Cyberdefence 24

aut. Szymon Palczewski 13.08.2020

PÓŁNOCNOKOREAŃSKA OPERACJA W IZRAELU. HAKERZY UDERZYLI W PRZEMYSŁ OBRONNY

Przemysł obronny Izraela był celem północnokoreańskich hakerów, którzy realizowali zadania w ramach kampanii cyberszpiegowskiej. Podczas operacji podszywali się pod pracodawców popularnych firm, aby nakłonić użytkowników do dalszej interakcji, oferując atrakcyjne propozycje zatrudnienia. Izraelskim specjalistom skutecznie udało się zneutralizować złośliwą kampanię.

Izraelski Directorate of Security for the Defense Establishment we współpracy z instytucjami ds. bezpieczeństwa „udaremnił cyberatak", wymierzony w krajowe podmioty przemysłu obronnego – czytamy w oświadczeniu wydanym przez Ministerstwo Obrony Izraela. Złośliwa kampania została przeprowadzona przez grupę północnokoreańskich hakerów „Lazarus".

W wyniku dochodzenia odkryto, że członkowie grupy stosowali różne techniki hakerskie, w tym socjotechnikę, aby zrealizować swoje cele. W ramach operacji stworzyli fałszywe profile w serwisie społecznościowym Linkedin.

„Osoby atakujące podszywały się pod menedżerów, dyrektorów generalnych i czołowych urzędników działów HR, a także przedstawicieli międzynarodowych firm, a także kontaktowali się z pracownikami wiodących podmiotów przemysłu obronnego w Izraelu w celu nawiązania kontaktu i skuszenia ich różnymi ofertami pracy" – czytamy w oświadczeniu. Następnie hakerzy próbowali włamać się na komputery ofiar, aby w ten sposób infiltrować ich sieci i zebrać poufne dane.

Według Ministerstwa Obrony Izraela cyberataki zostały zidentyfikowane w czasie rzeczywistym i skutecznie odparte przez specjalistów Tech Unit (zespołu funkcjonującego przy Directorate of Security for the Defense Establishment), a także specjalne jednostki pracujące w ramach konkretnych przedsiębiorstw. „Żadne sieci nie zostały ani uszkodzone ani zakłócone" – wskazuje izraelski resort obrony.

Podobną kampanię hakerzy grupy Lazarus prowadzili w Stanach Zjednoczonych. Jak informowaliśmy wcześniej, ich działania były wymierzone w amerykański sektor obronny, lotniczy, a także inne istotne z punktu widzenia państwa branże.

W ramach kampanii mającej miejsce w 2020 roku, eksperci McAfee Advanced Threat Research (ATR) zidentyfikowali serię zainfekowanych plików i innych dokumentów, zawierających ogłoszenia o pracę, które rzekomo miały pochodzić od czołowych podmiotów wspominanych wyżej sektorów. Atrakcyjne dla nieświadomych pracowników pliki służyły jako „wabiki". Były one rozsyłane w wiadomościach spearphishingowych. W ten sposób hakerzy infekowali urządzenia ofiar złośliwym oprogramowaniem przeznaczonym do zbierania danych.

Czytaj też: „Poszukujemy pracownika". Amerykański sektor obronny ofiarą hakerów Korei Północnej