Dr.WEB®
с 1992 года

Обзор вирусной активности для мобильных Android-устройств в апреле 2017 года

Обзор вирусной активности для мобильных Android-устройств в апреле 2017 года

28 апреля 2017 года

В апреле был обнаружен Android-троянец, предназначенный для кибершпионажа. Также в прошедшем месяце в каталоге Google Play было выявлено несколько банкеров, созданных для похищения конфиденциальной информации и кражи денег со счетов. Один троянец был встроен в программы для просмотра видео из Интернета, другой представлял собой приложение-фонарик.

Главные тенденции апреля

- Обнаружение троянца-шпиона для ОС Android
- Проникновение банковских троянцев в каталог Google Play

Обзор вирусной активности для мобильных Android-устройств в апреле 2017 года

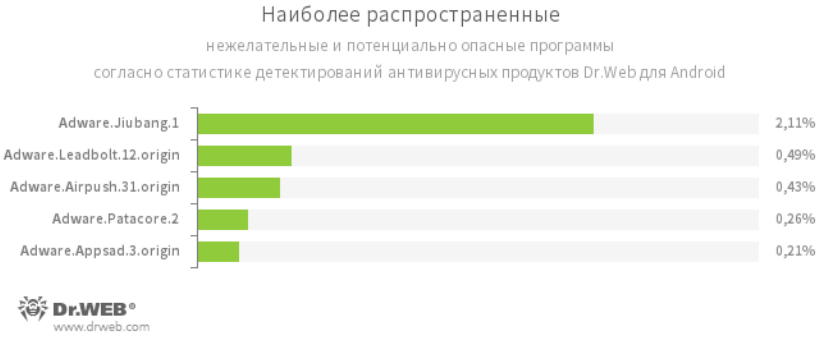
«Мобильная» угроза месяца

В апреле был обнаружен троянец Android.Chrysaor.1.origin, которого вирусописатели использовали для кибершпионажа. Эта вредоносная программа похищала переписку из множества программ для онлайн-общения, таких как Skype, Viber, WhatsApp и других, крала историю веб-браузера, СМС-сообщения и другие конфиденциальные данные. Кроме того, она отслеживала работу клавиатуры мобильного устройства и перехватывала всю вводимую информацию, создавала снимки экрана и выполняла «прослушку» окружения, незаметно отвечая на звонки киберпреступников.

По данным антивирусных продуктов Dr.Web для Android

- **Android.HiddenAds.83.origin**
- **Android.HiddenAds.76.origin**
- **Android.HiddenAds.68.origin**
- **Android.HiddenAds.93**
  Троянцы, предназначенные для показа навязчивой рекламы. Распространяются под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают их в системный каталог.
- **Android.Sprovider.9**
  Троянская программа, предназначенная для показа навязчивой рекламы в панели уведомлений ОС Android, а также загрузки и запуска других приложений, в том числе вредоносных.

Обзор вирусной активности для мобильных Android-устройств в апреле 2017 года



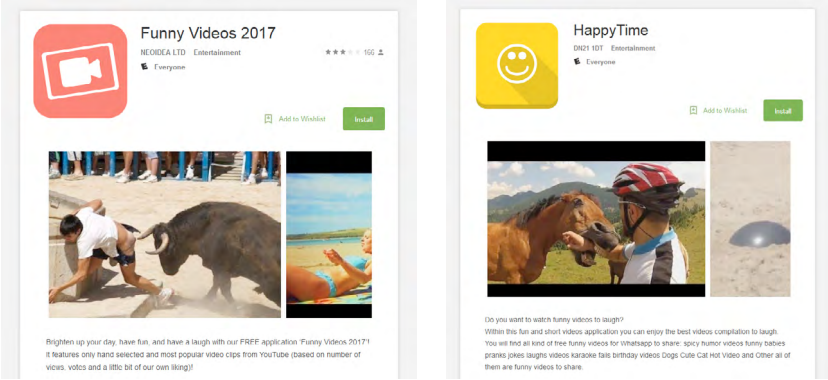
- **Adware.Jiubang.1**
- **Adware.Leadbolt.12.origin**
- **Adware.Airpush.31.origin**
- **Adware.Patacore.2**
- **Adware.Appsad.3.origin**

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

Обзор вирусной активности для мобильных Android-устройств в апреле 2017 года

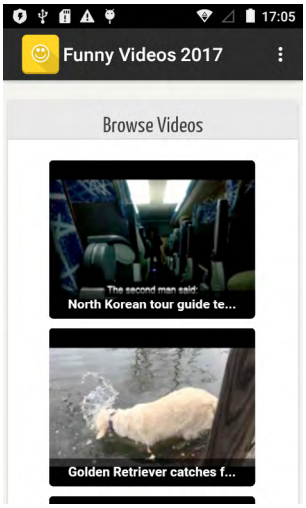
Банковские троянцы

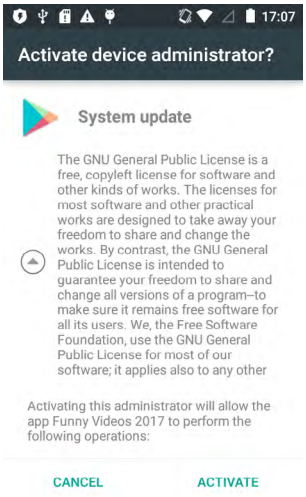
В апреле в каталоге Google Play было обнаружено несколько банковских троянцев для ОС Android. Один их них был добавлен в вирусную базу Dr.Web как Android.BankBot.179.origin. Он скрывался в приложениях под названием Funny Videos 2017 и HappyTime, предназначенных для просмотра юмористических видео. Этот троянец является модификацией другого Android-банкера, о котором компания «Доктор Веб» рассказывала в январе. Он основан на исходных кодах, опубликованных вирусописателями в открытом доступе.



Android.BankBot.179.origin получает от управляющего сервера конфигурационный файл со списком банковского и другого ПО, работу которого он будет отслеживать. При запуске любой банковской программы из этого списка троянец показывает поверх нее поддельное окно авторизации для ввода логина и пароля. Если же пользователь запускает приложение Google Play, Android.BankBot.179.origin отображает мошенническую форму настройки платежного сервиса и запрашивает данные банковской карты. Кроме того, этот троянец отслеживает входящие СМС-сообщения и перехватывает поступающие проверочные коды.

Обзор вирусной активности для мобильных Android-устройств в апреле 2017 года

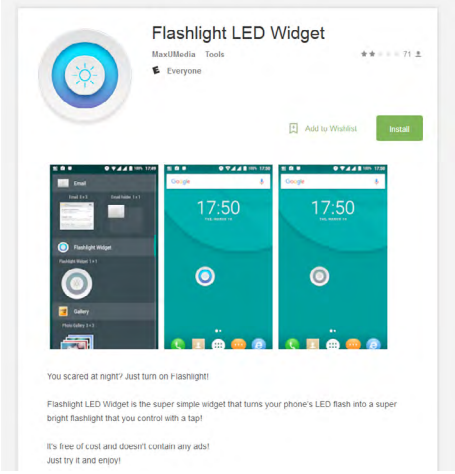




Особенности Android.BankBot.179.origin:

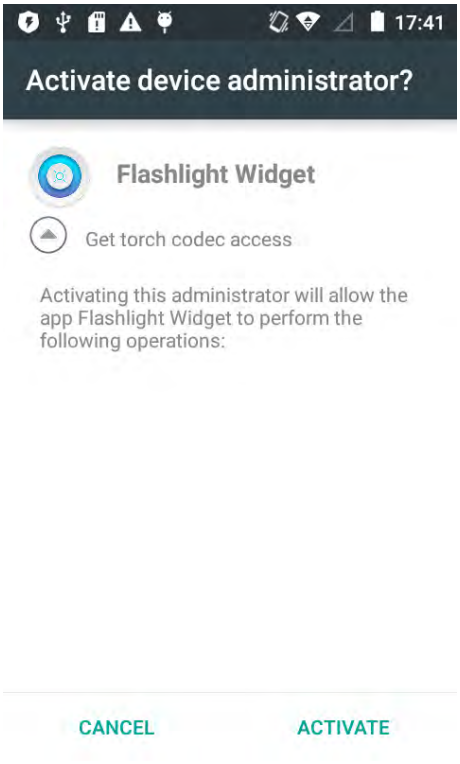
- создан на основе исходного кода банковского троянца, который вирусописатели разместили в Интернете;
- распространялся через каталог Google Play;
- встроен в полнофункциональное приложение-видеоплеер;
- через некоторое время после запуска запрашивает доступ к функциям администратора мобильного устройства, чтобы затруднить свое удаление;
- может атаковать сотни банковских программ и другое популярное ПО – злоумышленникам достаточно обновить конфигурационный файл.

Другой Android-банкер, обнаруженный в Google Play в апреле, получил имя Android.BankBot.180.origin. Он был встроен в приложение-фонарик под названием Flashlight LED Widget. При запуске этот троянец удаляет свой значок с домашнего экрана и запрашивает доступ к правам администратора мобильного устройства. После этого работа фонарика контролируется через виджет вредоносной программы.



Обзор вирусной активности для мобильных Android-устройств в апреле 2017 года

Android.BankBot.180.origin отслеживает запуск банковских программ и показывает поверх них поддельное окно ввода логина и пароля. Аналогично троянцу Android.BankBot.179.origin, это вредоносное приложение пытается украсть у пользователя данные о банковской карте, отображая мошенническую форму при запуске Google Play.



Android-банкеры являются одними из самых опасных вредоносных программ, поскольку с их помощью киберпреступники похищают деньги со счетов. Еще большую угрозу представляют банковские троянцы, которые распространяются через Google Play. Этот каталог считается наиболее надежным источником ПО для мобильных устройств под управлением ОС Android, поэтому владельцы смартфонов и планшетов проявляют меньшую осторожность при загрузке приложений из него. Для защиты от банковских троянцев и других опасных программ пользователям следует установить антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных Android-устройств в апреле 2017 года

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

Полезные ресурсы
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