Dr.WEB®
с 1992 года

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

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

31 января 2017 года

В первом месяце 2017 года специалисты компании «Доктор Веб» обнаружили Android-троянца, который внедрялся в рабочий процесс программы Play Маркет и незаметно скачивал приложения из каталога Google Play. Позднее вирусные аналитики исследовали банковского троянца, исходный код которого вирусописатели разместили в Интернете. Кроме того, в январе был выявлен другой Android-банкер, распространявшийся под видом игры Super Mario Run, которая все еще недоступна для Android-устройств. Также в прошлом месяце в каталоге Google Play был найден троянец-вымогатель, блокировавший экран Android-смартфонов и планшетов.

Главные тенденции января

- Обнаружение Android-троянца, который внедрялся в активный процесс приложения Play Маркет и незаметно загружал программы из каталога Google Play
- Распространение новых банковских троянцев
- Обнаружение в каталоге Google Play троянца-вымогателя

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

«Мобильная» угроза месяца

В начале января вирусные аналитики компании «Доктор Веб» обнаружили троянца Android.Skyfin.1.origin, который внедрялся в работающий процесс приложения Play Маркет, крал конфиденциальные данные и незаметно скачивал приложения из каталога Google Play, искусственно увеличивая их популярность. Особенности Android.Skyfin.1.origin:

- распространяется другими вредоносными программами, которые пытаются получить root-полномочия и устанавливают троянца в системный каталог;
- крадет аутентификационные данные и другую конфиденциальную информацию из приложения Play Маркет, имитирует его работу и незаметно для пользователя скачивает программы из каталога Google Play;
- после загрузки приложений сохраняет их на карту памяти, но не устанавливает, чтобы не вызывать подозрений у владельца зараженного мобильного устройства;
- оставляет в каталоге Google Play поддельные отзывы на указанные злоумышленниками программы.

Подробнее об этом троянце рассказано в публикации, размещенной на сайте компании «Доктор Веб».

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

По данным антивирусных продуктов Dr.Web для Android

- **Android.Loki.34**
  Вредоносная программа, предназначенная для загрузки других троянцев.
- **Android.Xiny.26.origin**
  Троянец, который загружает и устанавливает различные приложения, а также показывает навязчивую рекламу.
- **Android.DownLoader.337.origin**
  Троянец, предназначенный для загрузки других вредоносных приложений.
- **Android.Triada.161.origin**
  Представитель многофункциональных троянцев, выполняющих разнообразные вредоносные действия.
- **Android.Mobifun.7**
  Троянец, предназначенный для загрузки других Android-приложений.

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

- **Adware.Adpush.7**
- **Adware.Airpush.31.origin**
- **Adware.Leadbolt.12.origin**
- **Adware.WalkFree.2.origin**
- **Adware.Appsad.3.origin**

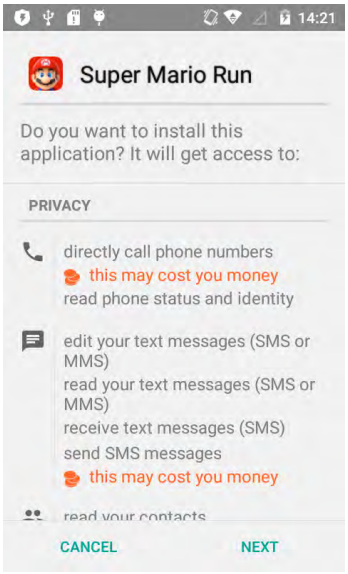
Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

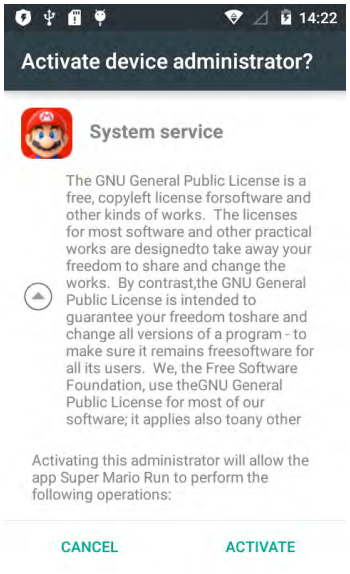
Android-банкеры

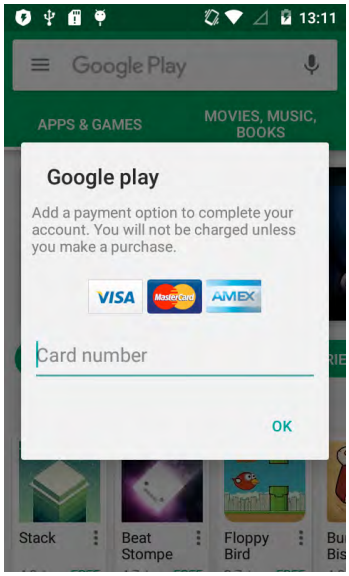
В январе владельцам Android-смартфонов и планшетов угрожал банковский троянец Android.BankBot.140.origin, которого вирусописатели распространяли под видом игры Super Mario Run. В настоящее время она доступна лишь для устройств под управлением iOS, поэтому при помощи такого обмана злоумышленники увеличивали вероятность того, что заинтересованные пользователи установят вредоносную программу.

Android.BankBot.140.origin отслеживал запуск банковских приложений и отображал поверх их окон фишинговую форму ввода логина и пароля для доступа к учетной записи пользователя. Кроме того, при открытии программы Play Маркет троянец пытался украсть информацию о банковской карте, показывая поддельное окно настройки платежного сервиса Google Play.

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

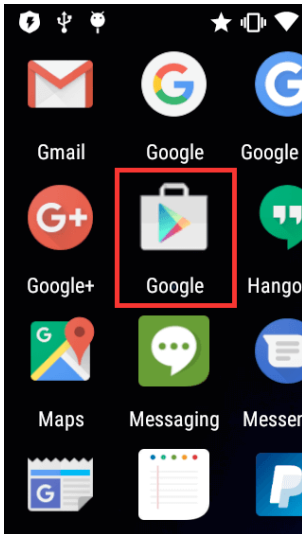


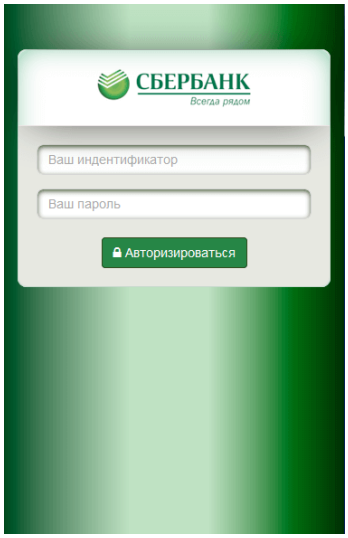


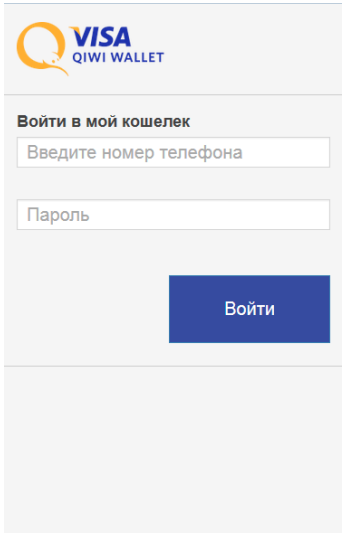


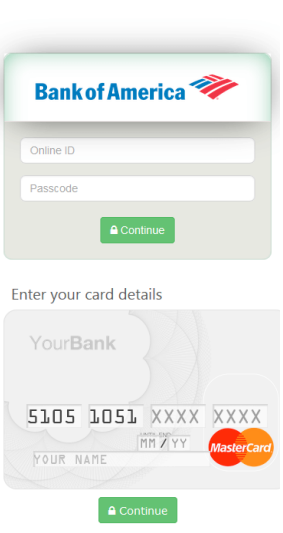
В середине месяца вирусные аналитики «Доктор Веб» обнаружили банковского троянца Android.BankBot.149.origin, исходный код которого вирусописатели ранее опубликовали в Интернете. Это вредоносное приложение отслеживало запуск программ для доступа к услугам дистанционного банковского обслуживания и платежным системам и показывало поверх них мошенническую форму для ввода логина и пароля от учетной записи пользователя. Кроме того, Android.BankBot.149.origin пытался получить сведения о банковской карте, показывая фишинговое окно поверх программы Play Маркет.

Также этот троянец перехватывал входящие СМС и пытался скрыть их, отслеживал GPS-координаты зараженного устройства, похищал информацию из телефонной книги и мог рассылать сообщения по всем доступным номерам. Подробнее об Android.BankBot.149.origin можно узнать, ознакомившись с опубликованной на сайте компании «Доктор Веб» новостью.





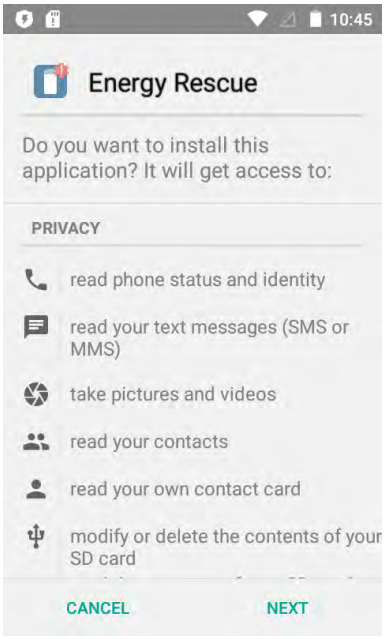


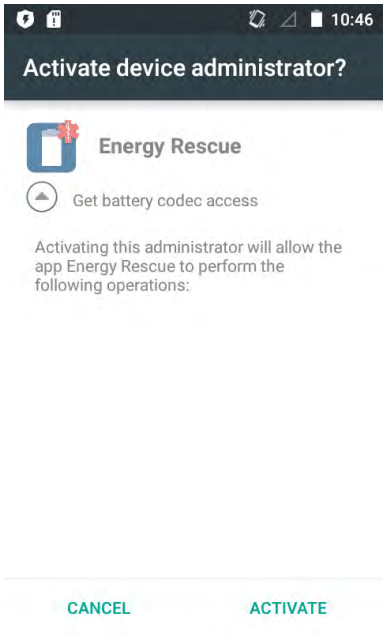


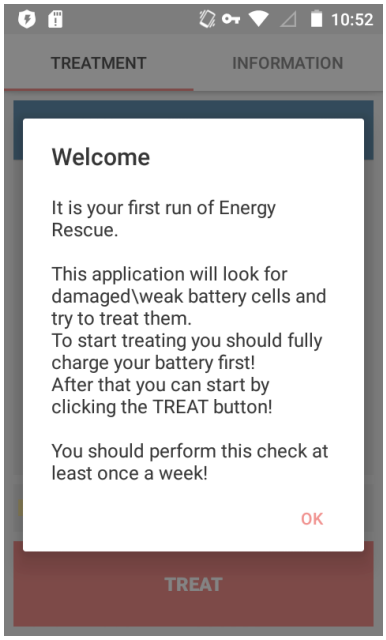
Обзор вирусной активности для мобильных Android-устройств в январе 2017 года

Троянцы в Google Play

В прошедшем месяце в каталоге Google Play был обнаружен троянец-вымогатель Android.Locker.387.origin, который для усложнения анализа и детектирования был защищен специальным упаковщиком. Несмотря на это, он успешно обнаруживается антивирусными продуктами Dr.Web для Android как Android.Packed.15893. Этот троянец распространялся под видом программы Energy Rescue, которая якобы оптимизировала работу аккумулятора. После запуска Android.Locker.387.origin запрашивал доступ к функциям администратора мобильного устройства и блокировал зараженный смартфон или планшет, требуя выкуп за его разблокировку. При этом устройства пользователей из России, Украины и Беларуси вымогатель не атаковал.







Помимо блокировки Android-устройств, Android.Locker.387.origin крал информацию об имеющихся в телефонной книге контактах и все доступные СМС-сообщения.

Киберпреступники по-прежнему проявляют интерес к мобильным устройствам под управлением ОС Android и создают множество новых вредоносных приложений для этой мобильной платформы. Для защиты смартфонов и планшетов пользователям рекомендуется установить антивирусные продукты Dr.Web для Android, которые успешно детектируют Android-троянцев и другие опасные программы.

Обзор вирусной активности для мобильных Android-устройств в январе 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