aut. Sylwia Gliwa 16.09.2020

FBI I CISA OSTRZEGAJĄ PRZED IRAŃSKIMI HAKERAMI

Irańska grupa hakerska wykorzystuje luki w zabezpieczeniach VPN do przeprowadzania ataków – informuje amerykańska Agencja ds. Cyberbezpieczeństwa i Infrastruktury (CISA) oraz FBI. Cyberprzestępcy atakują agencje federalne, ale również podmioty z szerokiego wachlarza branż w Stanach Zjednoczonych.

CISA i FBI informują o wykrytej zakrojonej kampanii hakerskiej prowadzonej przez irańską grupę, skierowanej przeciwko branżom: technologicznej, rządowej, opieki zdrowotnej, finansów, ubezpieczeń i mediów w całych Stanach Zjednoczonych.

We wspólnym komunikacie obu instytucji wskazano, że wykorzystywane taktyki, techniki i procedur wskazują na korelacje z działalnością grupy Pioneer Kitten i UNC757. Co więcej podmiot ten wykorzystuje do ataków narzędzia open source.

Przeprowadzona analiza pozwoliła ustalić schemat działania cyberprzestępców - po uzyskaniu wstępnego dostępu do docelowej sieci, podmiot ten dąży do przejęcia poświadczenia na poziomie administratora. Jak się wydaje celem działań jest transfer danych zaatakowanego podmiotu.

Jak stale informujemy na naszych łamach, irańscy hakerzy stale prowadzą działanie w obszarze cyberprzestrzeni próbując ingerować w amerykańskie podmioty rządowe jak i biznesowe. Wczoraj wniesiony został akt oskarżenia, na podstawie którego amerykański wymiar sprawiedliwości chce pociągnąć do odpowiedzialności dwóch hakerów (Irańczyka i Palestyńczyka) za przeprowadzenie cyberataków wymierzonych w amerykańskie strony internetowe w ramach odwetu za zabójstwo Qasema Soleimaniego. Mężczyźni są oskarżeni o spisek w celu „umyślnego uszkodzenia chronionego komputera”.