

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.

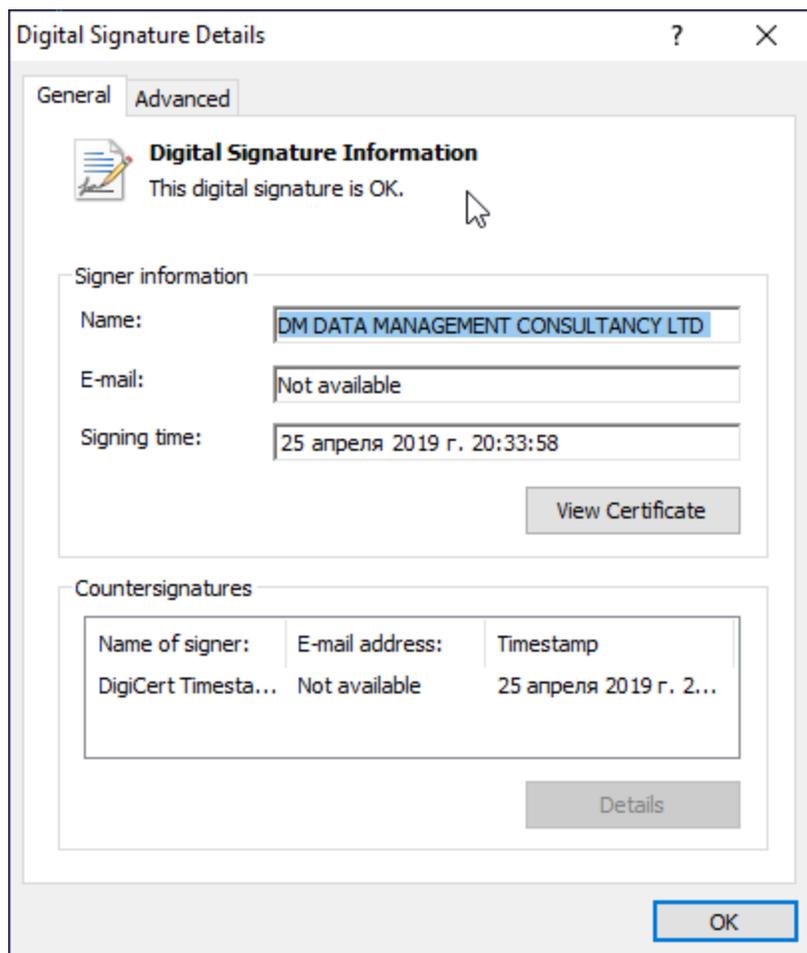
Mac.BackDoor.Siggen.20 попадает на устройства через сайты, принадлежащие его разработчикам. Один такой ресурс оформлен как сайт-визитка с портфолио несуществующего человека, а второй замаскирован под страницу с приложением WhatsApp.

The image shows the top portion of the WhatsApp website. At the top is a teal navigation bar with the WhatsApp logo and the text 'WhatsApp' on the left, and links for 'WHATSAPP WEB', 'FEATURES', 'DOWNLOAD', 'SECURITY', and 'FAQ' on the right. Below this, the page is split into two main sections. The left section, titled 'DOWNLOAD WHATSAPP FOR Phones', features three smartphone images labeled 'Android', 'iPhone', and 'Windows Phone'. Below these images, it says 'Visit whatsapp.com/dl on your mobile phone to install.' and 'OTHER PLATFORMS' with a link for 'Nokia S40'. The right section, titled 'DOWNLOAD WHATSAPP FOR Mac or Windows PC', shows a laptop displaying the WhatsApp web interface. Below the laptop, it states 'WhatsApp must be installed on your phone. By clicking the Download button, you agree to our [Terms & Privacy Policy](#).' and lists 'Supported versions: Mac OS X 10.9 and higher, Windows 8 and higher (64-bit version), Windows 7 and higher (32-bit version)'.

The image shows a LinkedIn profile page for Catherine Hornung. At the top, there are navigation tabs for 'Profile', 'Experience', and 'Contact'. The profile picture shows a woman with glasses. Below the name 'Catherine Hornung', there is a bio in French: 'Avec plus de 20 ans d'expérience, l'avocat Hornung est un partenaire fiable pour votre étape au Luxembourg. Grâce à diversancements de sociétés sur le marché, leur expérience dans le domaines juridique et fiscal est excellente.' Below the bio, there are two lines of text: 'Pour le références et les articles de journaux actuels, veuillez télécharger le document pdf du 'Public Relation'' and 'Pour une demande, veuillez remplir le formulaire de contact.' At the bottom, there is a large '15' followed by 'Years of experience' and 'Avocat à la cour - Fondatrice de l'étude C. HORNUNG'. The LinkedIn logo is at the bottom, along with the copyright notice '© 2010 Catherine Hornung. All Rights Reserved.'

При посещении этих ресурсов встроенный код определяет операционную систему пользователя и в зависимости от нее загружает бэкдор или троянец. 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?](#)

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»

2003 — 2022

«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