Cyberdefence 24

aut. Sylwia Gliwa 14.10.2019

IRAŃSCY HAKERZY UDERZAJĄ W AMERYKAŃSKICH WETERANÓW. CZY SFORSUJĄ SYSTEMY PENTAGONU?

Irańscy hakerzy wykorzystują fałszywą stronę do atakowania amerykańskich wojskowych - ostrzegają eksperci. Witryna o nazwie „Hire Military Heroes" zawierająca oferty pracy skierowane do weteranów chcących powrócić do aktywnego życia cywilnego zachęcała do pobrania aplikacji infekującej używany sprzęt.

Gwardia Narodowa Stanów Zjednoczonych (National Guard) wydała w tej sprawie oświadczenie ostrzegając weteranów przed stroną i pobieraniem aplikacji, która po pobraniu infekuje sprzęt złośliwym oprogramowaniem – poinformował portal military.com.

Urzędnicy z Departamentu Obrony ustalili, że działania ukierunkowane są na osoby, które już niebawem opuszczą struktury wojskowe i będą zainteresowane poszukaniem pracy w sektorze cywilnym. W ich opinii, działania mają na celu pozyskanie dostępu do systemów informatycznych Pentagonu. Hakerzy mają nadzieję, że choć jeden z weteranów pobierze i uruchomi złośliwe oprogramowanie – wskazali w notatce. Stwierdzili również, że szanse na pozyskanie dostępu do systemów departamentu przez irańską grupę zidentyfikowaną jako Tortoiseshel jest nikła, nadali jednak tej sprawie wysoką rangę.

Jako pierwsze o sprawie poinformowało Cisco Talos Intelligence Group, które już dwa tygodnie temu wskazało, że nazwa strony jest bardzo podobna do legalnej witryny prowadzonej na rzecz pomocy amerykańskim weteranom w znalezieniu miejsca na cywilnym rynku pracy. Wcześniej, tego lata, grupa była oskarżana o atak na dostawców usług IT z Arabii Saudyjskiej. Eksperci firmy wskazali, że aplikacja umożliwia hakerom podejrzenie m.in informacji o systemie, nazwie administratora, wersji oprogramowania czy konfiguracji sieci. Informacje są wystarczające, aby przygotować dodatkowy atak na sprzęt.

O działalności hakerów powiązanych z rządem Iranu poinformował w zeszły piątek również Microsoft, który potwierdził, że doszło do próby włamania na 241 kont e-mail, należących również do urzędników rządowych, przedstawicieli mediów, emigrantów arabskich oraz konta, które obsługiwało jedną z prezydenckich kampanii wyborczych. Firma zidentyfikowała hakerów pod nazwą Phosphorous. Przedsiębiorstwo potwierdziło, że do ataków doszło w sierpniu i wrześniu, jednak odmówiło podania o które konta chodzi.