Cyberdefence 24

aut. Sylwia Gliwa 05.12.2019

SEKTOR ENERGETYCZNY NA BLISKIM WSCHODZIE ZNÓW POD CYBEROSTRZAŁEM. MOŻLIWE POWIĄZANIA Z IRANEM

Sektor energetyczny na Bliskim Wschodzie jest pod kolejnym cyberatakiem. Nowe złośliwe oprogramowania ZeroCleare które uderzyło w przedsiębiorstwa przemysłowe i energetyczne prawdopodobnie jest powiązanie prowadzonej kampanii z grupami pracującymi na zlecenie irańskiego rządu – twierdzi IBM X-Force.

IBM X-Force potwierdza, że od 2012 roku bada i śledzi destrukcyjne oprogramowanie, wykorzystywane do uderzeń i wywoływanie zakłóceń w sektorze przemysłowym i energetycznym. Eksperci IBM nazwali nowo odkryte oprogramowanie „ZeroCleare" a z uwagi na brak wcześniejszych przejawów wykorzystania tego oprogramowania, nie wykluczają, że zostało ono opracowane niedawno. Wykryta kampania jest prawdopodobnie jedną z pierwszych która z niego korzysta.

Na podstawie analizy oprogramowania oraz jego zastosowania, eksperci uważają, że mogło być ono stworzone przez Irańskich hakerów. Oprogramowanie wykazuje podobieństwo do działania, znanego już z bardzo destrukcyjnych skutków dla sektora naftowego, oprogramowania Shamoon, który w 2012 r. był odpowiedzialny za poważne zniszczenia infrastruktury informacyjnej w państwowej firmie naftowej w Arabii Saudyjskiej. Podobnie jak Shamoon, również ZeroCleare atakuje główny rekord rozruchowy (MBR) i partycje dyskowe w bazujących na systemie Windows urządzeniach.

Cyberprzestępcom udało się dokonać szkód na „dużej liczbie urządzeń" – informuje IBM. Z uwagi na znaczne rozprzestrzenienie się na wiele urządzeń w atakowanej sieci, eksperci przewidują, że może on w najbliższym czasie wpłynąć a tysiące urządzeń i powodować zakłócenia, których usunięcie może potrwać nawet miesiące. Zastosowana taktyka przypominają sposób, w jaki Shamoon został wykorzystany podczas ataków na cele w Zatoce Arabskiej w 2018 roku.

Jak wskazuje IBM w swoim komunikacie „niszczycielskie ataki na sektory energetyczny i przemysłowy budzą coraz większy niepokój, szczególnie w krajach, w których gospodarka opiera się na przemyśle naftowym i gazowym, podobnie jak w niektórych częściach Bliskiego Wschodu i Europy". X-Force IRIS odnotowało znaczny do 200 procentowy wzrost liczby ataków w porównaniu pierwszej połowy 2019 roku do drugiej połowy 2018 roku. Kluczowa rola wydobycia i przetwarzania ropy i gazu zarówno na poziomie krajowym, jak i globalnym stanowi wartościowy cel dla sponsorowanych przez państwo podmiotów. Działania mogą zostać skupione wokół szpiegostwa przemysłowego czy doprowadzenie do zakłóceń w funkcjonowaniu infrastruktury krytycznej jako elementu prowadzonych wrogich działań pomiędzy państwami.

Ataki ZeroCleare, zdaniem ekspertów IBM, wydają się być ukierunkowanymi operacjami przeciwko konkretnym organizacjom. Oceniają również, że możliwe jest przypisanie odpowiedzialności za przygotowanie i wykorzystanie złośliwego oprogramowania do irańskich grup hakerskich

sponsorowanych przez rząd.