Irańczycy cyberatakują

1 czerwca 2014

Firma iSight Partners poinformowała o odkryciu zaawansowanej operacji cyberszpiegowskiej prowadzonej od trzech lat przez irańskich hakerów. Napastnicy stworzyli fałszywe konta w serwisach społecznościowych oraz fałszywe witryny informacyjne, dzięki którym szpiegowali woskowych i polityków m.in. z USA i Izraela.

Wiadomo, że wśród ich ofiar znajdują się m.in. czterogwiazdkowy amerykański admirał, ambasadorowie i przedstawiciele władzy wykonawczej USA oraz amerykański personel pracujący w Afganistanie, Wielkiej Brytanii, Izraelu, Syrii i Arabii Saudyjskiej.

iSight odmówiła podania nazwisk osób, które Irańczycy wzięli na celownik. Firma nie jest też w stanie stwierdzić, czy i jakie informacje zostały ukradzione. Wiadomo, że hakerzy próbowali zdobyć dane potrzebne do logowania się w sieciach rządowych i korporacyjnych, poszukiwali też danych wywiadowczych na temat broni oraz negocjacji dyplomatycznych. „Skoro prowadzili te działania tak długo, to można przypuszczać, że odnosili jakieś sukcesy” – stwierdziła Tiffany Jones z iSight.

Napastnicy założyli fałszywe konta 14 osób, działali na Facebooku, LinkedIn, Google+ oraz Twitterze. Tam nawiązywali kontakt z interesującymi ich osobami, zapraszali na swoje profile. Początkowo wysyłali odnośniki do wiarygodnych źródeł informacji, z czasem odnośniki te infekowali czy przekierowywali ofiary na fałszywe portale, gdzie pojawiała się prośba o zalogowanie. „To powolny, cichy atak. Chcą pozostać poza podejrzeniami, w ukryciu” – mówi Jones.

iSight poinformowała o ataku zarówno ofiary, serwisy społecznościowe, FBI oraz władze odpowiednich krajów.

Przedstawiciele firmy poinformowali, że irańscy hakerzy zwiększyli swoją aktywność od 2010 roku. Wtedy to irańskie instalacje atomowe zostały zaatakowane przez robaka Stuxnet, który został najprawdopodobniej stworzony przez USA i Izrael. iSight nie posiada dowodów, by wspomniana powyżej operacja hakerska była prowadzona przez rząd w Teheranie, jednak biorąc pod uwagę stopień jej skomplikowania można przypuszczać, że hakerzy mieli co najmniej rządowe wsparcie.

Przed dwoma laty informowaliśmy o założeniu przez cyberszpiegów fałszywego profilu szefa Naczelnego Dowództwa Połączonych Sił Zbrojnych w Europie admirała Stavridisa.

Autor: Mariusz Błoński
Na podstawie: IT News
Źródło: Kopalnia Wiedzy