Cyberdefence 24

aut. Szymon Palczewski 22.11.2019

INFRASTRUKTURA KRYTYCZNA ZAGROŻONA? NOWY ETAP DZIAŁALNOŚCI IRAŃSKICH HAKERÓW

Iran szykuje się do przeprowadzenia cyberataków, które doprowadzą do fizycznych zniszczeń. W ostatnim czasie państwowi hakerzy zmienili swoją strategię działania, skupiając się na podmiotach odpowiedzialnych za infrastrukturę krytyczną. Czarny scenariusz jest bardziej prawdopodobny niż sądzono?

Irańscy hakerzy odpowiadają za jedne z najbardziej destrukcyjnych cyberataków ostatniej dekady w regionie Bliskiego Wschodu. Wśród celów znajdowały się również amerykańskie przedsiębiorstwa, szpitale wojskowe oraz instytucje państwowe. W tym czasie w wyniku złośliwej działalności cyberprzestępcy zniszczyli sieci oraz systemy komputerowe ofiar, generując ogromne straty materialne.

Według specjalistów Microsoft podczas najnowszych kampanii hakerzy zmienili swój cel. Teraz działania cyberprzestępców koncentrują się na systemach fizycznej kontroli w zakładach przemysłowych, elektrowniach oraz rafineriach.

Przemawiając na konferencji CyberwarCon w Arlington, specjalista ds. cyberbezpieczeństwa firmy Microsoft Ned Moran opublikował wyniki analizy prowadzonej przez ekspertów, które pokazują, w jaki sposób zmieniła się działalność irańskiej grupy hakerskiej APT33, znanej również jako Elfin. Według badań w ciągu ostatnich dwóch miesięcy państwowi cyberprzestępcy znacznie zawęzili obszar swoich działań, przeprowadzając 2 tys. prób cyberataków miesięcznie, co oznacza duży spadek w stosunku do minionych lat. Ich skuteczność jest jednak duża wyższa. Jak wskazał Ned Moran, średnia naruszonych kont personelu poszkodowanych podmiotów jest prawie dziesięciokrotnie większa.

Microsoft skategoryzował cele, na które hakerzy APT33 ukierunkowali swoje działania. Według danych zaprezentowanych przez firmę około połowa ofiar to podmioty przemysłowe, w tym producenci, konserwatorzy sprzętu oraz dostawcy komponentów. Od połowy października br. irańscy cyberprzestępcy wymierzyli swoje działania w dziesiątki firm produkujących sprzęt przemysłowy oraz oprogramowanie sterujące.

Nieznane są jednak motywy hakerów. Ned Moran sugeruje, że prowadzone kampanie mogą być podstawą do przeprowadzenia bardziej zaawansowanych cyberataków, które będą miały fizyczne skutki. „Nękają firmy przemysłowe oraz producentów oprogramowania, ale nie sądzę, żeby to te podmioty były ich ostatecznym celem" – podkreślił ekspert Microsoft. – „Próbują gdzieś dalej znaleźć swoją ofiarę, poznać ją lepiej, wiedzieć z czego korzysta. Chcą wyrządzić realne szkody, uderzając w infrastrukturę krytyczną, aby sprawić ogromne zniszczenia".

Zmiana charakteru działań APT33 jest niepokojąca. Jednak obecnie nie wykryto żadnych śladów wskazujących na przeprowadzenie zaawansowanego cyberataku na infrastrukturę krytyczną przez irańskich hakerów. Podstawą ich działania jest naruszanie systemów w celu włamania się do sieci lub

na konkretne konta, a następnie wprowadzanie złośliwego oprogramowania do usuwania danych, znanego jako Shamoon.

Eksperci Microsoft nie podali nazw podmiotów, które padły ofiarą działalności Teheranu. Ned Moran ostrzega jednak, że ukierunkowanie grupy na systemy kontroli sugeruje, że Iran może wyjść poza ramy swojej dotychczasowej działalności, decydując się na poważny cyberatak, który doprowadzi do powstania fizycznych zniszczeń. „Biorąc pod uwagę ich dotychczasowy sposób działania, oczywiste jest, że Teheran w końcu zdecyduje się na niszczycielski atak" – podkreślił specjalista koncernu.

Stanowisko eksperta Microsoft popiera Sam Curry, specjalista Cybereason, który ostrzega, że większość państw wykazuje wysoką podatność na cyberataki wymierzone w infrastrukturę krytyczną. Tłumaczy, iż w większości przypadków jest ona na ogół przestarzała, źle zabezpieczona, nieodpowiednio zarządza i zaprojektowana dużo wcześniej, zanim pojawił się problem cyberbezpieczeństwa. „To wszystko sprawia, że możliwość wyrządzania ogromnych strat jest znacząca, jeśli atakujący wie, co robi" – wyjaśnił Sam Curry.

W sytuacji, gdy hakerzy uzyskują dostęp do systemów kontroli przemysłowej oraz innych narzędzi wchodzących w skład infrastruktury krytycznej, mogą przeprowadzić szeroki zakres cyberataków. Najbardziej niepokojące są działania, które mogą całkowicie zakłócić funkcjonowanie sieci elektroenergetycznej.

Z drugiej strony Adam Meyers, wiceprezes Crowdstrike, wskazuje, że nie należy wyolbrzymiać potencjału Iranu i doszukiwać się w jego działaniu najgorszych scenariuszy. Według eksperta równie dobrze Teheran może w przyszłości skupić się wyłącznie na cyberszpiegostwie. Uważa, że działania podejmowane przez państwowych hakerów są idealnym sposobem na „wejście" do wnętrza danego podmiotu i gromadzenie interesujących danych.

Wiadomość o możliwym cyberataku wymierzonym w elementy infrastruktury krytycznej pojawia się w chwili silnego napięcia w stosunkach irańsko-amerykańskich. Działalność APT33 ma na celu wywołanie poczucia chaosu i destabilizacji, a także zastraszenie regionalnych przeciwników oraz Stanów Zjednoczonych. Zjawisko to zostanie spotęgowane w momencie, gdy Teheran będzie posiadał wszelkie potrzebne środki do przeprowadzenia cyberataku, którego fizyczne skutki będą bardzo dotkliwe. „Próbują dać sygnał swoim przeciwnikom i zmienić ich zachowanie" – podkreślił Ned Moran, przedstawiciel Microsoft na konferencji CyberwarCon.

Warto również podkreślić, że sprawą irańskiej aktywności w ostatnim czasie zajął się amerykański wywiad. Jak pisaliśmy wcześniej, w raporcie opracowanym przez Defense Intelligence Agency specjaliści wyraźnie sprecyzowali plany Iranu, stwierdzając jednoznacznie, że „Teheran ma aspiracje do dominacji w cyberprzestrzeni". Co więcej, państwowi hakerzy wykorzystywani są jako jedno z narzędzi zapewniania bezpieczeństwa wewnętrznego państwa. Obawy amerykańskiej społeczności wywiadowczej budzi również fakt stale rosnących zdolności Iranu w cyberprzestrzeni oraz wsparcie tego państwa przez największych konkurentów Waszyngtonu – Chiny i Rosję – w zakresie cyberbezpieczeństwa.

Przedstawione powyżej fakty skłaniają ekspertów do prowadzenia ściślejszej obserwacji działalności irańskich hakerów w cyberprzestrzeni oraz próby odkrycia ich motywacji. Zmiana charakteru operacji APT33 wymusza również zwiększenie czujności oraz gotowość służb na ewentualny incydent. Zagrożenie staje się realne. Teheran posiada podstawowe zasoby, które w każdej chwili mogą zostać użyte. Dodatkowo jest wspierany przez kluczowe na arenie międzynarodowej państwa. Czy to wszystko oznacza, że Iran rzeczywiście staje się cyberpotęgą?

Czytaj też: Amerykański wywiad: „Iran ma aspiracje do dominacji w cyberprzestrzeni”