5 MLN USD ZA ODBLOKOWANIE SYSTEMÓW PRZEDSIĘBIORSTWA NAFTOWEGO. HAKER STAWIA ŻĄDANIA

5 mln dolarów okupu za odblokowanie systemów komputerowych przedsiębiorstwa naftowego Petroleos Mexicanos (Pemex). Taką kwotę zażądał haker, który przejął kontrolę nad sieciami firmy. Spółka nie zgadza się na opłatę i chce rozwiązać problem samodzielnie - podała agencja Bloomberga.

Przestępca posługujący się pseudonimem "Joseph Atkins" żąda uiszczenia opłaty w wysokości 565 bitcoinów (w przeliczeniu 4,8 mln USD) do końca miesiąca. W zwrotnej wiadomości e-mail dla Bloombeg News haker odmówił skomentowania sprawy do upływu terminu 30 listopada.

"Atkins" zaznaczył, że jego grupa prowadzi działania nie tylko na firmach paliwowych, sugerując, że był też współodpowiedzialny za ataki na firmę usług transportu ciężarowego Roadrunner Transportation z 2018 r. "Nie zapłacili nam i sami odzyskali system, ale zostawili nam gigabajty danych" - wskazał haker. Agencja zwraca uwagę na to, że posługuje się on łamanym angielskim. Bloomberg uzyskał adres hakera z oryginalnej informacji z żądaniem okupu, skierowanej do Pemeksa.

Meksykańska firma oświadczyła, że nie zapłaci żądanej sumy, a problem cyberataku rozwiąże samodzielnie - wynika z komentarza minister ds. energii Rocio Nahle. Petroleos Mexicanos również odmówiło komentarza, nie potwierdzając, czy haker faktycznie wyznaczył firmie ostateczny termin na opłacenie okupu. Koncern w sprawozdaniu z tego tygodnia wyjaśnił, że atak nie wpłynął na działanie firmy i dotknął ok. 5 proc. komputerów.

Zdaniem Bloomberga nielegalna operacja na Pemeksie jest kolejnym przykładem rozwijającego się trendu. Hakerzy dostający się do nieprawidłowo zabezpieczonych systemów komputerowych korporacji biorą za zakładnika dane, których międzynarodowe firmy potrzebują do codziennego funkcjonowania. Niektóre odmawiają współpracy z przestępcami, ale inne po cichu płacą okup, co napędza kolejne ataki tego typu.

Jeszcze w środę pracownicy Pemeksu byli instruowani by nie korzystać z firmowej sieci Wi-Fi i nie logować się na swoje komputery - poinformowały źródła Bloomberga. We wtorek technicy komputerowi zajęci byli formatowaniem zainfekowanych urządzeń i instalacją aktualizacji bezpieczeństwa - dodał jeden z informatorów.

W chwili obecnej Pemex polega na ręcznym rozliczaniu, co może wpłynąć na proces wypłacania pensji dla kadr i opłat dla dostawców, a także wydłużyć czas oczekiwania w łańcuchu dostaw - wskazują osoby pragnące zachować anonimowość. Pracownicy obawiają się problemu z wypłatami, planowanymi na 27 listopada.

Nie zidentyfikowano wirusa będącego przyczyną problemu, lecz według niektórych poszlak może być to oprogramowanie wymuszające pod nazwą DoppelPaymer - wskazała firma cyberbezpieczeństwa Crowdstrike. Eksperci wcześniej powiązali adres mailowy "Atkinsa" z uprzednimi atakami z wykorzystaniem tej techniki.