Dr.WEB®
с 1992 года

Обзор вирусной активности для мобильных устройств за 2015 год

Обзор вирусной активности для мобильных устройств за 2015 год

30 декабря 2015 года

Последние 12 месяцев стали очередным непростым периодом для владельцев смартфонов и планшетов. Как и прежде, киберпреступники уделили пристальное внимание пользователям устройств под управлением ОС Android, поэтому большая часть обнаруженных в 2015 году «мобильных» вредоносных и нежелательных программ предназначалась именно для этой платформы. В частности, заметную активность проявили всевозможные банкеры, возросло число Android-вымогателей, рекламных модулей и СМС-троянцев. Кроме того, участились случаи обнаружения предустановленного вредоносного ПО в прошивках ОС Android. Серьезной угрозой стало появление большого количества троянцев, которые пытались получить на мобильных Android-устройствах root-доступ и заразить системный каталог разнообразными руткитами. Вместе с тем злоумышленники не обошли стороной и приверженцев продукции компании Apple – для смартфонов и планшетов на базе iOS в течение 2015 года также было выявлено немало опасного ПО.

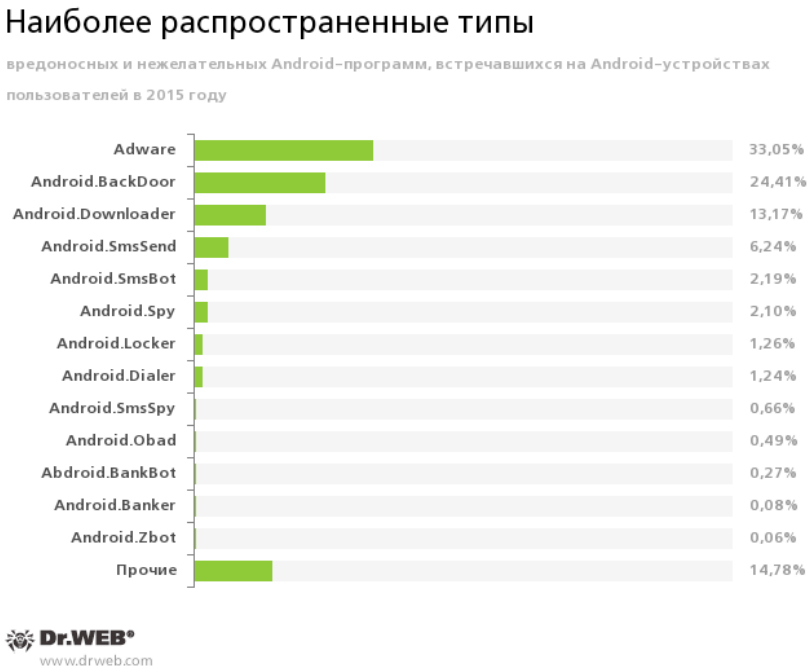
Главные тенденции года

- Распространение банковских Android-троянцев
- Увеличение числа троянцев, получающих root-доступ и заражающих системный каталог Android-устройств
- Рост случаев внедрения вредоносных приложений в Android-прошивки
- Появление новых вредоносных программ для iOS

Обзор вирусной активности для мобильных устройств за 2015 год

Вирусная обстановка в сегменте мобильных устройств

В 2015 году злоумышленники продолжили атаковать мобильные устройства, работающие под управлением ОС Android, при этом главной целью киберпреступников по-прежнему оставалось получение прибыли за счет пользователей. Однако за последние 12 месяцев тактика вирусописателей претерпела значительные изменения. Если раньше для обогащения они массово использовали вредоносные программы, отправляющие дорогостоящие СМС-сообщения на премиум-номера, то теперь все чаще ориентируются на другие схемы заработка. Так, согласно статистическим данным, собранным с использованием антивирусных продуктов Dr.Web для Android, в 2015 году чаще всего на Android-смартфонах и планшетах обнаруживались следующие типы вредоносных и нежелательных программ:

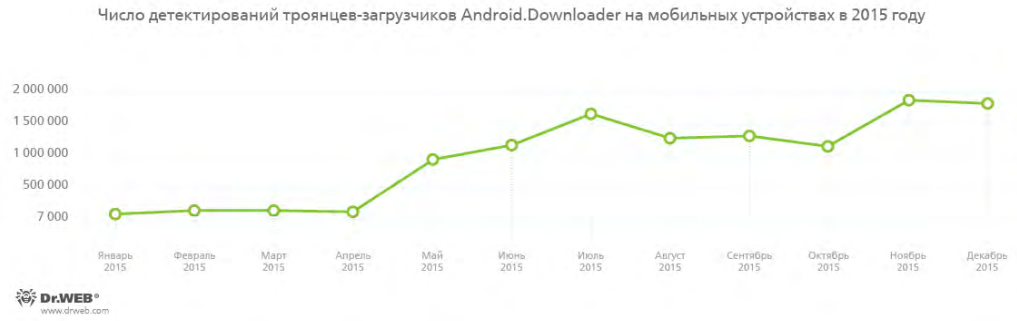


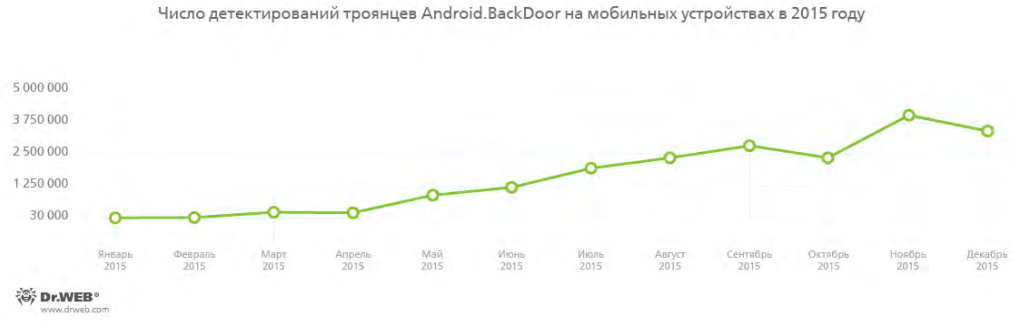
Данная статистика говорит о том, что самыми распространенными «мобильными» угрозами стали всевозможные рекламные модули, показывающие навязчивые коммерческие предложения. Также широкую популярность получили различные бэкдоры и троянцы-загрузчики, которые устанавливали на зараженные смартфоны и планшеты ненужное пользователям ПО. При этом часто такие вредоносные программы стремились получить root-доступ в инфицированной системе, чтобы выполнить инсталляцию незаметно. В целом можно с уверенностью сказать, что в 2015 году наблюдалась

Обзор вирусной активности для мобильных устройств за 2015 год

устойчивая тенденция к росту случаев использования злоумышленниками подобных троянцев. Подтверждением этому служит статистика детектирований антивирусными продуктами Dr.Web для Android: в десятку наиболее распространенных вредоносных приложений в минувшем году попали Android.BackDoor.240.origin и Android.DownLoader.155.origin, пытавшиеся получить root-привилегии на атакуемых устройствах, чтобы затем скрытно от пользователей устанавливать различное ПО.

Динамика выявлений Android-бэкдоров и троянцев-загрузчиков, многие из которых в 2015 году пытались получить root-доступ на мобильных устройствах, показана на следующих графиках:





Троянцы, получающие root-доступ

Как уже отмечалось ранее, одной из главных тенденций в сфере информационной безопасности для мобильных устройств в 2015 году стало появление большого числа вредоносных программ, которые пытались получить root-доступ на заражаемых Android-смартфонах и планшетах. В случае успеха такие троянцы обретали неограниченные права и могли, в частности, незаметно устанавливать всевозможное ПО, в том числе и внедрять его в системный каталог, фактически заражая мобильные устройства руткитами.

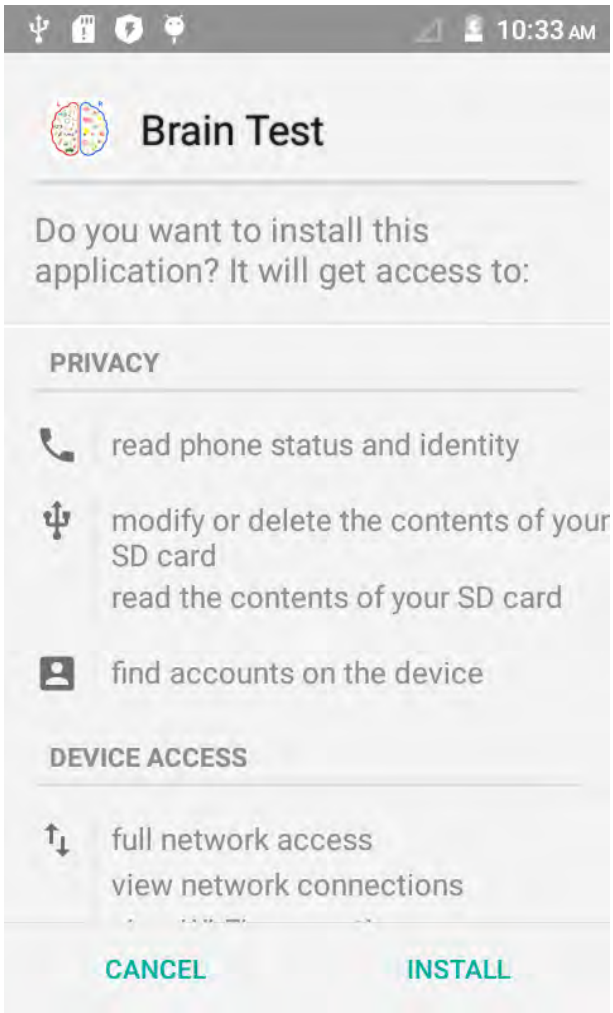
Один из первых случаев с участием таких троянцев в 2015 году был зафиксирован в марте, когда специалисты компании «Доктор Веб» обнаружили вредоносные приложения семейства Android.Toorch. Они распространялись вирусописателями через популярные в Китае онлайн-сборники ПО, а также при помощи агрессивных рекламных модулей, интегрированных в различные программы. При запуске на Android-устройствах эти троянцы пытались повысить свои системные привилегии до уровня root, после чего незаметно устанавливали в системный каталог один из своих компонентов. После этого по команде злоумышленников вредоносные приложения Android.Toorch могли без ведома пользователя загружать, устанавливать и удалять разнообразное ПО.

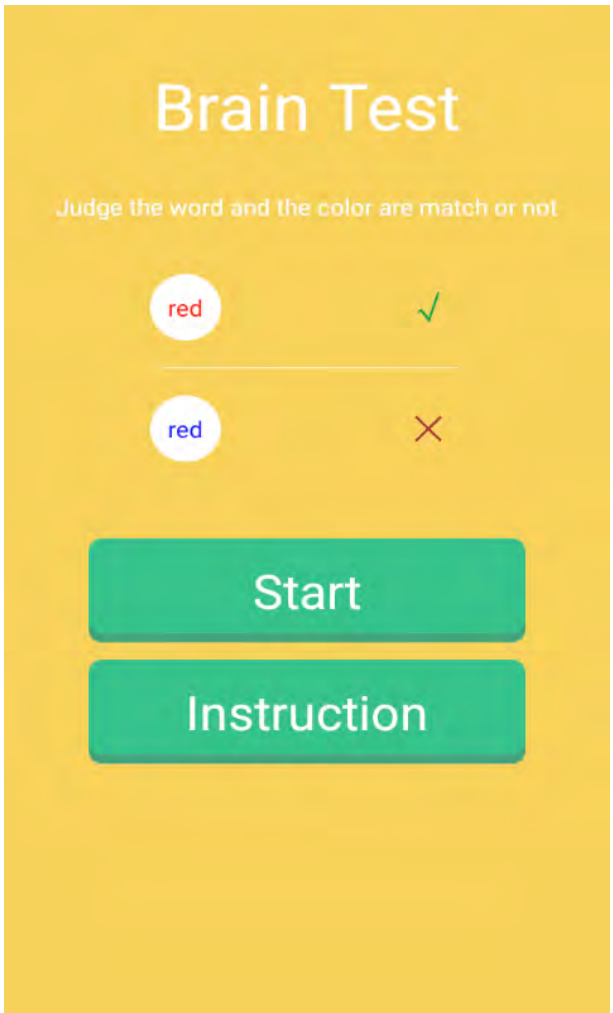
Другой троянец, добавленный в вирусную базу как Android.Backdoor.176.origin, пытался получить root-доступ на заражаемых смартфонах и планшетах при помощи загружаемой из Интернета модифицированной версии утилиты Root Master. В случае успеха он копировал в системный каталог несколько вспомогательных вредоносных модулей, после чего мог скрытно устанавливать и удалять приложения по команде с управляющего сервера. Кроме того, Android.Backdoor.176.origin передавал злоумышленникам подробные сведения о зараженном мобильном устройстве, отслеживал количество входящих и исходящих вызовов, а также отправленных и принятых СМС-сообщений. Этот троянец интересен тем, что присваивал себе специальные системные атрибуты, благодаря чему его было невозможно удалить из зараженной системы.

Чуть позднее была обнаружена новая версия Android.Backdoor.176.origin, добавленная в вирусную базу как Android.Backdoor.196.origin. Этот троянец аналогичным образом пытался получить root-доступ и, в случае успеха, запускал свой второй компонент, который загружался с сервера злоумышленников или копировался и расшифровывался из ресурсов самой вредоносной программы. Данный модуль, детектируемый как Adware.Xinyin.1.origin, выполнял все необходимые злоумышленникам действия. В частности, он мог незаметно загружать и устанавливать различные программы, отправлять СМС-сообщения, отслеживать количество совершенных и принятых звонков, а также полученных и отправленных СМС.

Обзор вирусной активности для мобильных устройств за 2015 год

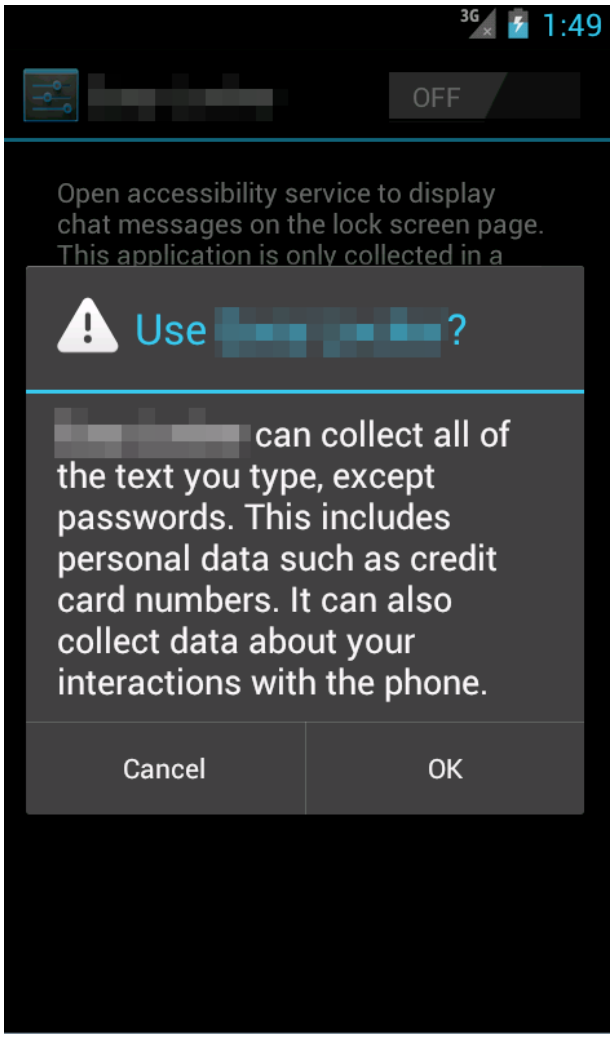
Еще один троянец, пытавшийся получить root-доступ в ОС Android, распространялся вирусописателями в каталоге Google Play под видом безобидного приложения с именем Brain Test. Эта вредоносная программа, известная как Android.Backdoor.273.origin, загружала с управляющего сервера и поочередно пыталась выполнить несколько эксплойтов, предназначенных для повышения системных полномочий в ОС Android. В случае успеха троянец скачивал с управляющего сервера вспомогательный вредоносный компонент, который незаметно устанавливался в системный каталог и в дальнейшем использовался злоумышленниками для загрузки и скрытной инсталляции других опасных приложений. Чтобы обезопасить себя от удаления, Android.Backdoor.273.origin помещал в системную директорию несколько дополнительных модулей, которые отслеживали целостность всех вредоносных компонентов троянца и переустанавливали их в случае удаления пользователем.





Обзор вирусной активности для мобильных устройств за 2015 год

Не меньшую опасность для владельцев Android-устройств представлял и троянец Android.DownLoader.244.origin, который распространялся через популярные сайты – сборники ПО в модифицированных киберпреступниками изначально безопасных программах и играх. Эта вредоносная программа пыталась получить на зараженном устройстве root-доступ, после чего по команде с управляющего сервера могла загружать и незаметно устанавливать в системный каталог различные приложения. Примечательно, что при первом запуске троянец запрашивал у пользователя доступ к специальным возможностям ОС (Accessibility Service). Если потенциальная жертва соглашалась предоставить ему необходимые права, Android.DownLoader.244.origin получал возможность контролировать все события, происходящие на устройстве, а также мог незаметно инсталлировать приложения, имитируя действия пользователя и самостоятельно нажимая на кнопки в диалоговых окнах при установке программ. В результате троянец имел «запасной вариант» для выполнения своей вредоносной деятельности на случай если получить root-полномочия ему не удавалось.



Троянцы в прошивках

Также в прошедшем году вновь актуальной стала проблема предустановленных на мобильные устройства троянцев. Подобный способ распространения вредоносных приложений представляет серьезную угрозу, т. к. приобретающие смартфоны и планшеты пользователи зачастую вовсе не догадываются о наличии такого «подарка», справедливо полагая, что их устройства не должны представлять какой-либо опасности. И даже если в дальнейшем скрытое вредоносное приложение будет обнаружено, его удаление может стать настоящей проблемой, потому что потребует либо получения root-доступа, либо обновления образа операционной системы на заведомо чистую версию. Однако и с установкой сторонних прошивок могут возникнуть проблемы, поскольку все чаще злоумышленники встраивают троянское ПО и туда.

Одна из таких вредоносных программ была выявлена в январе 2015 года. Троянец, получивший имя Android.CaPson.1, внедрялся киберпреступниками в различные образы ОС Android и мог незаметно отправлять и перехватывать СМС-сообщения, открывать интернет-страницы, передавать на удаленный сервер информацию о зараженном мобильном устройстве, а также загружать другие приложения.

Позже, в сентябре, специалисты компании «Доктор Веб» обнаружили, что известный еще с 2014 года троянец Android.Backdoor.114.origin был предустановлен злоумышленниками на планшете Oysters T104 HVi 3G. Эта вредоносная программа может незаметно загружать, устанавливать и удалять приложения по команде с управляющего сервера, при этом троянец также способен самостоятельно активировать отключенную опцию установки ПО из непроверенных источников. Кроме того, Android.Backdoor.114.origin собирает и отправляет на удаленный сервер очень подробную информацию о зараженном устройстве. Детали данного инцидента изложены в опубликованном на сайте компании «Доктор Веб» материале.

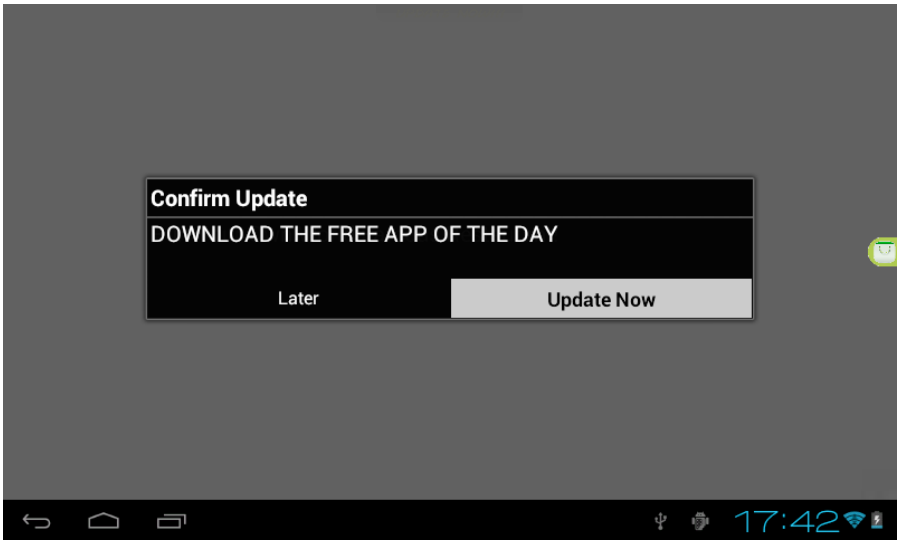
Уже в октябре 2015 года на нескольких мобильных Android-устройствах был обнаружен предустановленный троянец Android.Cooee.1. Эта опасная программа находилась в приложении-лаунчере (графической оболочке Android) и содержала в себе ряд специализированных модулей, предназначенных для показа рекламы. Также данный троянец мог незаметно загружать и запускать на исполнение как дополнительные рекламные пакеты, так и другие приложения, включая вредоносное ПО.

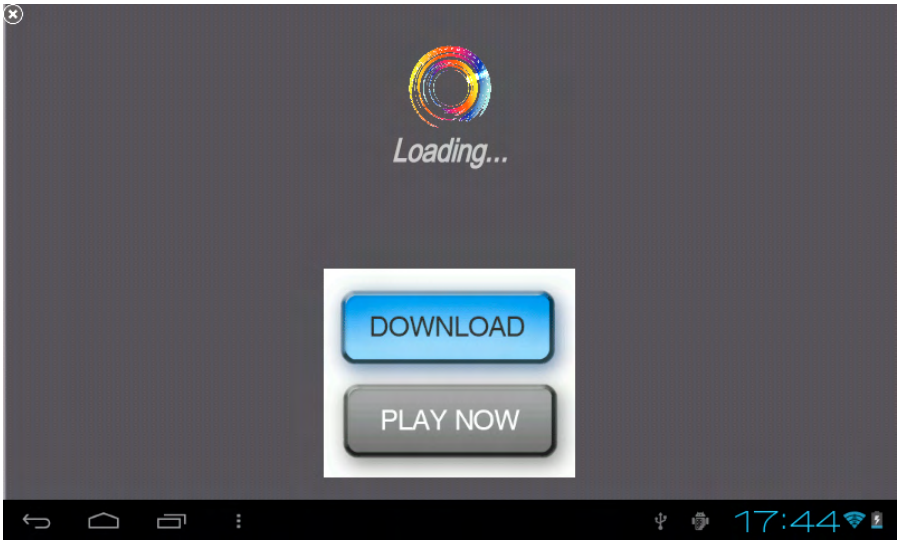
Рекламные модули

Разнообразные рекламные платформы, встраиваемые разработчиками в Android-приложения, приносят им прибыль и одновременно сохраняют распространяемое ПО бесплатным. Это устраивает большинство пользователей, т. к. позволяет им экономить деньги. Однако недобросовестные создатели программ и даже вирусописатели все чаще применяют агрессивные типы рекламных модулей, которые показывают навязчивые коммерческие предложения, крадут конфиденциальную информацию и выполняют другие нежелательные действия. В 2015 году эта тенденция сохранилась. Количество обнаруженных в течение года нежелательных рекламных приложений на Android-устройствах показано на следующем графике:

В январе был обнаружен рекламный плагин Adware.HideIcon.1.origin, который был встроен в несколько распространяемых через каталог Google Play программ. После установки этих приложений пользователи сталкивались с целым шквалом навязчивых сообщений. В частности, в панели уведомлений мобильных устройств с определенной периодичностью возникали сообщения о доступности неких обновлений, там же мог имитироваться процесс загрузки важных файлов, при попытке открыть которые владелец смартфона или планшета перенаправлялся на различные веб-сайты. Кроме того, при запуске различных программ на весь экран показывалась реклама.

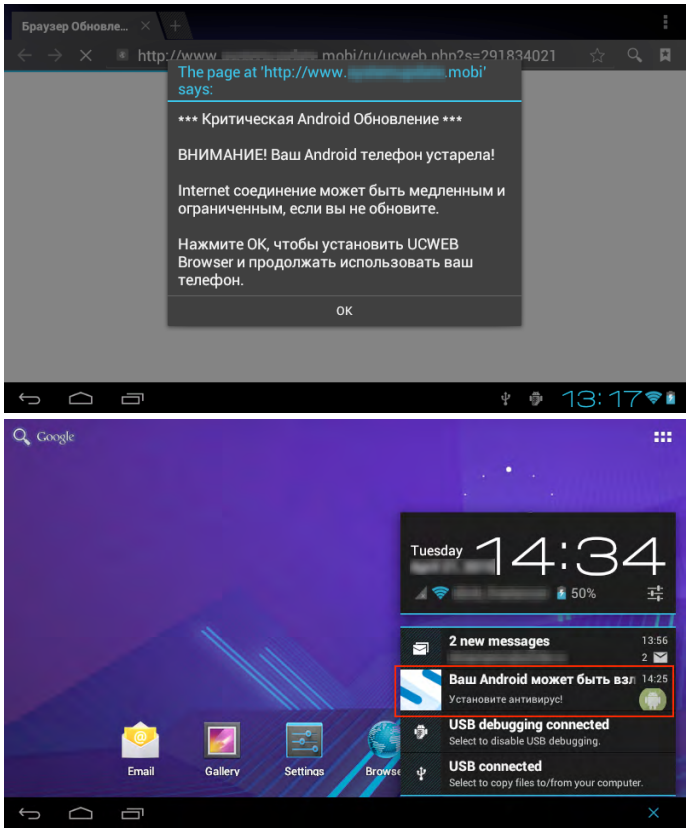
Обзор вирусной активности для мобильных устройств за 2015 год



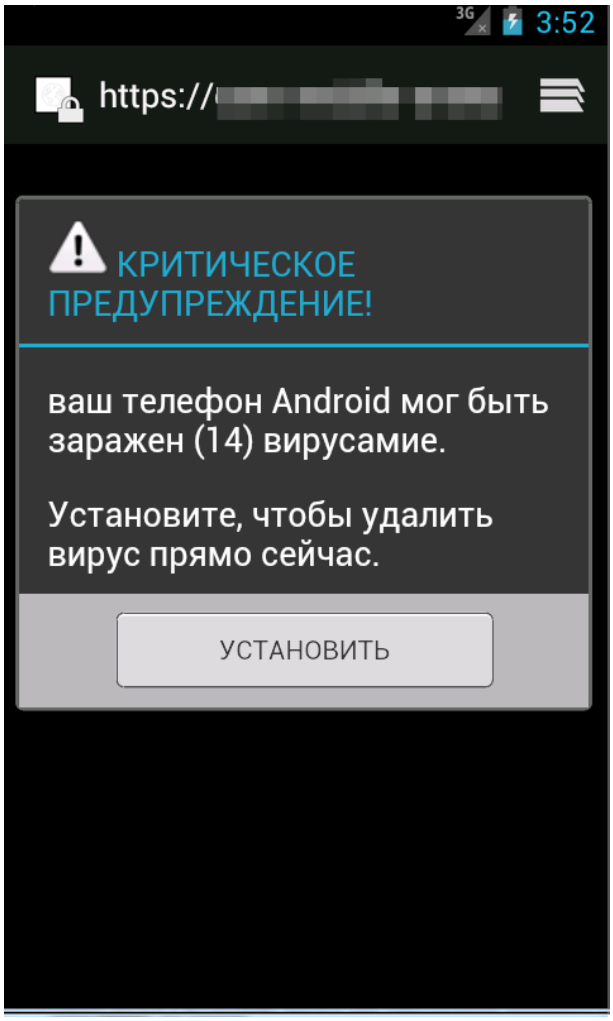


Чуть позже, в феврале, было выявлено сразу несколько новых нежелательных рекламных модулей. Один из них получил имя Adware.MobiDash.1.origin. Злоумышленники встроили его в распространяемые через каталог Google Play программы, которые в общей сложности были загружены десятки миллионов раз. При каждом выходе Android-устройства из режима ожидания Adware.MobiDash.1.origin загружал в веб-браузере интернет-страницы с разнообразной рекламой, а также сомнительными сообщениями, такими как предупреждения о якобы имеющих место неполадках, предложения установить обновления или всевозможное ПО и т. п. Кроме того, Adware.MobiDash.1.origin мог отображать рекламу поверх интерфейса операционной системы и пользовательских приложений, а также демонстрировать рекламные и иные сообщения в панели уведомлений. Примечательно, что этот модуль начинал свою деятельность не сразу, а лишь по прошествии достаточно длительного времени с момента установки содержащей его программы, поэтому к моменту активизации Adware.MobiDash.1.origin пользователям было труднее определить истинный источник нежелательной активности на устройствах.

В апреле была выявлена новая версия этого модуля, которая обладала аналогичным функционалом и получила имя Adware.MobiDash.2.origin. Как и его предшественник, Adware.MobiDash.2.origin распространялся в размещенных в Google Play программах, общее число загрузок которых превысило 2 500 000. Подробнее об Adware.MobiDash.2.origin рассказано в данном материале.



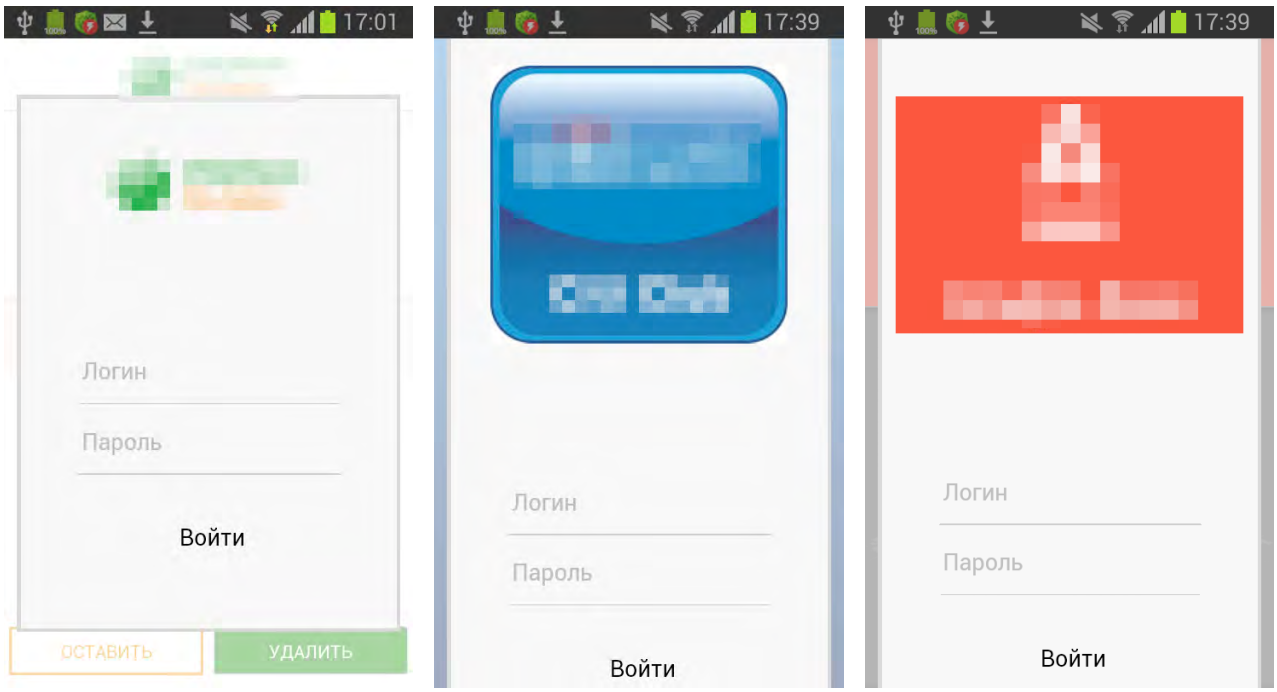
Также в феврале было обнаружено еще несколько агрессивных рекламных модулей для ОС Android. Один из них – Adware.HiddenAds.1 – устанавливался на устройства при помощи различных вредоносных программ. Он не имел ярлыка и графического интерфейса, работал в скрытом режиме и отображал в панели уведомлений различные рекламные сообщения. Другой модуль, получивший имя Adware.Adstoken.1.origin, распространялся в составе разнообразных приложений и показывал на экране рекламные баннеры, демонстрировал сообщения в панели уведомлений и мог открывать в веб-браузере сайты с рекламой. Уже в конце года вирусные аналитики компании «Доктор Веб» обнаружили очередной нежелательный рекламный плагин для ОС Android, который устанавливался при помощи троянца Android.Spy.510 и был добавлен в вирусную базу как Android.Spy.510. Это нежелательное ПО показывало рекламу поверх большинства запускаемых программ, в результате чего владельцы зараженных Android-устройств могли подумать, что источник навязчивых уведомлений – именно те приложения, которые они запускали в данный момент.



Рекламные модули

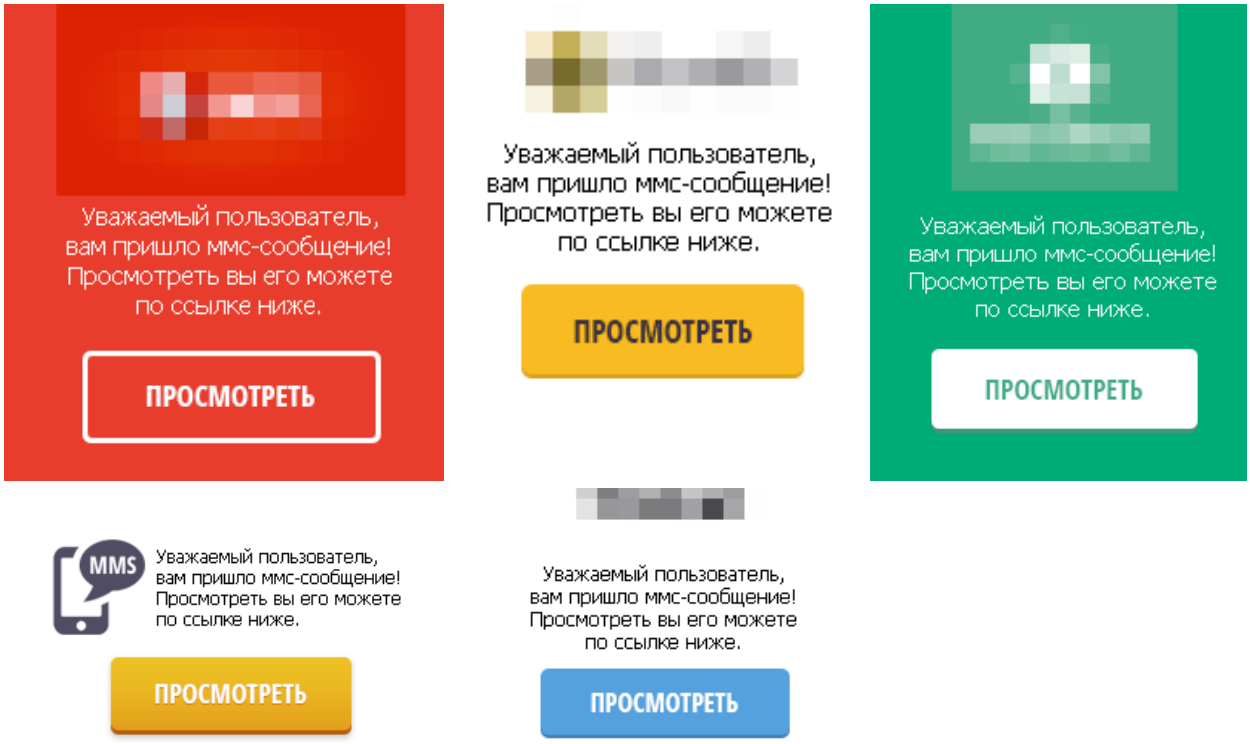
Серьезную опасность для финансового благополучия владельцев Android-смартфонов и планшетов представляют троянцы, которые похищают логины и пароли от учетных записей мобильного банкинга и незаметно крадут деньги со счетов. В 2015 году интерес злоумышленников к атакам с применением этих вредоносных программ сохранился. Так, в течение последних 12 месяцев антивирусные продукты Dr.Web для Android выявили более 880 000 случаев проникновения Android-банкеров на смартфоны и планшеты, при этом среди обнаруженных троянцев были представители хорошо известных семейств Android.BankBot, Android.Banker, а также ряда других.

Однако в прошедшем году вирусные аналитики компании «Доктор Веб» выявили множество банковских троянцев нового семейства Android.ZBot. Данные вредоносные программы опасны тем, что помимо уже привычной возможности незаметно переводить деньги со счетов пользователей на счета злоумышленников способны показывать поверх запускаемых приложений поддельные диалоговые окна и формы ввода конфиденциальных данных (чаще всего – пары «логин-пароль» для доступа к услугам мобильного банкинга).

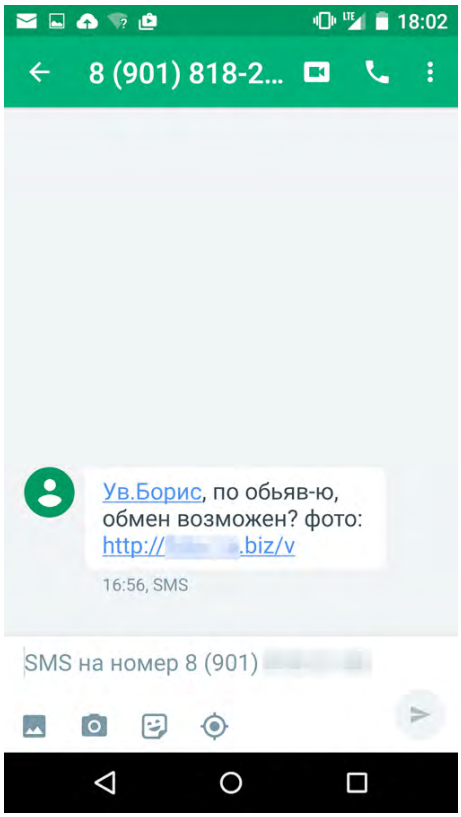


Жертвы таких троянцев могут ошибочно подумать, что подобные экранные формы принадлежат запущенным программам, в результате чего рискуют предоставить важную информацию злоумышленникам. Получив нужные данные, банкеры Android.ZBot отправляют их на сервер вирусописателей, после чего последние могут управлять счетами пользователей и незаметно красть с них деньги. В 2015 году эти опасные вредоносные приложения успели отметиться на более чем 600 000 мобильных Android-устройствах.

Одним из популярных способов распространения банковских троянцев является рассылка нежелательных СМС, в которых потенциальным жертвам под тем или иным предлогом рекомендуется перейти по указанной в тексте сообщения ссылке. Если пользователь Android-смартфона или планшета поддается на уловку злоумышленников, то он либо попадает на принадлежащий киберпреступникам мошеннический веб-сайт, с которого под видом полезного приложения вредоносная программа загружается самим владельцем мобильного устройства, либо перенаправляется непосредственно на файл троянца, скачиваемый автоматически с одного из интернет-ресурсов. Например, в России злоумышленники распространяли СМС, в которых потенциальным жертвам предлагалось ознакомиться с якобы поступившим ММС-сообщением. При этом после перехода по указанной в полученном тексте ссылке пользователи чаще всего попадали на мошеннические сайты, в оформлении которых для большей достоверности применялись логотипы популярных мобильных операторов. Среди распространявшихся таким образом Android-банкеров были замечены троянцы семейства Android.SmsBot – в частности, **Android.SmsBot.269.origin** и **Android.SmsBot.291.origin.**

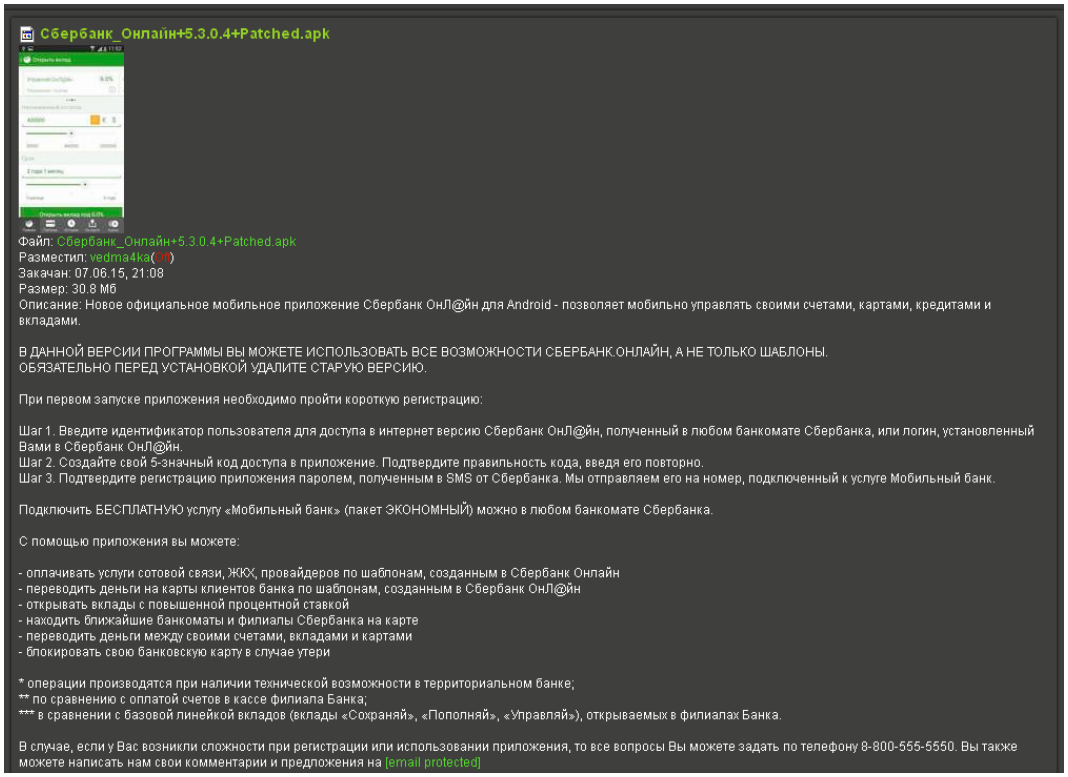


Кроме того, злоумышленники рассылали мошеннические сообщения и от имени якобы заинтересованных покупателей, откликнувшихся на размещенные ранее объявления о продаже чего-либо:



Помимо рассылки нежелательных СМС, в которых содержатся ведущие на загрузку того или иного троянца ссылки, киберпреступники применяют и другие методы распространения банкеров. Например, обнаруженная в июне вредоносная программа Android.BankBot.65.origin была внедрена злоумышленниками в официальное приложение для доступа к мобильному банкингу и распространялась под видом его обновленной версии через популярный сайт, посвященный мобильным устройствам. Модифицированная вирусописателями программа сохраняла все свои оригинальные функции, поэтому у потенциальных жертв троянца не было причин ожидать какого-либо подвоха. По указанию злоумышленников Android.BankBot.65.origin может незаметно отправлять и перехватывать СМС-сообщения, благодаря чему способен управлять счетами пользователей через сервис мобильного банкинга. Кроме того, вирусописатели могут применять данного троянца для организации мошеннических схем, внедряя в список входящих сообщений различные СМС с заданным текстом.

Обзор вирусной активности для мобильных устройств за 2015 год



Android-вымогатели

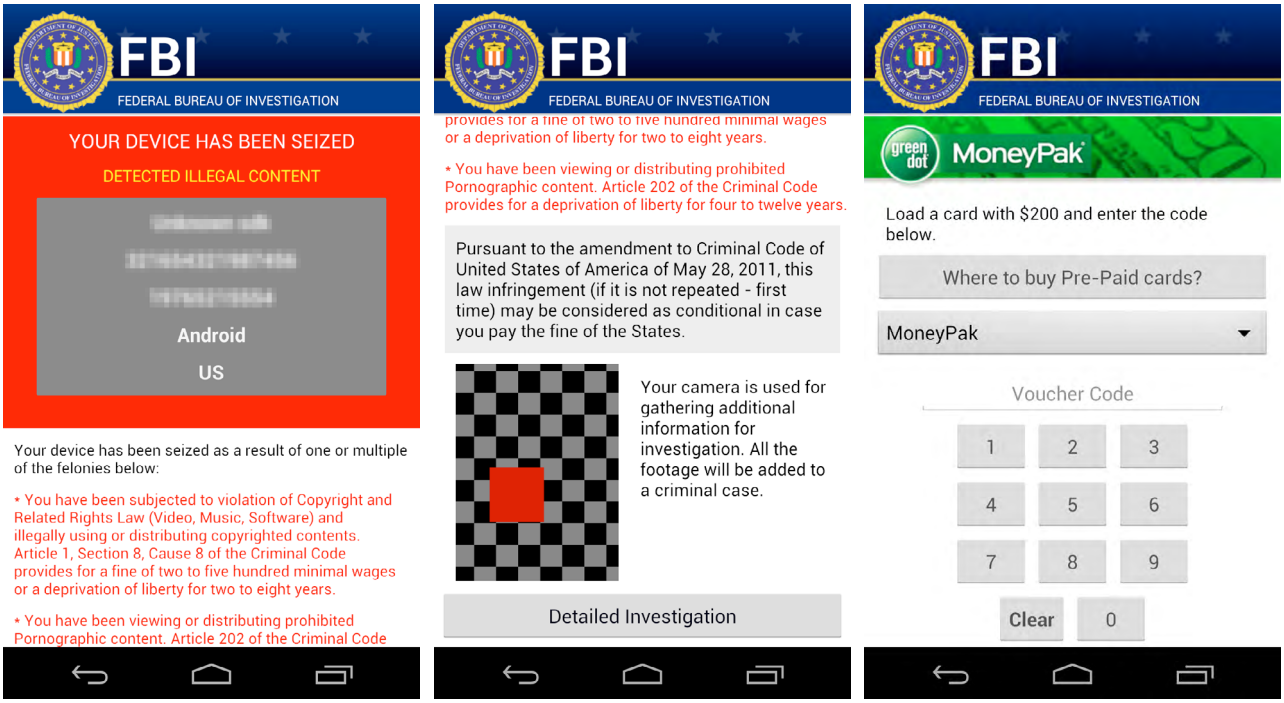
В 2015 году троянцы-вымогатели представляли серьезную угрозу для пользователей ОС Android. В течение последних 12 месяцев эти вредоносные приложения были зафиксированы на устройствах пользователей свыше 1 300 000 раз.

Узнайте больше

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

Обзор вирусной активности для мобильных устройств за 2015 год

Данные троянцы опасны тем, что блокируют смартфоны и планшеты и требуют у их владельцев денежный выкуп за разблокировку. Большинство Android-вымогателей работает именно по такой схеме, однако среди них встречаются и чрезвычайно опасные экземпляры. В частности, в феврале была обнаружена новая версия трояна-блокировщика Android.Locker.71.origin, который шифровал все доступные файлы и блокировал зараженные мобильные устройства, требуя у пострадавших пользователей выкуп в размере $200. Шифрование файлов на каждом смартфоне или планшете происходило с использованием уникального криптографического ключа, поэтому восстановить поврежденные троянцем данные было практически невозможно.



В сентябре 2015 года был обнаружен очередной Android-вымогатель, который блокировал зараженные смартфоны и планшеты благодаря установке собственного пароля на разблокировку экрана. Подобная методика не нова и ранее уже применялась злоумышленниками в других троянцах, однако блокировщики для ОС Android с таким функционалом встречаются все еще достаточно редко. После запуска эта вредоносная программа, добавленная в вирусную базу Dr.Web как Android.Locker.148.origin, пытается получить доступ к функциям администратора мобильного устройства, однако в отличие от большинства других аналогичных вредоносных приложений делает это весьма оригинальным способом. В частности, поверх стандартного системного запроса она показывает собственное диалоговое окно, предлагая установить некое обновление. Соглашаясь на установку этого «обновления», пользователь на самом деле предоставляет троянцу доступ к расширенным системным функциям, после чего Android.Locker.148.origin уже беспрепятственно блокирует атакованный смартфон или планшет, устанавливая пароль на разблокировку экрана, и требует выкуп у своей жертвы.

Обзор вирусной активности для мобильных устройств за 2015 год

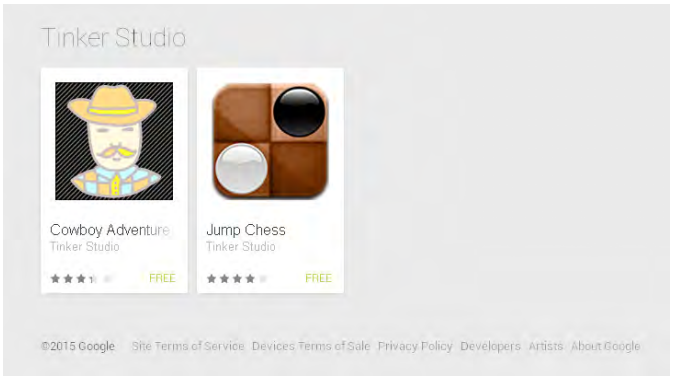
СМС-троянцы

СМС-троянцы, отправляющие премиум-сообщения на короткие номера и подписывающие абонентов мобильных операторов на платные контент-услуги, по-прежнему остаются для злоумышленников весьма популярным инструментом заработка, хоть и начинают постепенно уступать место другим вредоносным приложениям. Несмотря на то, что в 2015 году эти троянцы были обнаружены на Android-смартфонах и планшетах пользователей более 6 000 000 раз, ближе к концу года наблюдалась тенденция к снижению интенсивности их распространения.

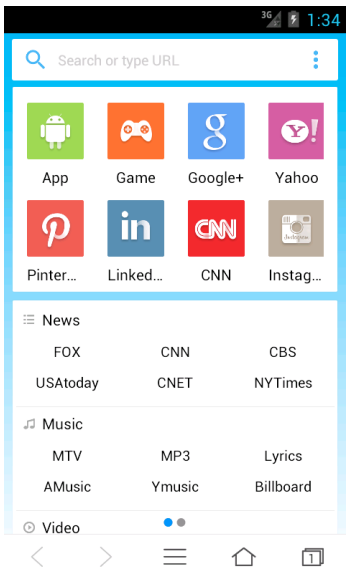
СМС-троянцы

Несмотря на то, что каталог приложений Google Play является официальным и наиболее надежным источником ПО для ОС Android, время от времени в него все же проникают различные троянцы. В этом плане не стал исключением и 2015 год. Так, в июле в нем были обнаружены троянцы Android.Spy.134 и Android.Spy.135, которые скрывались в безобидных на первый взгляд играх. Эти вредоносные программы были способны демонстрировать на экране зараженных смартфонов и планшетов поддельное окно аутентификации приложения-клиента Facebook, запрашивая у владельцев мобильных устройств логин и пароль от их учетных записей, и передавали введенные данные на удаленный сервер. Вскоре после этого многие пользователи социальной сети, находящиеся в списке контактов жертв, могли получить сообщение от «друга»,

в котором рекомендовалось установить игру, перейдя по указанной ссылке. Благодаря такому приему создатели троянцев добились значительных успехов в их распространении: на момент удаления Android.Spy.134 и Android.Spy.135 из каталога Google Play в общей сложности они были загружены более 500 000 раз.



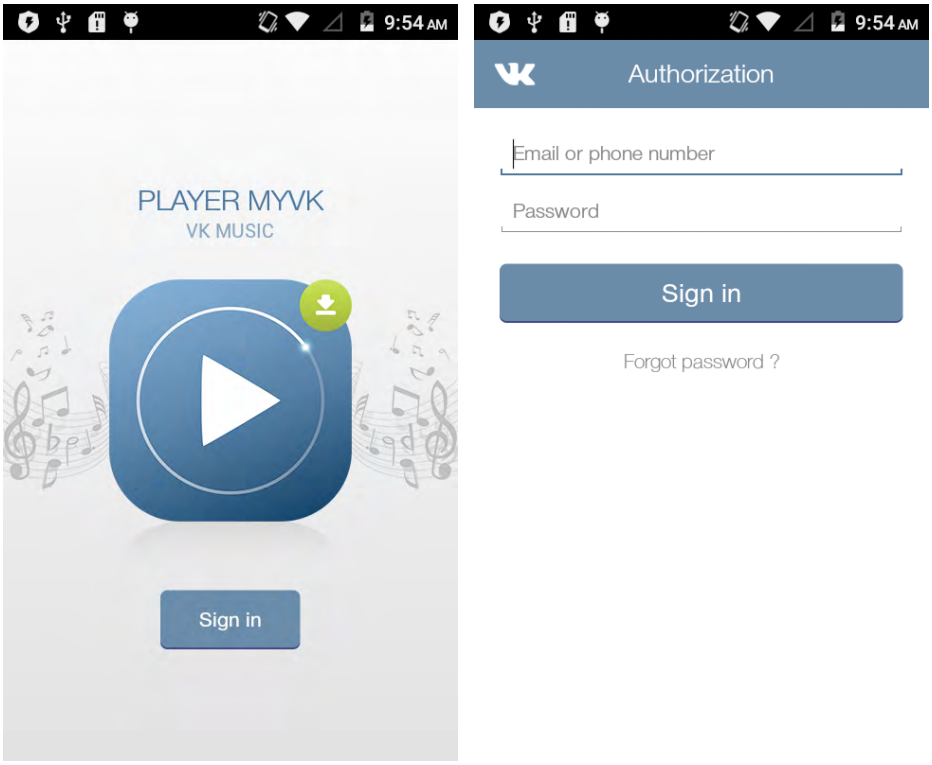
В этом же месяце вирусные аналитики «Доктор Веб» обнаружили в каталоге Google Play другого троянца, получившего имя Android.DownLoader.171.origin. Основное предназначение этой вредоносной программы – загрузка и установка различных приложений. Кроме того, по команде вирусописателей троянец мог удалять уже установленное ПО. Еще одной вредоносной функцией Android.DownLoader.171.origin являлась демонстрация рекламы в панели уведомлений операционной системы. На момент обнаружения этого троянца в каталоге Google Play его успели скачать более 100 000 пользователей. Однако злоумышленники распространяли данное приложение и на других популярных онлайн-площадках, ориентированных преимущественно на китайскую аудиторию. В результате общее число установивших Android.DownLoader.171.origin владельцев Android-устройств превысило 1 500 000. Подробнее о троянце рассказано в опубликованном материале на сайте компании «Доктор Веб».



В сентябре 2015 года в каталоге Google Play специалисты по информационной безопасности нашли троянца Android.MKcap.1.origin, который был встроен в различные игры и автоматически подписывал пользователей на платные сервисы. Для этого вредоносная программа распознавала проверочные изображения CAPTCHA, а также перехватывала и обрабатывала СМС-сообщения с кодами подтверждений.

Чуть позднее в этом же месяце в Google Play был обнаружен еще один опасный троянец, который получил имя Android.MulDrop.67. После запуска вредоносная программа извлекала скрытого внутри нее троянца-загрузчика и пыталась установить его на устройство. Основное предназначение этих троянцев – загрузка и инсталляция другого вредоносного ПО, а также показ рекламы.

Уже в октябре в каталоге Google Play был обнаружен троянец Android.PWS.3, скрывавшийся во внешне безобидном аудиоплеере. Эта вредоносная программа позволяла прослушивать музыку, размещенную в социальной сети «ВКонтакте», однако для своей работы требовала логин и пароль от пользовательской учетной записи, которые незаметно передавала на удаленный сервер злоумышленников. После этого троянец мог автоматически добавлять пострадавших владельцев мобильных устройств в различные группы, «накручивая» популярность последних.



Троянцы для iOS

В отличие от мобильных Android-устройств, смартфоны под управлением iOS долгое время практически не интересовали вирусописателей. Однако начиная с 2014 года специалисты по информационной безопасности с завидным постоянством обнаруживают все новые вредоносные и нежелательные программы для мобильной платформы от корпорации Apple. Эта тенденция продолжилась и в 2015 году.

Так, в августе в вирусные базы Dr.Web была добавлена запись для троянца IPhoneOS.BackDoor.KeyRaider. Это вредоносное приложение распространялось в модифицированных злоумышленниками изначально безопасных программах и заражало устройства, подвергнутые процедуре «jailbreak». IPhoneOS.BackDoor.KeyRaider собирал различную конфиденциальную информацию с зараженных мобильных устройств и передавал ее на сервер злоумышленников.

Обзор вирусной активности для мобильных устройств за 2015 год

Уже в сентябре в официальном магазине iOS-приложений App Store был выявлен опасный троянец IPhoneOS.Trojan.XcodeGhost. Вредоносная программа смогла проникнуть туда благодаря тому, что киберпреступники модифицировали одну из официальных версий среды разработки приложений Xcode, которая незаметно для использующих ее программистов встраивала троянца в создаваемые приложения на этапе их сборки. В результате «зараженные» таким образом изначально безобидные игры и приложения успешно прошли предварительную проверку компании Apple и беспрепятственно попали в каталог App Store. Основное предназначение IPhoneOS.Trojan.XcodeGhost – показ поддельных диалоговых окон с целью проведения фишинг-атак, а также открытие заданных злоумышленниками ссылок. Кроме того, вредоносная программа собирала подробную информацию о зараженном мобильном устройстве и отправляла ее на сервер вирусописателей. А в ноябре специалисты компании «Доктор Веб» обнаружили другую модификацию данного троянца, которая обладала аналогичным функционалом.

В октябре был обнаружен очередной iOS-троянец, который получил имя IPhoneOS.Trojan.YiSpecter.2. Эта вредоносная программа распространялась злоумышленниками преимущественно среди жителей Китая и могла загружаться на их мобильные устройства под видом безобидных приложений. Поскольку для дистрибуции троянца вирусописатели использовали метод, который позволяет инсталлировать iOS-программы, минуя каталог App Store, IPhoneOS.Trojan.YiSpecter.2 мог устанавливаться как на смартфоны и планшеты с наличием «jailbreak», так и на устройства с немодифицированной версией ОС. Данный троянец устанавливал дополнительные вредоносные модули, мог показывать различную рекламу, а также по команде киберпреступников удалять программы и заменять их поддельными версиями.

Обзор вирусной активности для мобильных устройств за 2015 год

В конце года стало известно о появлении троянца IPhoneOS.Trojan.TinyV, распространявшегося в модифицированных вирусописателями изначально безобидных программах, которые загружалась на iOS-устройства при посещении веб-сайтов, посвященных мобильным приложениям. IPhoneOS.Trojan.TinyV инсталлировался в систему iOS, в которой был выполнен «jailbreak», и по команде с управляющего сервера мог незаметно скачивать и устанавливать различное ПО, а также модифицировать файл hosts, в результате чего злоумышленники могли перенаправлять пользователей на нежелательные веб-сайты.

Помимо троянцев, в 2015 году было обнаружено и нежелательное приложение Adware.Muda.1, заражающее iOS-устройства, на которых присутствовал «jailbreak». Эта программа могла показывать рекламу поверх пользовательских приложений и в панели уведомлений, а также предназначалась для продвижения и загрузки различного ПО.

Перспективы

События минувшего года показали, что киберпреступники по-прежнему заинтересованы в атаках на владельцев мобильных устройств под управлением ОС Android, поэтому в 2016 году пользователям таких смартфонов и планшетов будут вновь угрожать многочисленные вредоносные приложения.

В течение последних 12 месяцев наблюдалось активное распространение троянских программ, пытавшихся получить root-доступ на Android-устройствах, – эта тенденция, вероятно, сохранится. Кроме того, возможны новые случаи внедрения вредоносного ПО непосредственно в прошивку смартфонов и планшетов.

Весьма вероятно, что вирусописатели предпримут новые попытки украсть деньги с банковских счетов пользователей при помощи специализированных троянцев-банкеров.

Также стоит ожидать появления большого числа новых агрессивных рекламных платформ, которые недобросовестные разработчики и даже вирусописатели будут внедрять в распространяемые ими программы.

В то же время возрастающий интерес злоумышленников к устройствам под управлением iOS может означать, что их владельцам также стоит подготовиться к увеличению числа атак со стороны вирусописателей – вполне возможно, что в 2016 году киберпреступники предпримут новые попытки заразить смартфоны и планшеты производства компании Apple. При этом троянцы IPhoneOS.Trojan.XcodeGhost и **IPhoneOS.Trojan.YiSpecter.2** показали, что опасность заражения iOS-устройств, на которых не выполнена процедура «jailbreak», вполне реальна, поэтому пользователям смартфонов и планшетов с немодифицированной версией мобильной ОС от компании Apple также необходимо оставаться начеку.

Обзор вирусной активности для мобильных устройств за 2015 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