**Irańscy hakerzy zaatakowali izraelskich i amerykańskich urzędników!**

**Irańscy cyberprzestępcy przeprowadzili ka mpanię spear-phishingową wymierzoną w izraelskich i amerykańskich urzędników oraz kadrę kierowniczą. Hakerzy byli w stanie przechwycić korespondencję e-mail, a następnie wykorzystali ją do namierzenia urzędników wysokiego szczebla w celu kradzieży danych osobowych – informują badający sprawę analitycy bezpieczeństwa z Check Point Research.**

Stosunki między Izraelem a Iranem z pewnością będą w najbliższym czasie jeszcze bardziej napięte. Powodem są kolejne ataki cybernetyczne prowadzone przez stronę irańską, a których ofiarami mogli być urzędnicy, wojskowi oraz menedżerowie z Izraela i USA. Check Point Research (CPR) ujawnił niedawno operację spear-phishingową, w ramach której hakerzy przejęli istniejące konta kadry kierowniczej oraz stworzyli kolejne - fałszywe, aby zachęcić swoje cele do wymiany e-maili, a następnie przejęcia ich danych logowania, skanów dokumentów i innych danych wrażliwych!

Wśród celów irańskich hakerów byli m.in.:

l Tzipi Livni – była minister spraw zagranicznych i wicepremier Izraela

l Były generał dywizji, który służył na bardzo wrażliwym stanowisku w IDF

l Przewodniczący jednego z wiodących izraelskich think-tanków zajmujących się bezpieczeństwem

l Były ambasador USA w Izraelu

l Były przewodniczący znanego centrum badawczego Bliskiego Wschodu

l Starszy dyrektor w izraelskim przemyśle obronnym

**Zdaniem ekspertów Check Point Research celem operacji była kradzież danych osobowych, skanów paszportów oraz dostęp do kont e-mail.** Początek operacji sięgał grudnia 2021 r., choć nie można wykluczyć, że całość planowana była jeszcze wcześniej.

Metodologia ataku polegała na uzyskaniu dostępu do rzeczywistych kont e-mailowych, a następnie przejęciu wiadomości i korespondencji z urzędnikami. Hakerzy następnie tworzyli podobne konta i mail oraz kontynuowali rozmowy z niczego nieświadomymi ofiarami. W kolejnych wiadomościach udostępniali łącza do dokumentów i formularzy (np. w formie zaproszenia na konferencję lub badania) z miejscem na wgranie skanów dokumentów.

**Hakerzy podszyli się pod wysokiej rangi generała**

Tzipi Livni, była minister spraw zagranicznych Izraela, otrzymała e-maila, w którym ktoś podszywał się pod dobrze znanego byłego generała dywizji IDF. Wiadomość zawierała łącze do pliku, o którego otwarcie i przeczytanie poprosił ją atakujący (sama wiadomość pochodziła z adresu, z którym już w przeszłości korespondowała). Ponieważ zwlekała, „fałszywy generał” kilkakrotnie zachęcał ją do otwarcia pliku przy użyciu jej hasła do poczty e-mail. Wzbudziło to jej podejrzenia, więc przy najbliższej okazji skontaktowała się osobiście ze wspomnianym generałem, pytając go o wiadomość. Ten zaprzeczył, by wysyłał jakiekolwiek e-maile z prośbą o logowanie. W ten sposób ujawniono pierwszą próbę wyłudzenia i przekazano sprawę służbom, które wspierał w analizach CPR.