Cyberdefence 24

aut. Andrzej Kozłowski 25.07.2019

LINKEDIN CELEM IRAŃSKICH HAKERÓW. KOLEJNY ELEMENT AMERYKAŃSKO-IRAŃSKIEGO CYBERKONFLIKTU

Amerykańska firma FireEye ostrzega przed kampanią phisingową ukierunkowaną na użytkowników LinkedIna. Autorem mają być hakerzy z grupy APT34 związanej z Iranem. To kolejny element zaostrzającego się konfliktu pomiędzy Iranem a Stanami Zjednoczonymi w cyberprzestrzeni.

Użytkownicy LinkedIna otrzymują zaproszenie do dołączenia do sieci zrzeszających ekspertów z danej branży. Następnie otrzymują dokument, który zawiera złośliwe oprogramowanie umożliwiające kradzież informacji oraz danych osobowych. Celem oczywiście nie są przypadkowe osoby, tylko użytkownicy LinkedIna związani z branżami, które znajdują się w orbicie zainteresowań Teheranu. Według amerykańskiej firmy FireEye grupa APT34 chce przede wszystkim dostać się do osób związanych z branżą energetyczną, finansową oraz do urzędników rządowych. Celem są również naukowcy. To właśnie od jednej z pracownic naukowych Uniwersytetu Cambridge ma pochodzić informacja o tej próbie oszusta. Nie jest to pierwszy raz kiedy grupa APT34 próbuje za pomocą ofert pracy, współpracy akademickiej czy biznesowej dotrzeć do potencjalnych ofiar i zainfekować je złośliwym oprogramowaniem.

W kampanii grupy APT34, firma FireEye zidentyfikowała nowy rodzaj złośliwego oprogramowania, który infekuje systemy w celu zbierania informacji. Eksperci znaleźli również narzędzia do wykradania danych logowania znajdujących się w Windows Vault. Jest to szczególnie istotne przy atakach na najważniejsze cele takie jak infrastruktura krytyczna, systemy rządowe czy największe korporacje. Kradzież danych logowania jest początkiem zaawansowanych operacji.

LinkedIn jest bardzo dobrym polem do operacji hakerskich, ponieważ użytkownicy są o wiele mniej uważni i sceptyczni co do otrzymywanych wiadomości niż w przypadku normalnej skrzynki pocztowej. FireEye określa LinkedIn platformą społecznością, która umożliwia skuteczne dostarczenie złośliwego oprogramowania tym organizacjom, które cechują się bardzo dobrą obroną przed phisingiem za pomocą poczty elektronicznej.

To kolejna odznaka rosnącej aktywności irańskich hakerów, którzy po raz kolejny na swój cel wzięli cywilne obiekty. Wcześniej o wzrastającej liczbie cyberataków informował wiceprezes Microsoftu Tom Burt. Podczas swojego przemówienia w ramach Aspen Security Forum w Kolorado podkreślił, że jego firma zaobserwowała niespotykany dotychczas wzrost aktywności od momentu, w którym Stany Zjednoczone wycofały się z porozumienia nuklearnego. Jak zaznaczył przedstawiciel Microsoft, hakerzy „w dużej mierze" ukierunkowali swoją działalność w organizacje przemysłu petrochemicznego.

Czytaj też: Iran zwiększa liczbę cyberataków przeciwko USA

Wcześniej podobne ostrzeżenie wydał również Departament Bezpieczeństwa Wewnętrznego (DHS). Dyrektor agencji ds. bezpieczeństwa infrastruktury krytycznej i cyberbezpieczeństwa (CISA) w DHS Christopher Krebs, wydał ostrzeżenie, w którym podkreślił wzrost aktywności sponsorowanych przez państwo irańskich podmiotów cyberprzestępczych. Do podobnych wniosków doszli również autorzy raportu opracowanego przez Recorded Future. W jednym z wywiadów Christopher Krebs zaznaczył, że ostrzeżenie zostało wydane, ponieważ działalność hakerów nie ma już charakteru regionalnego.

Według specjalistów Recorded Future aktywność irańskiej grupy hakerów, znanej jako APT33, gwałtownie wzrosła. Cyberprzestępcy stworzyli 1200 domen przeznaczonych do kontrolowania i rozprzestrzeniania złośliwego oprogramowania. Grupa rozpoczęła swoje działania kierując uderzenie w saudyjskie firmy, a także podmioty indyjskie. Głównym celem mają być jednak Stany Zjednoczone. Iran podejrzewany jest też o sabotaż wystrzelenia rakiety przenoszącej wojskowego satelitę Zjednoczonych Emiratów Arabskich.

Czytaj też: Iran strącił satelitę ZEA cyberatakiem?

Źródło: Forbes/FireEye