Cyberdefence 24

aut. Szymon Palczewski 29.03.2019

IRAN NĘKA SWOICH WROGÓW. HAKERZY NARUSZAJĄ SYSTEMY WIELU SEKTORÓW

W ostatnich trzech latach eksperci ds. cyberbezpieczeństwa firmy Symantec zaobserwowali wzmożoną działalność irańskiej grupy hakerskiej, której głównym celem są organizacje, instytucje oraz inne podmioty znajdujące się na terenie Arabii Saudyjskiej oraz Stanów Zjednoczonych.

Eksperci wskazują, że celem irańskich hakerów są instytucje badawcze, organizacje państwowe, systemy rządowe oraz wiele innych podmiotów różnych sektorów (m.in. finansowego, przemysłowego, telekomunikacyjnego, energetycznego).

Grupa znana jako Elfin lub APT33 została już wcześniej zauważona przez FireEye. Po przeprowadzeniu analiz specjaliści stwierdzili, że „APT33 działa na zlecenie irańskiego rządu", a jej głównym obiektem zainteresowania jest sektor lotniczy.

Jon DiMaggio, ekspert Symantec, zaznaczył, że hakerzy posługują się złośliwym oprogramowaniem o nazwie Stonedrill. „To trojan, który ma na celu wymazanie danych z dysków twardych zainfekowanych systemów, czyniąc je bezużytecznymi dla ofiary" – tłumaczy.

Działalność Elfin opiera się na wykorzystaniu luk w zabezpieczeniach, które nie są systematycznie ulepszane i rozwijane przez operatorów. Przykładem może być cyberatak wymierzony w saudyjską organizację sektora chemicznego, gdzie hakerzy próbowali wykorzystać błąd w oprogramowaniu przeznaczonego do archiwizacji plików WinRAR.

Jak informuje Nalani Fraser, specjalista FireEye, w zeszłym miesiącu irańscy hakerzy rozsyłali zainfekowane e-maile do osób powiązanych z sektorem energetycznym. W ich treści zawarty był załącznik WinRAR, który zawierał w sobie złośliwe oprogramowanie.

Według specjalistów Symantec APT33 „jest jedną z najbardziej aktywnych grup działających obecnie na Bliskim Wschodzie". Wykazuje ona stałą „gotowość do ciągłego doskonalenia swojej taktyki i znajdowania wszelkich narzędzi potrzebnych do przeprowadzenia cyberataku na kolejne grupy ofiar".

Arabia Saudyjska i Stany Zjednoczone są dwoma największymi geopolitycznymi rywalami Iranu. Amerykanie postrzegają Teheran jako główne zagrożenie dla państwa, obok Rosji, Korei Północnej i Chin.