aut. Szymon Palczewski 17.06.2019

KOLEJNA ROSYJSKA GRUPA HAKERSKA? CELEM AMERYKAŃSKI SEKTOR ENERGETYCZNY

Hakerzy odpowiedzialni za cyberatak na infrastrukturę petrochemiczną Arabii Saudyjskiej z 2017 roku, ukierunkowali swoje działania na dostawców energii elektrycznej w Azji oraz Stanach Zjednoczonych.

Xenotime to grupa hakerska, która koncentruje swoje wysiłki na zakłóceniu działania elektronicznych systemów sterowania odpowiedzialnych za zarządzanie operacjami w zakładach przemysłowych. Jest jedną z niewielu grup na świecie, która używa specjalnie dostosowane do przemysłowych systemów sterowania złośliwego oprogramowanie – wskazuje Benjamin Read, specjalista FireEye.

Amerykańscy specjaliści od dawna ostrzegają przed cyberatakami wymierzonymi w sektory infrastruktury krytycznej. Zakłócenie dostaw energii elektrycznej może spowodować powszechny chaos wywołany przerwami w dostawach prądu, które z kolei sparaliżują rynki finansowe, transport i wiele innych.

„Większość hakerów na świecie nie chce zabijać ludzi. Jednak wydaje się, że hakerzy z Xenotime mają inne plany" – podkreśla Sergio Caltagirone, wiceprezes firmy Dragos. Specjaliści podkreślają, że cyberprzestępcom nie udało się złamać kluczowych systemów, ale nie można zakładać, iż nie zrezygnują z dalszych wysiłków.

Co więcej, Xenotime jest jedną z niewielu grup hakerskich, która działa w różnych sektorach przemysłu. „Koszt i zasoby potrzebne do przemieszczania się między sektorami są ogromne" – tłumaczy Sergio Caltagirone. To wskazuje, że działalność cyberprzestępców może być silnie wspierana przez państwo. Specjaliści FireEye sugerują, iż grupa może być powiązana z rosyjską instytucją badawczą – Central Scientific Research Institute of Chemistry and Mechanics.

Źródło: Bloomberg