Cyberdefence 24

aut. Szymon Palczewski 25.03.2020

PRZEMYSŁ NA BLISKIM WSCHODZIE ZAATAKOWANY PRZEZ HAKERÓW

Hakerzy ponownie uderzyli na Bliskim Wschodzie. Głównym ich celem były przedsiębiorstwa i instytucje branży przemysłowej. Eksperci wskazują, że kampania była unikalna oraz ukierunkowana na inżynierów pracujących w tym sektorze. Obecnie nie wiadomo kto odpowiada za cyberataki.

Specjaliści z firmy Kaspersky odkryli kampanię hakerską, w ramach której cyberprzestępcy posługiwali się złośliwym oprogramowaniem w celu przeprowadzania ukierunkowanych cyberataków na podmioty z Bliskiego Wschodu. Wśród poszkodowanych znajdują się między innymi firmy z branży przemysłowej.

Jak wskazują eksperci, złośliwym oprogramowaniem, którym posługiwali się hakerzy był trojan C++. Analiza działań cyberprzestepców nie wykazała żadnych podobieństw do znanych współcześnie kampanii. Wirus prawdopodobnie służył do cyberszpiegostwa. „Cyberataki są unikalne i ukierunkowane. Nadaliśmy im nazwę WildPressure" – czytamy na oficjalnej stronie Kaspersky.

Obecnie specjaliści nie posiadają jednoznacznych danych na temat mechanizmu rozprzestrzeniania złośliwego oprogramowania. Nieznane jest również źródło kampanii. Wiadomo jedynie, że hakerzy przeprowadzali złośliwe cyberataki wymierzone w specjalistów branży przemysłowej. Tego typu operacje trwały od dłuższego czasu w regionie Bliskiego Wschodu.

„Za każdym razem, gdy celem jest sektor przemysłowy, jest to sytuacja niepokojąca" – czytamy na oficjalnej stronie firmy. Jeden z analityków Kaspersky Lab Denis Legezo podkreślił, że nic nie wskazuje na to, aby hakerzy zrobili cokolwiek innego poza gromadzeniem informacji.

„Doszliśmy do wniosku, że jest to grupa APT, ponieważ złośliwe oprogramowanie jest rzadkie, atakuje bardzo konkretny region i nadaje się do szpiegostwa" – zaznaczył specjalista na łamach CyberScoop. – „Jak dotąd nie posiadamy danych na temat ewentualnego sponsorowania przez państwo".

Czytaj też: Iran buduje cyberszpiegowską potęgę? Kampania wymierzona w Turcję, Jordanię i Irak