Cyberdefence 24

aut. Szymon Palczewski 22.09.2020

KTO SZPIEGUJE IRAŃSKĄ OPOZYCJĘ?

Hakerzy działający z Iranu odpowiadają za kampanię cyberszpiegowską wymierzoną między innymi w przeciwników rządu w Teheranie. Operacja trwała od co najmniej sześciu lat. Jako „wabik" dla potencjalnych ofiar wykorzystywała budzące emocje tematy polityczne oraz wydarzenia w regionie. Kto jest odpowiedzialny za realizację działań hakerskich?

Hakerzy odpowiadają za kampanię szpiegowską wymierzoną w emigrantów, polityków oraz przeciwników rządu w Teheranie, która trwała od lat. Analiza przeprowadzona przez specjalistów Check Point wykazała, że seria cyberataków na różnorodne cele w Iranie oraz w innych „nieprzychylnych" z punktu widzenia reżimu państwach była przeprowadzona przez tego samego aktora.

Specjaliści podkreślają, że w ramach kampanii hakerzy wykorzystują backdoory w Androidzie do pozyskiwania kodu dwuskładnikowego uwierzytelniania z wiadomości SMS, rejestrowania dźwięku otoczenia oraz innych danych z zaatakowanego urządzenia. Cyberprzestępcy wykazywali również zainteresowanie kradzieżą informacji z systemu Windows, w tym dokumentów i plików osobistych ofiar. Ponadto używają stron phishingowych, do których linki wysyłane są za pomocą fikcyjnych kont na Telegramie.

Jak wskazują specjaliści Check Point, kampania jest wymierzona głównie przeciwko mniejszości irańskiej za granicą, organizacjom opozycyjnym oraz ruchom oporu, takim jak: Association of Families of Camp Ashraf and Liberty Residents (AFALR), Azerbaijan National Resistance Organization czy społeczności Beludżystanu.

Jednym z pierwszych zainfekowanych plików, jaki specjaliści napotkali w sieci, tytułem nawiązywał do walki między Teheranem a ruchem Mudżahedin-e Khalq. Wykorzystując tematykę polityczną budzącą emocje, hakerzy chcieli przykuć uwagę potencjalnych ofiar. Wspomniany materiał to plik dokumentu Word o nazwie „The Regime Fears the Spread of the Revolutionary Cannons.docx". Po jego otwarciu przez ofiarę hakerzy uzyskiwali możliwość pobrania na jej urządzenie złośliwe oprogramowanie.

W ten sposób cyberprzestępcy mogli swobodnie przesyłać pliki z Telegrama użytkowników, a także w pełni wykorzystywać ich konto w ramach platformy do dalszych działań. Co więcej, hakerzy posiadając dostęp do urządzenia ofiary wykradali informacje z aplikacji KeePass (menager haseł) oraz dane ze schowka komputera. Zainstalowanie złośliwego oprogramowania pozwalało również cyberprzestępcom na dokonywanie zrzutów z ekranów i przesyłanie na zewnętrzne serwery wszystkich znalezionych plików.

W ramach kampanii hakerzy implementowali mechanizm trwałej obecności oparty na aktualizacji Telegrama. „Śledząc ruch tego ataku, ujawniliśmy operację na dużą skalę" – czytamy w oficjalnym komunikacie Check Point. Zdaniem specjalistów cyberataki trwały od co najmniej sześciu lat.

Analiza wykazała, że operacje prowadzone są z obszaru Iranu, a hakerzy wykorzystują wiele wektorów do działań szpiegowskich, a także infekowania komputerów i urządzeń mobilnych w celu przejęcia m.in. prywatnej komunikacji prowadzonej przez Telegrama oraz inne media społecznościowe.

Co warte podkreślenia, większość zidentyfikowanych przez ekspertów ofiar pochodzi z Iranu. To sugeruje, że za kampanię najprawdopodobniej odpowiadają podmioty, które są zainteresowane gromadzeniem informacji na temat przeciwników obecnego rządu w Teheranie.

Hakerzy działający na zlecenie Iranu są znani z prowadzenia szeroko zakrojonych operacji kradzieży danych. Jak informowaliśmy na naszym portalu 17 września, amerykańskim służbom udało się zidentyfikować irańskich cyberprzestępców – 30-letniego Hoomana Heidariana i 34-letniego Mehdiego Farhadi – którzy na zlecenie rządu w Teheranie od wielu lat wykradali poufne informacje na temat polityki bezpieczeństwa Stanów Zjednoczonych oraz innych krajów w Europie i na Bliskim Wschodzie. Poza realizacją zadań zlecanych przez państwo, hakerzy handlowali pozyskanymi danymi na „czarnym rynku" w celu czerpania korzyści finansowych.

Skradzione przez Irańczyków dane dotyczyły przede wszystkim „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" – stwierdził Departament Sprawiedliwości USA w komunikacie przedstawiającym zarzuty pod adresem hakerów.

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

Czytaj też: Tajemnice polityki bezpieczeństwa USA w rękach Iranu? Poufne dane przez lata trafiały do Teheranu