AMERYKAŃSKI ATAK NA IRAN W CYBERPRZESTRZENI [ANALIZA]

Prezydent Donald Trump miał zatrzymać operacje odwetową przeciwko Iranowi 10 minut przed jej rozpoczęciem. Okazuje się jednak, że wstrzymano tylko działania powietrzne i morskie, ponieważ w cyberprzestrzeni Amerykanie zaatakowali irańską infrastrukturę – podają media w Stanach Zjednoczonych.

Celem operacji przygotowywanej przez ostatnie tygodnie było wyłączenie irańskich systemów komputerowych odpowiedzialnych za obronę przeciwrakietową oraz ośrodka szpiegowskiego monitorującego przepływ statków w cieśnienie Ormuz. Zaatakowane zostały systemy należące do irańskiej armii oraz Korpusu Strażników Rewolucji Islamskiej. Formacja ta została uznana przez administrację Trumpa za organizację terrorystyczną. Celem działań była również irańska grupa, która miała być odpowiedzialna za ataki na statki komercyjne w zatoce Ormuz.

Nie ujawniono szczegółów operacji, m.in. nie powiedziano czy udało się osiągnąć zakładane cele. Z informacji do których dotarł dziennik The Washington Post wynika, że operacja doprowadziła do poważnych zakłóceń w działaniu systemu obrony przeciwlotniczej. Iran jednak zaprzecza. Minister ds. łączności i technologii informacyjnej Mohammad Dżawad Azari Dżahrumi powiedział, że amerykańskie cyberataki nie powiodły się. Dodał, że krajowa zapora sieciowa miała w zeszłym roku zneutralizować 33 milionów ataków.

Cyberataki były jedną z opcji odpowiedzi na ataki na dwa tankowce, która została przedstawiona prezydentowi Trumpowi. Doniesienia medialne potwierdzają, że amerykański przywódca zdecydował się właśnie na taką formę odpowiedzi i osobiście zaaprobował takie działania. Operacja podjęta przez USCYBERCOM była demonstracją rosnących zdolności Stanów Zjednoczonych w cyberprzestrzeni oraz kolejnym dowodem potwierdzającym coraz agresywniejszą strategię w środowisku wirtualny, którą przyjęła administracja prezydenta Trumpa.

Obecny kryzys w Zatoce Perskiej jest rezultatem zaostrzenia się relacji między Waszyngtonem a Teheranem. Doszło do niego w momencie wycofania się Stanów Zjednoczonych z porozumienia nuklearnego z Iranem. Od tego czasu napięcie we wzajemnych relacjach tylko rośnie. Administracja prezydenta Trumpa stara się wywrzeć presję na Teheran, co omal nie doprowadziło do konwencjonalnego konfliktu zbrojnego, kiedy Irańczycy strącili amerykańskiego drona.

Konflikt irańsko-amerykański w cyberprzestrzeni

Operacja ofensywna przeprowadzona przez Amerykanów jest kolejnym z serii ciosów wymierzanych przez obie strony w cyberprzestrzeni. W ostatnich tygodniach, hakerzy, którzy mieli być powiązani z reżimem ajatollahów zaatakowali amerykańskie agencje rządowe oraz przedsiębiorstwa działające w sektorze finansowym. Celem była również infrastruktura krytyczna w sektorze energetycznym. Firmy badające incydenty: CrowdStrike i FireEye, wskazały, że głównym narzędziem ataku było wysyłanie

spearphisingowych emaili. Operacje te miały się rozpocząć w momencie nałożenia dodatkowych sankcji przez administrację Trumpa na irański sektor petrochemiczny w tym roku. Nie podano żadnych informacji na temat skutków ataku i tego, czy Irańczykom udało się włamać do zaatakowanych obiektów. Grupa zaangażowana w te operacje została określona kryptonimem „Refined Kitten" i od lata atakuje sektor energetyczny i wojskowy, jak również sojuszników Stanów Zjednoczonych takich jak Arabia Saudyjska czy Zjednoczone Emiraty Arabskie.

Nie można wykluczyć, że Iran wykorzysta jeszcze bardziej swój arsenał w cyberprzestrzeni do zaatakowania celów w Stanach Zjednoczonych. Irańczycy prowadzili takie operacje już w przeszłości. Wprawdzie zdolności Iranu nie mogą równać się z Amerykanami, ale nie można określić reżimu ajatollahów mianem słabego gracza w cyberprzestrzeni. Puntem zwrotnym dla rozwoju ich zdolności w przestrzeni wirtualnej był atak za pomocą Stuxenta na ośrodek wzbogacania uranu w Natanz. Od tego czasu Iran dynamicznie rozwija swoje możliwości działania. Wzmocnieniu uległa obrona najważniejszych elementów systemu bezpieczeństwa oraz infrastruktury krytycznej. Wiele z nich zostało również odłączonych od Internetu.

W oficjalnym oświadczeniu Departamentu Bezpieczeństwa Wewnętrznego (DHS) – odpowiedzialnego m.in. za ochronę infrastruktury krytycznej napisano, że urząd jest świadomy wysokiego ryzyka cyberataków, których autorem może być Iran oraz grupy z nim powiązane. Christopher C. Krebs, który odpowiada za agencję cyberbezpieczeństwa i infrastruktury w DHS powiedział, że współpracuje blisko z wspólnotą wywiadowczą oraz innymi podmiotami odpowiedzialnym za bezpieczeństwo monitorując irańską aktywność. W oficjalnym komunikacie prasowym NSA powiedziała, że w przeszłości występowało wiele incydentów cyberbezpieczeństwa, za którymi stał Iran. W czasie podwyższonego ryzyka, każdy powinien być bardziej wyczulony na wszystkie sygnały mogące świadczyć o ataku – czytamy w komunikacie NSA.

Operacje ofensywne Iranu w cyberprzestrzeni

W przeszłości, Iran wielokrotnie atakował infrastrukturę energetyczną, wodną czy systemy finansowe. Operacje te znacznie się zmniejszył po podpisaniu porozumienia nuklearnego. Po wycofaniu się z niego Stanów Zjednoczonych w 2018 roku, znowu aktywność irańskich hakerów uległa zwiększeniu. Iran zaatakował również sojuszników USA. W 2012 roku, jego celem stało się przedsiębiorstwo naftowe Saudi Aramco. Wirus wyczyścił dane z 30 tys. komputerów a na ekranie monitorów pojawiał się obraz przedstawiający palenie amerykańskiej flagi. Iran stał również za atakiem na amerykańskie kasyna w 2015 roku oraz w 2016 roku na banki w Stanach Zjednoczonych oraz tamę zlokalizowaną w pobliżu Nowego Jorku.

Irańczycy zaatakowali też członków 5 floty Stanów Zjednoczonych. W tym celu wykorzystali fałszywe profile na mediach społecznościach, przedstawiając się jako atrakcyjne kobiety szukające samotnych marynarzy. Osoby, które dały się nabrać na ten trik, dzieliły się z nimi informacjami. Irańczycy w ten sposób byli w stanie dowiedzieć się o ruchach okrętów marynarki Stanów Zjednoczonych.

Eksperci komentujący zaostrzające się relacje pomiędzy Iranem a Stanami Zjednoczonymi, podkreślają, że Teheran nie musi wykorzystywać dostępu, który uzyskał do sieci i systemów teleinformatycznych w USA. Może starać się je utrzymać na gorsze czasy i pogorszenie relacji z Waszyngtonem.

Zdaniem Davida Hoague, dyrektora technicznego z NSA, ostatnio irańscy hakerzy skupiają się głównie na zbieraniu informacji, a nie na niszczeniu danych. Głównych ich celem jest uzyskanie informacji na temat polityki USA w stosunki do Iranu. Grupy APT 33 i 34, które kojarzone są z reżimem ajatollahów wypróbują m.in. za pomocą metody siłowego łamania haseł uzyskać dostęp do kont wojskowych. Ze względu na fakt, że wiele osób używa tego samego hasła do kilku serwisów, strategia ta może okazać

się skuteczna.

Cyberprzestrzeń niezbędnym elementem operacji wojskowych

Były analityk NSA Oren Falkowitz podkreśla, że cyberataki nie są magicznym sposobem na wygrywanie wojen i nie maja takiej możliwości rażenia jak ładunki nuklearne. Powiedział, że planowanie operacji w cyberprzestrzeni trwa miesiącami. Zauważył też, że jeżeli zostaną użyte to bardzo trudno się jest bronić przed nimi.

Cyberatak na Iran nie jest żadnym zaskoczeniem. Obecnie każdy konflikt zbrojny zaczyna się od operacji w cyberprzestrzeni. Nie powinien również dziwić cel takiej działalności. Wszystkie dostępne plany działań przewidują zastosowanie środków w cyberprzestrzeni do oślepienia przeciwnika lub zneutralizowania jego systemów rozpoznania. Warto też zadać pytanie, czy fakt, że cyberatak został przeprowadzony bez współdziałania z innymi rodzajami wojsk jest błędem, wynikającym ze złej współpracy jednostek cyber z ich konwencjonalnymi odpowiednikami czy może częścią operacji psychologicznej. W końcu administracja Donalda Trumpa może odeprzeć krytykę przeciwników, że nie podjęła żadnych działań w odwecie za zestrzelenie amerykańskiego drona. Jest również pokazem dla Iranu możliwości Stanów Zjednoczonych, bo skoro udało się zneutralizować irańską obronę rakietową, to co jeszcze mogą zrobić Amerykanie?