aut. Szymon Palczewski 09.01.2020

CYBERATAK NA ARABIĘ SAUDYJSKĄ. IRAŃSKI ODWET ZA DZIAŁANIA WASZYNGTONU?

Cyberatak na saudyjskie organizacje i instytucje państwowe miał miejsce w momencie eskalacji napięcia na linii Teheran-Waszyngton. Jego celem było trwałe zniszczenie konkretnych baz danych o kluczowym znaczeniu. Specjaliści sugerują, że za złośliwą kampanię prawdopodobnie odpowiadają irańscy hakerzy działający na zlecenie rządu. Czy amerykańscy sojusznicy „zapłacą" za politykę Waszyngtonu na Bliskim Wschodzie?

29 grudnia 2019 roku Arabia Saudyjska padła ofiarą złośliwego cyberataku. Incydent miał miejsce w momencie eskalacji napięcia irańsko-amerykańskiego. Specjaliści podejrzewają, że autorem złośliwej kampanii jest jedna z grup hakerskich wspierana przez rząd w Teheranie – donosi serwis CyberScoop.

Złośliwe oprogramowanie, które wykorzystali cyberprzestępcy podczas cyberataku zostało nazwane przez specjalistów „Dustman". Jak informuje Yahoo News, eksperci przeanalizowali incydent, znajdując podobieństwa z poprzednimi kampaniami prowadzonymi przez irańskich hakerów. W świetle uzyskanych dowodów Teheran jest głównym podejrzanym.

Cyberatak został wykryty przez Saudi Arabia's National Cybersecurity Authority (NCA). Specjaliści państwowego organu wskazują, że podczas kampanii wykorzystano jeden z rodzajów złośliwego oprogramowania, przeznaczonego do trwałego usunięcia danych wybranych celów. Nie ujawniono jednak podmiotów, które padły ofiarą cyberataku.

Incydent pokazuje, w jaki sposób irańscy hakerzy wykorzystują złośliwe oprogramowanie do prowadzenia operacji, których celem jest wymazywanie baz danych konkretnych instytucji oraz organizacji, działających w regionie Bliskiego Wschodu. Najnowsza kampania jest potwierdzeniem ewoluującej taktyki prowadzonych przez Teheran operacji w cyberprzestrzeni.

Jeden ze specjalistów ds. cyberbezpieczeństwa, zajmujący się cyberatakami w tej części świata, wskazał w rozmowie dla CyberScoop, że ślady najnowszej kampanii prowadzą na trop irańskich grup hakerskich. Dodał, iż w porównaniu z poprzednimi złośliwymi operacjami skutki analizowanego incydenty są znacznie ograniczone. „Jednak szkody były ograniczone w porównaniu z poprzednimi latami" – podkreślił ekspert, który pragnął pozostać anonimowym.

Z kolei Adam Meyers, wiceprezes CrowdStrike, stwierdził, że niektóre elementy najnowszej kampanii zostały zaczerpnięte z operacji prowadzonych przez Teheran już w 2012 roku. „Cyberatak jest zgodny z irańskimi operacjami sięgającymi 2012 roku" – wskazał ekspert dla CyberScoop. „To jeden z wariantów narzędzi, których celem jest zniszczenie danych i wywołanie zakłóceń".

Złośliwa kampania miała miejsce dwa dni przed amerykańskim uderzeniem na irańskie cele, w wyniku którego śmierć poniósł Qassem Soleimani, dowódca elitarnej jednostki „Al Kuds". W wyniku rosnącego napięcia Departament Bezpieczeństwa Wewnętrznego USA ostrzegł przed możliwością nagłego

wzrostu aktywności grup hakerskich, sponsorowanych przez Teheran – informuje Yahoo News.

W tym miejscu warto zaznaczyć, że operacje w cyberprzestrzeni są bardzo tanim i równocześnie efektywnym narzędziem odwetowym, redukującym możliwość wszczęcia konwencjonalnego konfliktu. Arabia Saudyjska, jako sojusznik Stanów Zjednoczonych na Bliskim Wschodzie, może być jednym z głównych celów złośliwych kampanii ze strony irańskich hakerów.

Czytaj też: Amerykanie nie wycofują się z Kuwejtu. Hakerzy zaatakowali agencję medialną