Cyberdefence 24

aut. Szymon Palczewski 26.08.2020

PRZEZ LINKEDIN… DO KONTA OFIARY. HAKERZY KOREI PÓŁNOCNEJ SZUKAJĄ ŹRÓDEŁ FINANSOWANIA

Północnokoreańscy hakerzy wykorzystali platformę LinkedIn do przeprowadzenia kampanii phishingowej, której celem byli przedstawiciele uznanych firm z całego świata. W ramach operacji cyberprzestępcy rozsyłali spreparowane oferty pracy wraz z załącznikiem zawierającym złośliwe oprogramowanie.

Hakerzy grupy Lazarus odpowiadają za najnowszą kampanię wymierzoną w 14 firm z całego świata, w tym z Wielkiej Brytanii oraz Stanów Zjednoczonych. Ostatnią ofiarą złośliwych działań jest przedsiębiorstwo zajmujące się kryptowalutami – donosi serwis ZDNet.

Analiza przeprowadzona przez specjalistów F-Secure ujawniła, że w ramach kampanii hakerzy północnokoreańskiej grupy wykorzystywali platformę LinkedIn do rozsyłania wiadomości phishingowych. Zawarty w nich zainfekowany plik imitował rzeczywistą ofertę pracy w firmie zajmującej się technologią blockchain. Dokument był skierowany do starannie wybranych osób, których kompetencje odpowiadały wymaganiom opisanym w ofercie stanowiska – czytamy w raporcie F-Secure.

Kliknięcie w załącznik powodowało, że na urządzeniu ofiary instalowane było złośliwe oprogramowanie. Umożliwiało ono hakerom zdalne wykonywanie poleceń, takich jak pobieranie informacji czy uruchamianie dodatkowych programów lub plików. Główną motywacją Lazarus stanowiło zbieranie danych uwierzytelniających z zainfekowanego urządzenia, które zabezpieczały dostęp do środków finansowych (kont bankowych czy kryptowalutowych) – informuje ZDNet.

Zdaniem specjalistów, pomimo wykrycia kampanii hakerzy Pjongjangu nadal będą rozsyłać fikcyjne propozycje pracy do firm powiązanych z rynkiem finansowym, w tym kryptowalut, aby w ten sposób generować zyski. Co więcej, eksperci wskazują, że grupa może nawet rozszerzyć swoją działalność na sektor łańcucha dostaw, aby utrwalić prowadzone operacje.

„Grupa Lazarus nadal używa niektórych narzędzi (…), które zaobserwowano w 2016 roku, jednak analiza kilku próbek sugeruje, że są one aktualizowane z biegiem czasu” – stwierdzono w raporcie. Hakerzy zainwestowali w rozwój złośliwego oprogramowania oraz operacyjne zabezpieczenia w celu minimalizacji wykrycia swojej obecności w sieciach.

Czytaj też: Spektakularny rozwój cyberwojsk Korei Północnej. Hakerzy rozmieszczeni poza granicami kraju