Cyberdefence 24

aut. Szymon Palczewski 22.04.2020

TROJAN W E-MAILU OD EGIPSKIEGO GIGANTA NAFTOWEGO. HAKERZY UDERZYLI W BRANŻĘ PETROCHEMICZNĄ

Hakerzy podszywali się pod egipskiego giganta naftowego, aby rozsyłać wiadomości spearphshingowe w celu kradzieży wrażliwych danych. Złośliwe oprogramowanie wykorzystywane przez cyberprzestępców to popularny w czasie pandemii koronawirusa trojan szpiegowskich. Takie samo narzędzie zostało użyte przez hakerów podczas kampanii wymierzonej w Światową Organizację Zdrowia.

Eksperci odkryli kampanię spearphishingową, w ramach której hakerzy podszywali się pod Enppi, firmę naftową należącą do egipskiego rządu. Do ataków wykorzystano złośliwe oprogramowanie o nazwie Agent Tesla.

Używany w kampanii trojan szpiegowski umożliwia cyberprzestępcom kradzież loginów oraz haseł, wpisywanych przez użytkowników do różnych witryn, za pomocą rejestracji ruchów na klawiaturze. Eksperci wskazują, że złośliwe oprogramowanie było już wcześniej wykorzystywane przez hakerów podczas cyberataków na branżę przemysłu energetycznego między innymi w Malezji, Stanach Zjednoczonych, Iranie, Afryce Południowej, Omanie czy Turcji.

W ramach kampanii cyberprzestępcy podszywają się pod egipską państwową firmę naftową Engineering for Petroleum and Process Industries (Enppi). W treści wiadomości zapraszają odbiorcę do złożenia oferty na sprzęt i materiały w ramach projektu „Rosetta Sharing Facilities Project”.

Jak czytamy na oficjalnej stronie egipskiego koncernu, firma posiada ogromne uznanie na światowym rynku i w wielu dziedzinach jest uznawana za lidera. Dodatkowo, Enppi posiada wieloletnie doświadczenie w realizacji projektów lądowych i morskich w branży petrochemicznej.

Spreparowany e-mail wydaje się być wiarygodny dla potencjalnego odbiorcy. Posiada wszelkie niezbędne informacje, takie jak na przykład termin składania oferty czy wadium. Jednak w załączonych do wiadomości plikach znajduje się złośliwe oprogramowanie, które jest instalowane na urządzeniu po kliknięciu w odnośnik.

Według rumuńskich ekspertów wirus Agent Tesla istnieje od co najmniej 2014 roku, choć jego popularność znacznie wzrosła w ostatnim czasie w związku z kampaniami wykorzystującymi pandemię koronawirusa.

Jako przykład można podać operację, w ramach której hakerzy podszywali się pod Światową Organizację Zdrowia. Specjaliści IBM X-Force IRIS przeanalizowali e-maile phishingowe dotyczące COVID-19, wskazując, że w ich treści zawarto trojana Agent Tesla – czytamy w oficjalnym komunikacie IBM X-Force Exchange.

Obecnie specjaliści nie wskazują na konkretne źródło złośliwej kampanii podszywającej się pod egipski koncern. Część ekspertów uważa, że ze względu na charakter użytego wirusa, identyfikacja sprawcy będzie bardzo trudna – donosi serwis CyberScoop.