Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в марте 2018 года

Обзор вирусной активности для мобильных устройств в марте 2018 года

3 апреля 2018 года

В марте 2018 года компания «Доктор Веб» опубликовала результаты исследования троянца Android.Triada.231, которого злоумышленники встроили в прошивки десятков моделей Android-смартфонов. Кроме того, в прошедшем месяце вирусные аналитики выявили большое число вредоносных программ в каталоге Google Play. Среди них был Android-банкер Android.BankBot.344.origin, предназначенный для кражи денег у российских пользователей, а также троянцы семейства Android.Click, способные загружать и показывать любые веб-страницы. Также в марте специалисты «Доктор Веб» обнаружили новых банковских троянцев, созданных на основе исходного кода Android.BankBot.149.origin.

Главные тенденции марта

- Выявление опасного троянца в прошивках десятков моделей мобильных Android-устройств
- Обнаружение вредоносных программ в Google Play
- Появление новых банковских троянцев

Обзор вирусной активности для мобильных устройств в марте 2018 года

Мобильная угроза месяца

В прошедшем месяце компания «Доктор Веб» сообщила об обнаружении троянца Android.Triada.231 в прошивках более 40 моделей Android-смартфонов. Эта вредоносная программа, известная с 2017 года, заражает процессы всех работающих приложений и по команде киберпреступников может незаметно выполнять различные действия. Например, она способна устанавливать и удалять ПО. После того как специалисты «Доктор Веб» проинформировали производителей зараженных мобильных устройств о троянце, некоторые из этих компаний оперативно выпустили обновления прошивок, из которых Android.Triada.231 был удален.

Обзор вирусной активности для мобильных устройств в марте 2018 года

По данным антивирусных продуктов Dr.Web для Android

Android.HiddenAds.253

Android.HiddenAds.246.origin

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.Mobifun.4

Троянец, предназначенный для загрузки других Android-приложений.

Android.RemoteCode.117.origin

Троянская программа, которая скачивает и запускает различные программные модули, в том числе вредоносные.

Android.Packed.15893

Детект для Android-троянцев, защищенных программным упаковщиком.

Обзор вирусной активности для мобильных устройств в марте 2018 года

По данным антивирусных продуктов Dr.Web для Android

Adware.Adtiming.1.origin

Adware.Adpush.601

Adware.Jiubang.2

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

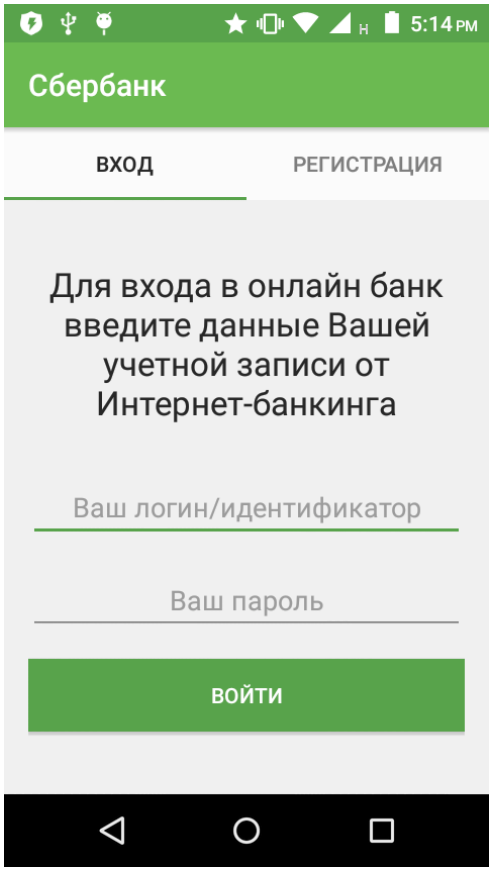
Tool.SilentInstaller.1.origin

Tool.SilentInstaller.6.origin

Потенциально опасные программы, предназначенные для незаметного запуска приложений без вмешательства пользователя.

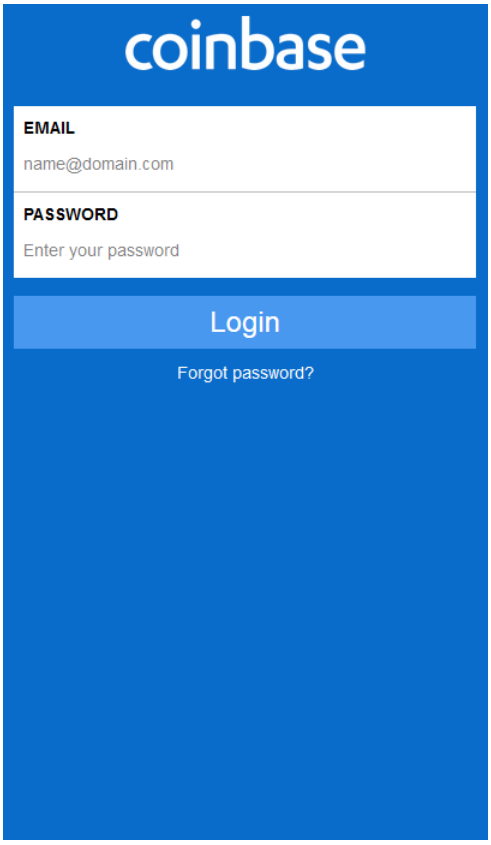
Банковские троянцы

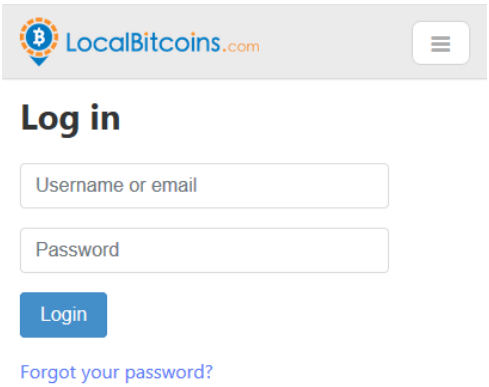
В начале прошедшего месяца вирусные аналитики «Доктор Веб» обнаружили в каталоге Google Play троянца Android.BankBot.344.origin, который распространялся под видом универсального приложения для работы с системами онлайн-банкинга нескольких российских кредитных организаций. Вредоносная программа предлагала потенциальной жертве войти в банковскую учетную запись, указав логин и пароль, либо зарегистрироваться, предоставив сведения о банковской карте. Вся вводимая информация передавалась киберпреступникам, после чего они могли украсть деньги с пользовательских счетов. Подробнее о троянце рассказано в новости, опубликованной на сайте компании «Доктор Веб».



Банковские троянцы

В середине марта специалисты «Доктор Веб» рассказали о новых Android-банкерах, созданных с использованием исходного кода вредоносного приложения Android.BankBot.149.origin. Один из них получил имя Android.BankBot.325.origin. Этот троянец отслеживает запуск банковских программ, а также ПО для работы с социальными сетями и криптовалютами и показывает поверх их окон мошеннические формы авторизации. После того как пользователи вводят логины, пароли и другую конфиденциальную информацию, Android.BankBot.325.origin передает ее злоумышленникам. Кроме того, вирусописатели могут использовать троянца для кибершпионажа и дистанционного доступа к зараженным устройствам.

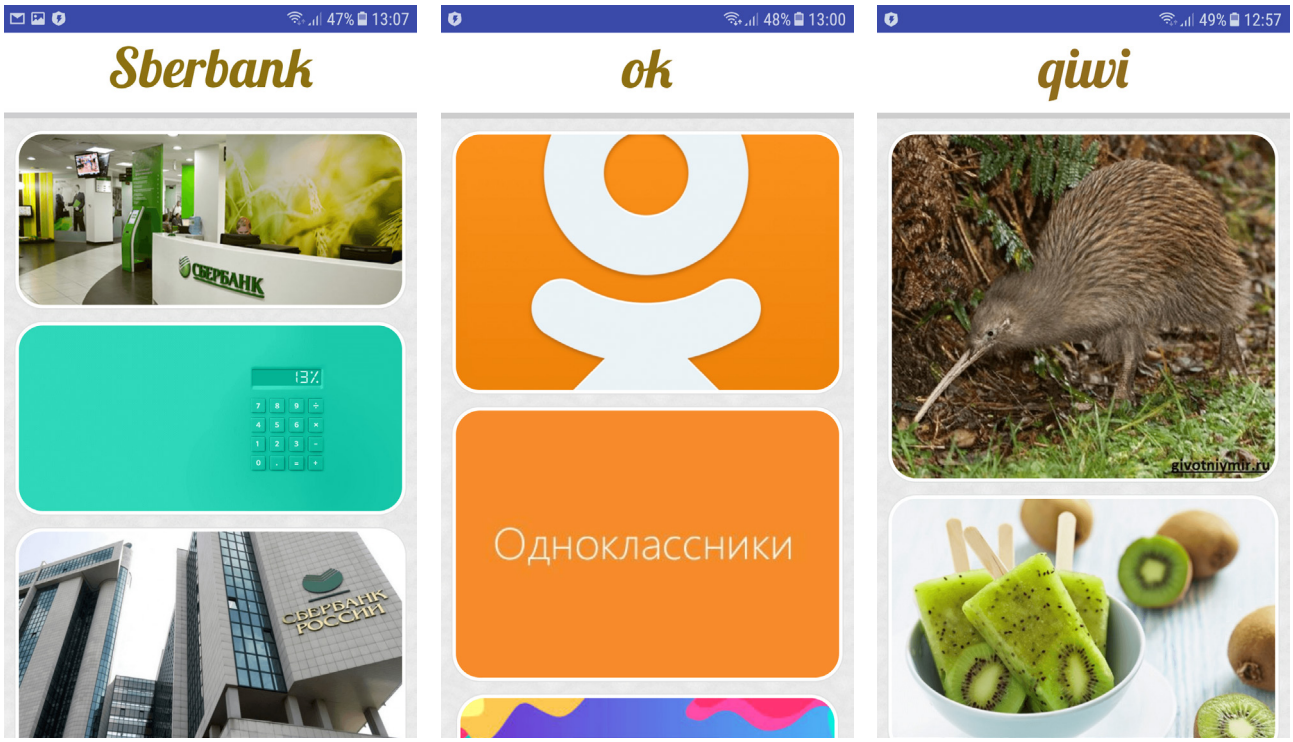




Обзор вирусной активности для мобильных устройств в марте 2018 года

Троянцы в Google Play

В марте специалисты «Доктор Веб» выявили в Google Play более 70 программ с троянцами семейства Android.Click. Вредоносные приложения, получившие имена Android.Click.415, Android.Click.416 и Android.Click.417, распространялись под видом известного ПО, внутри поддельных игр, в различных сборниках рецептов и пособиях по вязанию. Эти троянцы по команде управляющего сервера могли загружать и показывать любые веб-страницы, в том числе мошеннические.



Вредоносные программы для мобильных Android-устройств представляют серьезную угрозу, т. к. с их помощью злоумышленники крадут конфиденциальную информацию, управляют зараженными смартфонами и планшетами и похищают деньги с банковских счетов. Вирусописатели по-прежнему распространяют троянцев через каталог Google Play и встраивают их в прошивки. Для защиты мобильных устройств от вредоносных и нежелательных приложений пользователям следует установить антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных устройств в марте 2018 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
125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах