

TAJEMNICE POLITYKI BEZPIECZEŃSTWA USA W RĘKACH IRANU? POUFNE DANE PRZEZ LATA TRAFIAŁY DO TEHERANU

Amerykańskim służbom udało się zidentyfikować irańskich hakerów, którzy na zlecenie rządu w Teheranie od wielu lat wykradali poufne dane na temat polityki bezpieczeństwa Stanów Zjednoczonych oraz innych krajów w Europie i na Bliskim Wschodzie. Poza realizacją zadań zleczanych przez państwo, cyberprzestępcy handlowali pozyskanymi danymi na „czarnym rynku” w celu czerpania korzyści finansowych. Irańczycy zostali oskarżeni o liczne przestępstwa i są ścigani przez amerykańskie służby.

Zgodnie z aktem oskarżenia 30-letni Hooman Heidarian i 34-letni Mehdi Farhadi, obaj pochodzący z Iranu, dopuścili się kradzieży setek terabajtów danych z urzędzeń i systemów znajdujących się w Stanach Zjednoczonych, Europie oraz na Bliskim Wschodzie. Mężczyźni prowadzili operacje na zlecenie rządu w Teheranie – czytamy w komunikacie Departamentu Sprawiedliwości USA, wydanym 16 września br.

Skradzione przez hakerów dane dotyczyły „bezpieczeństwa narodowego, wywiadu, informacji na temat polityki nuklearnej wielu państw, danych lotniczych, informacji o inicjatywach na rzecz praw człowieka, danych finansowych ofiar i danych osobowych, a także własności intelektualnej, w tym nieopublikowanych badań naukowych”.

Część działań podejmowanych przez Irańczyków było motywowanych politycznie lub realizowanych bezpośrednio na zlecenie rządu. Wiele skradzionych danych hakerzy sprzedawali również na czarnym rynku dla własnego zysku.

„Nie wprowadzimy praworządności do cyberprzestrzeni, dopóki rządy nadal będą wspierać hakerów w swoich granicach” – podkreślił zastępca prokuratora generalnego John C. Demers. Jak dodał, ostatnie wydarzenia wskazują, że co najmniej cztery państwa – Iran, Chiny, Rosja, Korea Północna – popierają działalność hakerską wymierzoną w podmioty z całego świata, zwłaszcza gdy jest ona zgodna z polityką rządu. „Dzisiejsi oskarżeni zobaczą, że tego typu służba na rzecz Teheranu nie jest żadnym atutem, lecz zbrodniczym jarmem” – stwierdził przedstawiciel prokuratury.

Craig Carpenito, prokurator Stanów Zjednoczonych z okręgu New Jersey, podkreślił, że Irańczycy „bezcelnie” infiltrowali systemy i naruszyli własność intelektualną państw uznawanych przez Teheran za przeciwników. „Takie postępowanie zagraża naszemu bezpieczeństwu narodowemu, dlatego też mężczyźni zostali postawieni w stan oskarżenia i są poszukiwani przez FBI” – zaznaczył Craig Carpenito.

Z kolei agent specjalny FBI George M. Crouch zadeklarował, że służby nieustannie współpracują z partnerami, aby skutecznie zidentyfikować cyberprzestępców, których celem jest „wyrządzenie

krzywdy” amerykańskiemu społeczeństwu, niezależnie od tego, gdzie mogą przebywać. „Mehdi Farhadi i Hooman Heidarian zostali uznani za zbiegów i dodani na listę groźnych przestępców” – wskazał przedstawiciel FBI.

Zgodnie z aktem oskarżenia od co najmniej 2013 roku mężczyźni prowadzili skoordynowaną kampanię włamań do systemów komputerowych w Stanach Zjednoczonych oraz w innych częściach świata. „Wśród ofiar znalazło się między innymi kilka amerykańskich i zagranicznych uniwersytetów na czele z ośrodkiem analitycznym w Waszyngtonie, wykonawcy sektora obronnego, firmy lotnicze, podmioty odpowiedzialne za politykę zagraniczną czy rządy narodowe państw uznawanych przez Iran za wrogie” – czytamy w komunikacie Departamentu Sprawiedliwości USA.

Poza kradzieżą wysoce chronionych danych, hakerzy naruszyli również wiele stron internetowych, zamieszczając na nich wiadomość, wskazującą na upadek rywali Teheranu, w tym Izraela i Arabii Saudyjskiej, oraz irańskiej opozycji na krajowej scenie politycznej.

W celu wybrania konkretnych ofiar mężczyźni przeprowadzili szczegółowy rekonesans, gromadząc między innymi dane publicznie dostępne oraz informacje wywiadowcze. To pozwoliło im na poznanie obszaru specjalizacji określonej osoby bądź podmiotu i następnie, wykorzystując narzędzia hakerskie, ocenienie podatności danej sieci. „Oskarżeni uzyskali i utrzymywali nieautoryzowany dostęp do sieci ofiar przy użyciu różnych rozwiązań, w tym instalowaniu złośliwego oprogramowania” – wskazał Departament Sprawiedliwości USA.

Podczas operacji Irańczycy często korzystali z „trojanów zdalnego dostępu” do monitorowania działań użytkowników. Opracowali także narzędzie botnetowe, które ułatwiło im rozprzestrzenianie złośliwego oprogramowania, a także ataki DDoS czy kampanie spamowe.

Postawienie zarzutów było możliwe na podstawie wyników śledztwa przeprowadzonego przez agentów specjalnych FBI. Każdy z mężczyzn jest oskarżony o spisek mający na celu popełnienie oszustwa; nieautoryzowany dostęp do chronionych komputerów; nieuprawnione uszkodzenie chronionych komputerów; spisek w celu popełnienia oszustwa elektronicznego; kradzież tożsamości.

Czytaj też: [FBI i CISA ostrzegają przed irańskimi hakerami](#)



PRACA ZBIOROWA
SZTUKA WOJNY

FILOZOFIA I PRAKTYKA
ODDZIAŁYWANIA NA BIEG ZDARZEŃ

Wojna to konfrontacja dwóch ludzkich woli

Nowy przekład traktatu Sun Zi

- **Wśród współautorów wykładów i komentarzy m.in.**
- **prof. Jerzy Bralczyk • gen. Jarosław Kraszewski**
- **prof. Witold M. Orłowski • płk Leszek Elak • NAVAL**
- **płk Andrzej „Wodzu” Kruczyński**

Sklep.Defence **24**

[Z oferty Sklepu Defence24 - zapraszamy!](#)