Cyberdefence 24

aut. Szymon Palczewski 22.11.2019

AMERYKAŃSKI WYWIAD: „IRAN MA ASPIRACJE DO DOMINACJI W CYBERPRZESTRZENI”

Iran wykorzystuje cyberoperacje jako jedno z narzędzi zapewniania bezpieczeństwa wewnętrznego państwa, a jego wirtualne zdolności stale rosną – twierdzi amerykański wywiad. Czy to oznacza, że Teheran staje się „cyberpotęgą”?

„Iran postrzega cyberoperacje jako bezpieczną, a zarazem tanią metodę prowadzenia działań odwetowych oraz gromadzenia informacji wywiadowczych” – czytamy w raporcie „Iran Military Power. Ensuring Regime Survival and Securing Regional Dominance” opracowanym przez Defense Intelligence Agency. W jego treści eksperci wskazują, że Teheran bardzo często „maskuje” swoje operacje, aby zminimalizować ryzyko wykrycia. Niemniej jednak pomimo dużych starań związanych z zacieraniem śladów cyberataków, zagraniczne służby często wpadają na ich trop i jednoznacznie są w stanie stwierdzić, że to Teheran jest za nie odpowiedzialny. „Iran ma aspiracje do dominacji w cyberprzestrzeni” – stwierdzono w dokumencie.

W tym miejscu należy jednak podkreślić, że w porównaniu z bardziej zaawansowanymi technologicznie państwami, takimi jak Stany Zjednoczone, Chiny czy Rosja, ofensywne zdolności Teheranu są nadal słabo rozwinięte. Głównym wydarzeniem, które skłoniło irański rząd do zwiększenia nacisku na działania prowadzone w cyberprzestrzeni był incydent z wykorzystaniem wirusa Stuxnet z 2010 roku, kiedy to elementy krajowej infrastruktury nuklearnej zostały zniszczone za pomocą złośliwego oprogramowania.

Co równie ważne, Iran regularnie otrzymuje pomoc techniczną od kluczowych aktorów, których wirtualne zdolności znajdują się na najwyższym poziomie innowacyjności. „Teheran otrzymuje pomoc techniczną w zakresie obrony cyberprzestrzeni ze strony Rosji i Chin” – czytamy w raporcie. „Sam rząd regularnie zwiększa nakłady finansowe przeznaczone na budowę swoich cyberzdolności”. Eksperci podkreślają, że Iran jest państwem, które szybko przeszło ewolucję, od podstawowego wykorzystywania globalnej sieci dla potrzeb społecznych do prowadzenia wyrafinowanych cyberataków oraz cyberszpiegostwa.

Zgodnie z treścią dokumentu irańscy hakerzy specjalizują się w kampaniach phisingowych wymierzonych głównie przeciwko prywatnym firmom, a także w cyberszpiegostwie. Ich ofiarami najczęściej są przedsiębiorstwa z branży lotniczej, energetycznej, petrochemicznej, telekomunikacyjnej oraz kontrahenci wojska. Według statystyk zaprezentowanych w raporcie „co najmniej od 2014 roku irańscy hakerzy regularnie wykradają dane uwierzytelniające i rozprzestrzeniają złośliwe oprogramowanie w sieciach biznesowych. Te cyberszpiegowskie działania mogą wspierać irańskie wojskowe badania oraz rozwój, a także przemysł i handel”.

Autorzy dokumentu wskazują, że Iran już wielokrotnie pokazał, że jest zdolny do przeprowadzenia destrukcyjnych cyberataków wymierzonych w największych wrogów, w tym Stany Zjednoczone. Przykładem może być reakcja na incydent z 2012 roku, kiedy to systemy irańskiego zakładu

petrochemicznego zostały zainfekowane złośliwym oprogramowaniem. Wówczas Teheran odpowiedział przeprowadzeniem cyberataku na Saudi Aramco i Qatari RasGas, wyrządzając ogromne straty materialne.

W tym miejscu warto również zaznaczyć, że irańscy hakerzy prowadzą także szeroko zakrojone operacje informacyjne wspierające konkretną retorykę polityczną. „Państwowi hakerzy prowadzą działania mające na celu promowanie rosyjskich interesów za pomocą sieci fałszywych kont w mediach społecznościowych" – mówi treść raportu. Autorzy dokumentu podkreślają, że konta te z reguły promują postawy antyzachodnie oraz wspierają politykę, którą Teheran uważa za korzystną.

Potwierdzeniem wniosków płynących z analizy ekspertów mogą być najnowsze wydarzenia, w których irańscy hakerzy brali czynny udział. Jak informowaliśmy w tym tygodniu, grupa cyberprzestępców, działających na zlecenie Teheranu, wykorzystała botnety do infekowania systemów i sieci szpitali oraz uniwersytetów, znajdujących się na Bliskim Wschodzie, w Stanach Zjednoczonych oraz Azji. Celem złośliwej kampanii były również instytucje, mające kluczowe znaczenie dla bezpieczeństwa USA.

Czytaj też: Irańscy hakerzy nie śpią. Wojskowe szpitale nowym celem