представляют и Android-вымогатели. В следующем году также стоит ожидать новых атак с их участием. Кроме того, не исключено появление новых вредоносных программ, которые предназначены для работы на устройствах под управлением iOS. Смартфоны и планшеты, работающие на этой операционной системе, все еще остаются достаточно защищенными. Однако 2016 год показал, что интерес злоумышленников к этой платформе по-прежнему сохраняется. Вирусописатели всегда пытаются извлечь выгоду там, где это возможно, поэтому и в 2017 году iOS-устройства будут оставаться потенциальными целями атак киберпреступников.

Обзор вирусной активности для мобильных устройств за 2016 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
125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | www.mobi.drweb.com | www.av-desk.ru
«Доктор Веб» в других странах