Dr.WEB®
с 1992 года

Обзор вирусной активности для мобильных Android-устройств в мае 2016 года

Обзор вирусной активности для мобильных Android-устройств в мае 2016 года

31 мая 2016 года

В мае вирусные аналитики компании «Доктор Веб» зафиксировали активность различных банковских троянцев, заражающих Android-смартфоны и планшеты. Так, продолжилось распространение банкера Android.SmsSpy.88.origin, способного атаковать клиентов множества кредитных организаций по всему миру. Кроме того, были выявлены мошеннические веб-сайты, которые киберпреступники используют для распространения вредоносного приложения Android.BankBot.104.origin и других банковских троянцев.

Главные тенденции апреля

- Распространение банковского троянца Android.SmsSpy.88.origin
- Появление новых мошеннических сайтов, помогающих злоумышленникам распространять банковских троянцев

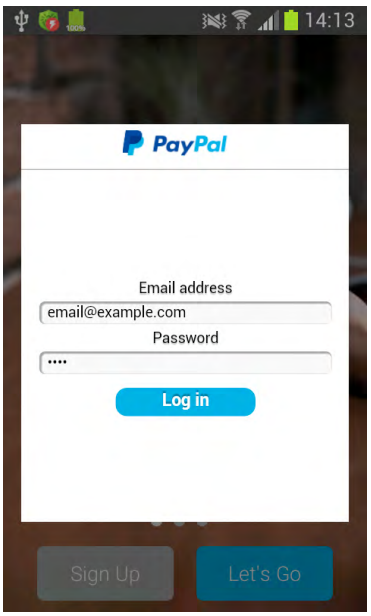
Обзор вирусной активности для мобильных Android-устройств в мае 2016 года

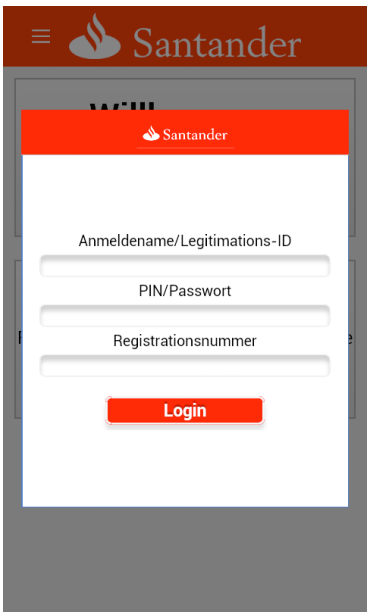
«Мобильная» угроза месяца

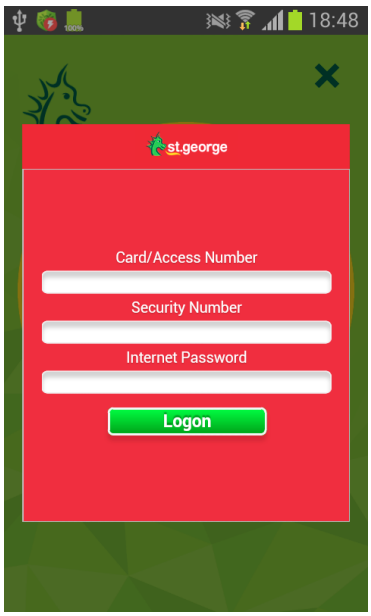
Всевозможные банковские троянцы по-прежнему представляют большую опасность для пользователей мобильных Android-устройств. Одна из таких вредоносных программ – Android.SmsSpy.88.origin – распространяется злоумышленниками с 2014 года. За это время функционал троянца значительно расширился, и к настоящему моменту этот банкер является серьезной угрозой для клиентов кредитных организаций по всему миру. В прошедшем мае распространение Android.SmsSpy.88.origin продолжилось.

Особенности Android.SmsSpy.88.origin:

- крадет логины и пароли от учетных записей мобильного банкинга, показывая поддельное окно аутентификации поверх запускаемых приложений «банк-клиент» (число атакуемых программ приближается к 100);
- похищает информацию о кредитных картах, показывая поддельное окно настроек платежного сервиса Google Play;
- перехватывает входящие СМС, а также незаметно рассылает сообщения;
- по команде управляющего сервера блокирует экран мобильного устройства и требует выкуп за разблокировку;
- препятствует работе ряда антивирусных приложений, не позволяя им запускаться.







Обзор вирусной активности для мобильных Android-устройств в мае 2016 года

По данным антивирусных продуктов Dr.Web для Android

- **Android.HiddenAds.1.origin**
  Троянец, предназначенный для показа навязчивой рекламы. Распространяется под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают его в системный каталог.
- **Android.Xiny.26.origin**
  Троянская программа, которая получает root-привилегии, проникает в системный каталог Android и в дальнейшем устанавливает различные программы без разрешения пользователя. Также может показывать навязчивую рекламу.
- **Android.CallPay.1.origin**
  Вредоносная программа, которая предоставляет владельцам Android-устройств доступ к эротическим материалам, но в качестве оплаты этой «услуги» незаметно совершает звонки на премиум-номера.
- **Android.DownLoader.662**
  Представитель семейства троянцев, предназначенных для загрузки и установки других вредоносных приложений.
- **Android.Sprovider.1**
  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 мае 2016 года

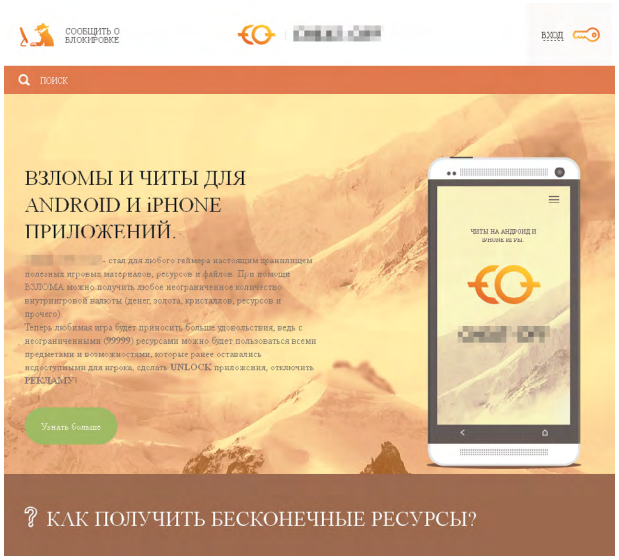
- **Adware.WalkFree.1.origin**
- **Adware.AdMogo.2.origin**
- **Adware.WalkFree.2.origin**
- **Adware.Leadbolt.12.origin**
- **Adware.Airpush.31.origin**

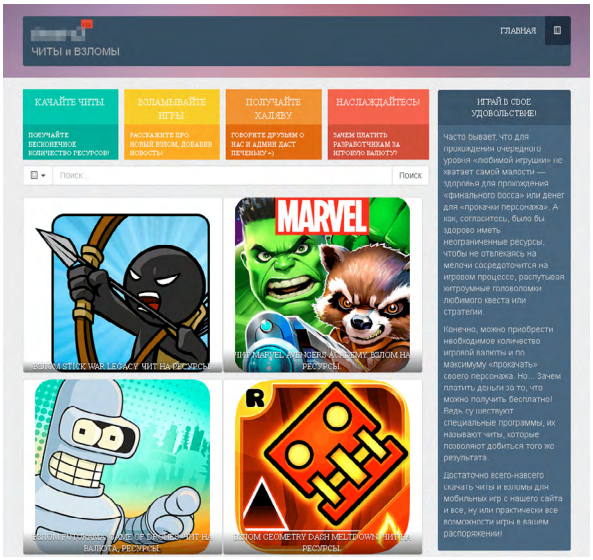
Нежелательный программный модуль, встраиваемый в Android-приложения и предназначенный для показа навязчивой рекламы на мобильных устройствах.

Обзор вирусной активности для мобильных Android-устройств в мае 2016 года

Банковские троянцы

Помимо троянца Android.SmsSpy.88.origin в мае владельцам Android-устройств угрожали и другие банкеры. Так, специалисты «Доктор Веб» выявили большое число мошеннических сайтов, которые злоумышленники используют для распространения банковских троянцев, в частности Android.BankBot.104.origin. На этих веб-порталах потенциальным жертвам предлагается загрузить программы для взлома множества игр и получения в них бесконечной игровой валюты и ресурсов. Однако при попытке загрузить это ПО пользователи перенаправляются на другой веб-сайт, с которого вместо ожидаемого приложения скачивается троянец.





Попадая на мобильное устройство, Android.BankBot.104.origin пытается украсть деньги с банковских счетов его владельца, может блокировать входящие сообщения и перехватывать их содержимое, а также незаметно отправлять СМС. Подробнее о троянце можно узнать из новости на сайте компании «Доктор Веб».

Банковские троянцы для ОС Android представляют серьезную угрозу для пользователей, а распространяющие эти вредоносные программы злоумышленники часто применяют различные приемы социальной инженерии, чтобы заставить владельцев смартфонов и планшетов установить такое ПО. Специалисты компании «Доктор Веб» рекомендуют не загружать программы с сомнительных веб-сайтов, даже если они содержат весьма заманчивые предложения.

Обзор вирусной активности для мобильных Android-устройств в мае 2016 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