

PARTNER AMERYKAŃSKIEGO WOJSKA ZHAKOWANY. W SIECI KRAŻY PLIK Z DANymi

Amerykański koncern technologiczny padł ofiarą złośliwej kampanii ransomware. Hakerzy wykradli dane znajdujące się w wewnętrznych systemach firmy, żądając okupu za ich odzyskanie. Władze przedsiębiorstwa nie przystały na zapłacenie wskazanej kwoty, w wyniku czego skradzione pliki zostały opublikowane w sieci.

Kimchuk, producent elektroniki dla sprzętu medycznego, systemów telekomunikacyjnych, sieci energetycznych oraz urządzeń dla marynarki wojennej z siedzibą w Danbury padł ofiarą złośliwego cyberataku. W wyniku incydentu zainfekowane zostały sieci i systemy firmy. Podczas kampanii cyberprzestępcy wykorzystali najnowszą odmianę złośliwego oprogramowania ransomware do kradzieży danych, a następnie zażądali okupu za ich odzyskanie – informuje serwis TechCrunch.

Firma nie zapłaciła wskazanej sumy pieniędzy, na skutek czego hakerzy zaczęli publikować pozyskane pliki w sieci. Znajdowały się w nich między innymi dane finansowe przedsiębiorstwa, zatwierdzenia brokerów czy zamówienia zakupu. Specjaliści wskazują, że obecnie udostępnione informacje nie należy uznać za tajne.

Na razie nie wiadomo dokładnie, kiedy złośliwa kampania miała miejsce. Analiza incydentu sugeruje jednak, że ostatni zamieszczony w sieci plik z danymi został opublikowany 5 marca bieżącego roku, co świadczy, iż cyberatak mógł mieć miejsce pod koniec lutego.

„Incydenty związane z oprogramowaniem ransomware należy traktować jako naruszenie bezpieczeństwa danych, dopóki nie można ustalić, że jest inaczej” – podkreślił ekspert firmy Emsisoft Brett Callow, cytowany przez serwis TechCrunch.

Czytaj też: [Ransomware zmusza dostawcę technologii dla banków do wyłączenia systemów](#)