Cyberdefence 24

aut. Szymon Palczewski 10.01.2020

IRAN SPARALIŻUJE STANY ZJEDNOCZONE W ODWECIE?

Rosnące napięcie między Waszyngtonem a Teheranem może skłonić irańskie władze do przeprowadzenia odwetu w postaci dotkliwego cyberataku. Mógłby on zostać wymierzony w amerykańską infrastrukturę krytyczną, wywołując chaos oraz częściowy paraliż państwa. Jednak czy Teheran stać na tak zaawansowaną operację w cyberprzestrzeni?

Irańscy hakerzy od dłuższego czasu prowadzili kampanie, których celem było uzyskanie dostępu do sieci i systemów amerykańskich przedsiębiorstw energetycznych. Działania cyberprzestępców miały miejsce na długo przez eskalacją napięć ze Stanami Zjednoczonymi – informuje serwis Wired.

Specjaliści firmy Dragos, prowadząc badania dotyczące najnowszych cyberataków, wykryli kampanię hakerską, w którą zaangażowani byli irańscy hakerzy. Cyberprzestępcy realizowali zadania w ramach szeroko zakrojonej operacji na rzecz kradzieży wrażliwych danych do logowania w amerykańskich przedsiębiorstwach sektora energetycznego. Eksperci wskazują, że złośliwe działania były prowadzone przez grupę APT33, zwaną również Elfin lub Refined. Jej hakerzy regularnie realizują zadania na zlecenie Teheranu.

Firma Dragos zaznaczyła, że połączone ze sobą kampanie kradzieży haseł i loginów były prowadzone przez cały 2019 rok. Specjaliści podkreślają, że podczas analizy złośliwych operacji nie trafili na żaden znak, aby irańscy hakerzy uzyskali dostęp do wyspecjalizowanego oprogramowania infrastruktury krytycznej, które odpowiada za kontrolę fizycznych urządzeń – donosi serwis Mashviral.

Joe Dragik, ekspert Dragos, w rozmowie dla Wired zaznaczył, że kampanie polegające na kradzieży haseł i loginów nie ograniczają się wyłącznie do operatorów branży energetycznej, choć to te podmioty są głównym celem. Zagrożenie dotyczy wszystkich firm zarządzających obiektami infrastruktury krytycznej. „Prowadzenie operacji na taką skalę, wydaje się nieukierunkowane, niechlujne lub chaotyczne, ale pozwala stworzyć stosunkowo szybko i tanio wiele punktów dostępu, które można rozszerzyć na działania, kontynuowane w wybranym przez nich miejscu” – wyjaśnił specjalista Dragos.

Wydaje się jednak, że przeprowadzenie niszczycielskiego cyberataku na amerykańską infrastrukturę krytyczną jest mało prawdopodobne. Irańscy hakerzy nie uzyskali dostępu do kluczowego oprogramowania wrażliwych obiektów, które zostały zbadane przez specjalistów. Ograniczenia grupy wspieranej przez Teheran wynikają między innymi z braku odpowiednich narzędzi.

Jednak w obliczu napiętej sytuacji między Iranem a Stanami Zjednoczonymi, amerykańskie podmioty odpowiedzialne za infrastrukturę krytyczną powinny poważnie podchodzi do dotychczasowych działań cyberprzestępców i nie lekceważyć ich złośliwych operacji. W obecnej sytuacji należy zachować wzmożoną czujność oraz wdrożyć dodatkowe zabezpieczenia, aby być gotowym na zagrożenie.

Sytuacja dotyczy również sojuszników Waszyngtonu, którzy również są narażeni na odwetowe operacje w cyberprzestrzeni prowadzone przez Iran. Jedną z ofiar agresywnej polityki Stanów Zjednoczonych na Bliskim Wschodzie jest ich bliski partner w tym regionie Arabia Saudyjska. Państwo to regularnie zmaga się ze złośliwą działalnością ze strony irańskich hakerów. W momencie eskalacji ostatnich wydarzeń Rijad padł ofiarą kolejnej kampanii, za której przeprowadzenie prawdopodobnie odpowiadają cyberprzestępcy sponsorowani przez Teheran.

Czytaj też: Cyberatak na Arabię Saudyjską. Irański odwet za działania Waszyngtonu?