Новая угроза для macOS распространяется под видом WhatsApp

news.drweb.ru/show/

Doctor Web

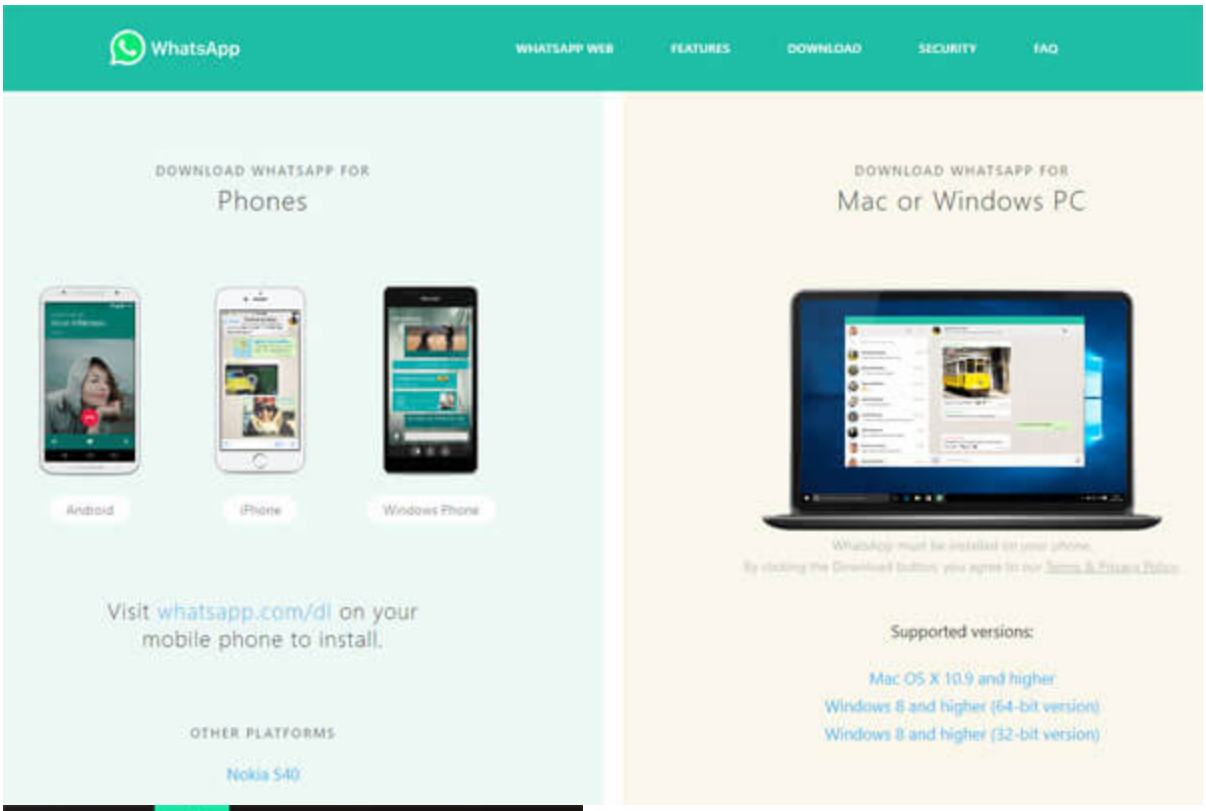
Назад к списку новостей

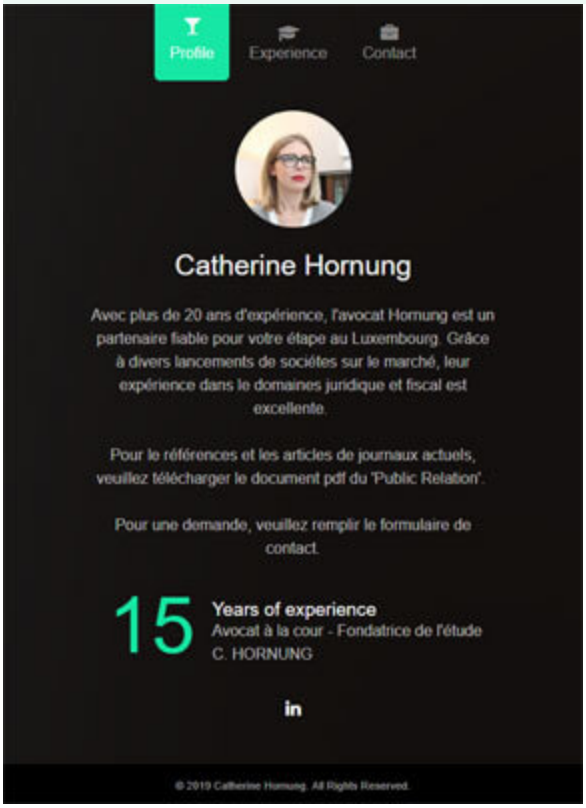
8 мая 2019 года

Специалисты «Доктор Веб» обнаружили угрозу для операционной системы macOS, позволяющую загружать и исполнять на устройстве пользователя любой код на языке Python. Кроме того, сайты, распространяющие это вредоносное ПО, также заражают опасным шпионским троянцем пользователей ОС Windows.

Новая угроза для устройств под управлением macOS была обнаружена нашими специалистами 29 апреля. Это вредоносное ПО получило название **Mac.BackDoor.Siggen.20** и представляет собой бэкдор, позволяющий загружать с удаленного сервера вредоносный код и исполнять его.

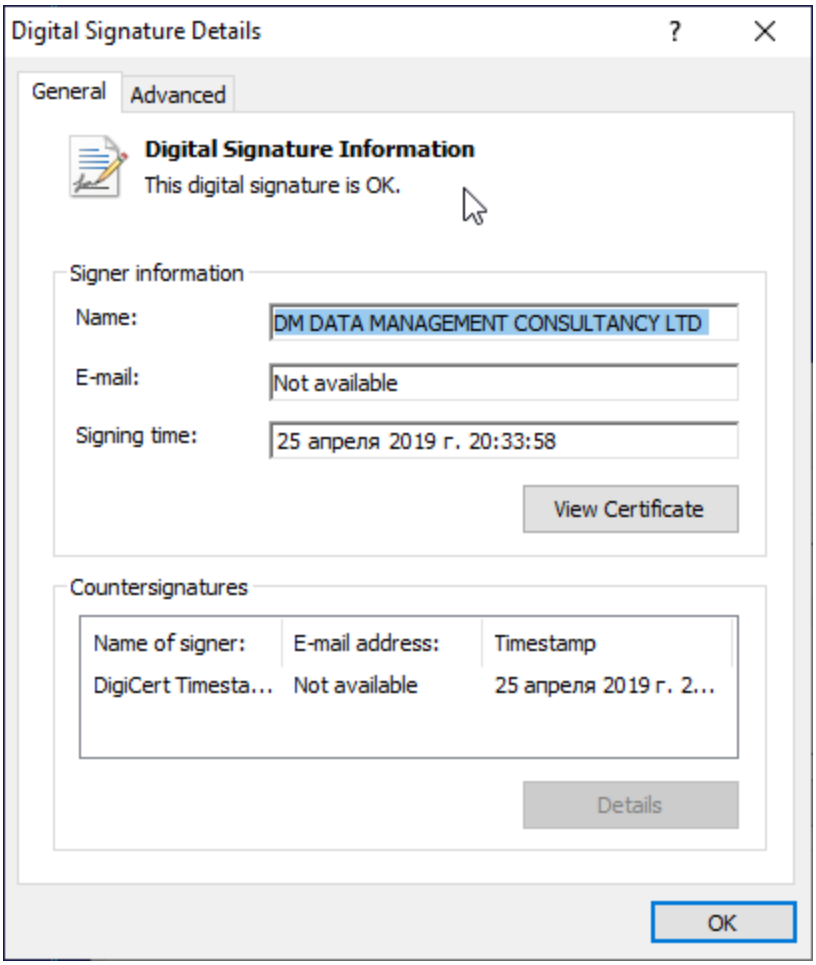
Mac.BackDoor.Siggen.20 попадает на устройства через сайты, принадлежащие его разработчикам. Один такой ресурс оформлен как сайт-визитка с портфолио несуществующего человека, а второй замаскирован под страницу с приложением WhatsApp.





При посещении этих ресурсов встроенный код определяет операционную систему пользователя и в зависимости от нее загружает бэкдор или троянца. Если посетитель использует macOS, его устройство заражается **Mac.BackDoor.Siggen.20**, а на устройства с ОС Windows загружается **BackDoor.Wirenet.517** (NetWire). Последнее является давно известным RAT-троянцем, с помощью которого хакеры могут удаленно

управлять компьютером жертвы, включая использование камеры и микрофона на устройстве. Кроме того, распространяемый RAT-троянец имеет действительную цифровую подпись.



По нашим данным, сайт, распространяющий **Mac.BackDoor.Siggen.20** под видом приложения WhatsApp, открывали около 300 посетителей с уникальными IP адресами. Вредоносный ресурс работает с 24.03.2019 и пока не использовался хакерами в масштабных кампаниях. Тем не менее специалисты «Доктор Веб» рекомендуют проявлять осторожность и вовремя обновлять антивирус. На данный момент все компоненты **Mac.BackDoor.Siggen.20** успешно детектируются только продуктами Dr.Web.

Подробнее об угрозе

Чтобы проголосовать надо войти на страницу новости через аккаунт на сайте «Доктор Веб» (или создать аккаунт). Аккаунт должен быть связан с вашим аккаунтом в социальной сети для наград за активности в них. Видео о связывании аккаунта

В чем преимущества аккаунта? | Как зарабатывать Dr.Web-ки?

Поделитесь информацией с вашими друзьями в социальных сетях

Нам важно Ваше мнение

Комментарии размещаются после проверки модератором. Чтобы задать вопрос по новости администрации сайта, укажите в начале своего комментария @admin. Если ваш вопрос к автору одного из комментариев — поставьте перед его именем @

Другие комментарии

— Российский разработчик антивирусов Dr.Web с 1992 года

— Dr.Web в Реестре Отечественного ПО

— Dr.Web совместим с российскими ОС и оборудованием

— Dr.Web пользуются в 200+ странах мира

— Техническая поддержка 24x7x365 Рус | En

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года.

125124, Россия, Москва, 3-я улица Ямского поля, д.2, корп.12А