

HAKERZY ATAKUJĄ WHO. SZUKAJĄ INFORMACJI O KORONAWIRUSIE?

Grupa hakerów DarkHotel próbowała włamać się do systemów Światowej Organizacji Zdrowia na początku tego miesiąca – informuje Reuters. To jedna z najpoważniejszych prób tego rodzaju w ostatnim czasie.

Chief security officer Światowej Organizacji Zdrowia Flavio Aggio powiedział, że atak skończył się niepowodzeniem. Dodał również, że nie udało się ustalić tożsamości atakujących. Liczba prób włamania do systemów agencji i jej partnerów znacznie wzrosła i jest związana z epidemią koronawirusa – dodał.

Reuters został poinformowany o incydencie przez Alexandra Urbeilisa, eksperta ds. cyberbezpieczeństwa i prawnika pracującego w Nowym Jorku. Urbeilis zajmuje się śledzeniem rejestracji podejrzanych witryn w Internecie. 13 marca udało mu się wysledzić aktywność, która wzbudziła jego zaniepokojenie - ktoś próbował stworzyć stronę bliźniaczą podobną do wewnętrznego systemu poczty elektronicznej WHO. Amerykański badacz w rozmowie z Reutersem wspomina, że szybko zdał sobie sprawę, że jest świadkiem ataku na Światową Organizację Zdrowia i to w środku kryzysu wywołanego przez pandemię koronawirusa. Ekspert przyznał, że wysledził tysiące stron o tematyce COVID-19, które powstają praktycznie każdego dnia. Dodał, że z taką sytuacją ma do czynienia po raz pierwszy w życiu.

Światowa Organizacja Zdrowia potwierdziła, że strona znaleziona przez Urbeilisa została wykorzystana w próbie kradzieży haseł od pracowników organizacji. Odpowiedzialny za bezpieczeństwo informatyczne Flavio Aggio powiedział Reutersowi, że liczba prób przełamania zabezpieczeń wzrosła dwukrotnie w ostatnim czasie.

Urbeilis przyznał, że nie wie kto może być sprawcą, ale dwa inne źródła twierdzą, że za atakiem stoi zaawansowana grupa hakerska DarkHotel, która przeprowadza kampanie cyberszpiegowskie od 2007 roku.

Wcześniej WHO opublikowało także ostrzeżenie przed hakerami, którzy próbują podszyć się pod organizację i wykraść pieniądze oraz wrażliwe dane. Komunikat o podobnej treści został opublikowany również przez Stany Zjednoczone i Wielką Brytanię.

Motywy ataku pozostają nieznane - donosi Reuters. Przypomina również, że agencje ONZ w tym WHO są regularnie atakowane przez cyberszpiegów. Pewien trop co do potencjalnego agresora mają firmy zajmujące się cyberbezpieczeństwem - rosyjski Kaspersky i rumuński BitDefender. Wskazują, że wiele śladów działalności DarkHotel prowadzi do Azji Wschodniej. Hakerzy mieli tam atakować przedstawicieli sektora publicznego i prywatnego w Chinach, Japonii i Stanach Zjednoczonych. Część specjalistów podejrzewa, że grupa jest powiązana z Koreą Północną.

Ekspert Kaspersky'ego wskazuje, że nie można jednoznacznie stwierdzić, że do DarkHotel stoi za atakiem. W komentarzu dla Reutersa przypomina, że podobne operacje z wykorzystaniem złośliwych domen były przeprowadzane przeciwko organizacjom medycznym na całym świecie.

Należy jednak podkreślić, że obecnie informacje o szczepionce czy lekarstwie są na wagę złota dlatego też wywiady wielu państw z pewnością są nimi zainteresowane.