aut. Szymon Palczewski 17.01.2020

PERSONEL ONZ OFIARĄ PHISHINGU. SETKI OSÓB POSZKODOWANYCH

Personel ONZ padł ofiarą złośliwej kampanii phishingowej. Głównym celem hakerów była kradzież wrażliwych danych oraz stworzenie podstaw pod bardziej zaawansowane cyberataki z wykorzystaniem ransomware. Jakie są szczegóły ukierunkowanej operacji?

Celem złośliwej kampanii były setki osób, które pracowały dla ONZ lub były z nią blisko związane. Cyberprzestępcy podczas operacji posługiwali się trojanem TrickBot – informuje serwis ThreatPost.

W ramach operacji hakerzy spreparowali e-maile, które rzekomo pochodziły ze Stałej Misji Norweskiej przy ONZ. Jak wskazuje Bleeping Computer, fikcyjne wiadomości zostały wysłane na 600 adresów, powiązanych z personelem organizacji. Ich treść informowała o nieprawidłowościach związanych z podpisaną niedawno umową. W celu rozwiązania problemu użytkownicy byli zachęcani do kliknięcia w zainfekowany dodatek wiadomości.

Załączony w e-mailu plik zawierał złośliwe oprogramowanie. Hakerzy ukryli trojana w dokumencie Microsoft Word, którego nazwa w każdym przypadku rozpoczynała się od „Doc_01_13”. Wiadomości zostały rzekomo podpisane przez Stałą Misję Norweską przy ONZ, aby dodatkowo wzbudzić zaufanie wśród odbiorców – donosi Bleeping Computer.

Specjaliści Cofense wskazują, że kliknięcie w złośliwy załącznik otwiera nową witrynę z informacją, że „dokument jest dostępny tylko dla wersji Microsoft Office Word na komputery stacjonarne lub laptopy”. Następnie pojawia się funkcja „enable content”, której kliknięcie otwiera złośliwy plik, umożliwiający hakerom zainfekowanie danego urządzenia.

Jak informuje ThreatPost, wirus TrickBot umożliwiał cyberprzestępcom kradzież informacji (np. pliki cookies czy dane logowania) oraz stworzenie podstaw pod kolejny cyberatak z wykorzystaniem oprogramowania ransomware. Użyte w kampanii złośliwe oprogramowanie po raz pierwszy zostało wykryte przez specjalistów w 2016 roku i przez lata było regularnie udoskonalane przez hakerów.

Czytaj też: Szybko usuń te fotki – ostrzeżenie o nowej kampanii phishingowej