

ELEKTROWNIE PRZY ZAPORACH WODNYCH GŁÓWNYM CELEM HAKERÓW

Elektrownie znajdujące się w pobliżu zapór wodnych to główny cel ataków ze strony hakerów działających na zlecenie adwersarzy USA - podał dziennik "Wall Street Journal". W sprawie ataków, których natężenie wzrosło latem tego roku, śledztwo prowadzi obecnie FBI.

Zdaniem specjalistów z branży cyberbezpieczeństwa, hakerzy mogą być nadal aktywni - co oznacza, że zorganizowana kampania cyberataków wcale nie musiała dobiec końca.

FBI odmawia komentowania sprawy, jednakże przedstawiciele podmiotów, które były ofiarami ataków hakerskich, poinformowali, że Federalne Biuro Śledcze pomogło im m.in. w przeskanowaniu komputerów i sieci w poszukiwaniu luk w zaporach przeciwwirusowych, a także e-maili mogących zawierać złośliwe oprogramowanie w załącznikach.

Zaatakowane przez cyberprzestępców elektrownie zlokalizowane są w 18 stanach, w tym w Maine, Waszyngtonie i Michigan. Jedną z placówek, które za cel obrali hakerzy, jest siłownia Cloverland Electric Cooperative zlokalizowana tuż obok śluz Sault Ste. Marie Locks, mających krytyczne znaczenie w transporcie rudy żelaza. Inna zaatakowana elektrownia zlokalizowana w stanie Waszyngton znajduje się niedaleko federalnych struktur zaporowych i linii przesyłowych zapewniających energię elektryczną Kalifornii.

Schemat działania cyberprzestępców opierał się na próbach instalacji złośliwego oprogramowania w sieciach elektrowni poprzez wysyłanie e-maili do pracowników obsługujących je spółek. Korespondencja zawierała zawirusowane załączniki instalujące oprogramowanie znane jako "Lookback", które pozwalało atakującemu na całkowite przejęcie kontroli nad atakowanymi komputerami, a tym samym - wykradzenie dowolnych informacji.

Według nowojorskiej gazety identyfikacja zaatakowanych podmiotów była możliwa dzięki znalezionym przez badaczy cyberbezpieczeństwa informacjom, które hakerzy nieopatrznie zostawili na serwerze zarejestrowanym w Hongkongu. Jednakże, jak zaznacza dziennik, żadna z 11 zdefiniowanych w wyniku analizy materiałów elektrowni nie przyznała, jakoby była celem ataku hakerskiego. Przedstawiciele placówek poinformowali jednak, że otrzymali od FBI ostrzeżenie o zwiększonym ryzyku takich incydentów.