ZŁOŚLIWE OPROGRAMOWANIE, KTÓRYM ATAKOWANO UKRAINĘ POWRACA

Złośliwe oprogramowanie BlackEnergy , którym atakowano ukraińskie elektrownie w 2015 roku znowu jest w użyciu - ostrzegają specjaliści z branży cyberbezpieczeństwa. W 2015 r. ataki z użyciem tego oprogramowania spowodowały znaczne przerwy w dostawach prądu.

Jak przypomina w czwartek serwis Infosecurity Magazine, kampania ataków na elektrownie zlokalizowane na Ukrainie była sponsorowana przez obce państwo i miała doprowadzić do ich paraliżu. Według ekspertów firmy Venafi, obecnie wirus komputerowy obserwowany podczas tamtych działań powrócił i jest aktywnie wykorzystywany przez cyberprzestępców.

Złośliwe oprogramowanie, o którym mowa, służy do ataków na klucze SSH, które służą do zabezpieczania zdalnej komunikacji i połączeń pomiędzy urządzeniami, a także stanowią podstawę dla działania usług takich jak wirtualne sieci prywatne VPN, czy sieci urządzeń tzw. Internetu Rzeczy (IoT).

Naruszenie bezpieczeństwa klucza SSH może pozwalać hakerom na uzyskanie w niewykrywalny sposób dostępu do krytycznych dla działania placówek energetycznych systemów i ich procesów.

Technika ataku polegająca na łamaniu zabezpieczeń kluczy SSH była wykorzystywana m.in. przez operatorów botnetu TrickBot, a także przez cyberprzestępców działających w ramach zorganizowanej kampanii nielegalnego pozyskiwania kryptowalut CryptoSink.

"Klucze SSH mogą stanowić w niewłaściwych rękach potężną broń. Do niedawna jednak jedynie najbardziej wyrafinowane, dysponujące dobrym finansowaniem grupy hakerskie mogły prowadzić tego rodzaju działania skutecznie" - podkreślają eksperci Venafi.