aut. Szymon Palczewski 04.03.2021

100 WŁOSKICH BANKÓW CELEM HAKERÓW

100 włoskich banków oraz ich klientów było celem hakerów, którzy wykorzystali nowy wariant trojana bankowego do kradzieży wrażliwych informacji, w tym danych do logowania do kont. Wirus był rozpowszechniany w wiadomościach phishingowych i znajdował się w pliku Word. Specjaliści znaleźli również ponad 1700 skradzionych danych uwierzytelniających dla jednego z procesów płatności.

Specjaliści z Avast Threat Labs udało się uzyskać informacje na temat kampanii hakerskiej podczas której wykorzystano złośliwe oprogramowanie o nazwie „Ursnif". Jak tłumaczą eksperci, jest to wirus powstały w 2007 roku jako trojan bankowy, lecz przez lata ewoluował stając się „trwałym zagrożeniem" w cyberprzestrzeni.

Avast wskazuje, że Ursnif od lat jest wykorzystywany do atakowania użytkowników w wielu państwach na całym świecie, często za pomocą wiadomości phishingowych. Jednak w ostatnim czasie hakerzy zwrócili szczególną uwagę na Włochy i tamtejszy sektor bankowy. Xiaopeng Zhang z Fortinet już w połowie stycznie br. ostrzegał o rosnącej liczbie incydentów w tym kraju, które były związane z użyciem wirusa Ursnif. Specjalista wówczas informował o rozsyłaniu przez hakerów e-maili zawierających nowy wariant złośliwego oprogramowania, ukryty w pliku MS Word. Ich treść została napisana w języku włoskim i stanowiła przypomnienie o rzekomej płatności.

> *Drogi Kliencie,*
>
> *Niedawny audyt księgowy wykazał, że Twoja faktura o numerze 294316 z dnia 12.10.2020 wygasła 12.11.2020. Na dzień dzisiejszy opłata nie została jeszcze przez Ciebie uiszczona.*
>
> *Dlatego prosimy o jak najszybsze unormowanie płatności. Przypominamy również, że opłaty tej można dokonać przelewem bankowym przy użyciu numeru IBAN wskazanego na fakturze lub czekiem bądź przekazem bankowym.*
>
> *Możesz zapoznać się z fakturą i szczegółami płatności w załączonym pliku.*
>
> *Dziękujemy za uwagę i pozdrawiamy.*
>
> *Treść wiadomości phishingowej*

Pobranie, a następnie otwarcie zainfekowanego pliku powoduje instalację złośliwego oprogramowania. Xiaopeng Zhang wskazuje, że Ursnif zbiera poufne informacje z urządzenia ofiary, takie jak dane logowania, a także szczegóły na temat urządzenia (m.in. systemu operacyjnego).

Specjaliści Avast Threat Labs zidentyfikowali w sieci informacje, które pochodzą z kradzieży danych dokonanej przy użyciu wirusa Ursnif. Mowa tu np. o nazwach użytkowników, hasłach, kartach kredytowych, bankowości czy płatnościach. Eksperci odkryli dowody świadczące, że celem hakerów było ponad 100 włoskich banków i ich klientów. „Znaleźliśmy również ponad 1700 skradzionych danych uwierzytelniających dla jednego z procesów płatności” – wskazuje Avast.

Zespół specjalistów Avasta wskazał, że zebrał wszelkie zdobyte informacje na temat kampanii i udostępnił je podmiotom obsługującym płatności oraz bankom, które udało się zidentyfikować. Szczegóły zostały także przekazane specjalistycznym instytucjom i organizacjom, w tym m.in. CERTFin Italy. Na bazie udostępnionych informacji mają one podjąć odpowiednie kroki, aby zapewnić ochronę swoim klientom i pomóc we wzmocnieniu cyberbezpieczeństwa.

Czytaj też: Jak chronić się przed cyberprzestępcami w czasie pandemii? Kampania informacyjna NASK i Policji