KOLEJNY CYBERATAK NA INFRASTRUKTURĘ KRYTYCZNĄ. SPRAWCY SĄ ZNANI

Jak informuje serwis Motherboard, powołując się na doniesienia FireEye, wykryto nowy atak na infrastrukturę krytyczną. Za incydent mają być odpowiedzialni cyberprzestępcy stojący za opracowaniem złośliwego oprogramowania Triton.

Zespół FireEye ujawnił, iż w ubiegłym tygodniu został zatrudniony do rozwiązania problemów związanych z incydentem bezpieczeństwa w jednostce operacyjnej infrastruktury krytycznej, której nazwy nie ujawniono. Hakerzy odpowiadający za atak to według specjalistów ta sama grupa cyberprzestępcza, która posługuje się złośliwym oprogramowaniem Triton, wykorzystanym uprzednio do ataku na firmę petrochemiczną Petro Rabigh z Arabii Saudyjskiej.

W ataku na saudyjską petrochemię cyberprzestępcy użyli Tritona do przejęcia i zatrzymania systemów kontrolujących procesy przemysłowe. Serwis Motherboard podkreśla, że atak, do którego doszło w 2017 r. jest przez wielu specjalistów z branży cyberbezpieczeństwa uważany za najbardziej niebezpieczny przypadek użycia przez hakerów złośliwego oprogramowania, ze względu na ogromne ryzyko strat i zniszczeń fizycznych, jakie mógł spowodować. Opracowanie i utrzymanie wirusa Triton Firma FireEye przypisuje laboratorium badawczemu powiązanemu z Kremlem - dodaje serwis.

W raporcie podsumowującym podjęte działania firma stwierdziła, iż sprawcy ataku wykorzystali złośliwe oprogramowanie do wtargnięcia i utrzymania dostępu do systemów teleinformatycznych i operacyjnych zaatakowanej firmy. Dostęp do sieci ofiary mieli mieć już jednak od ponad roku - oceniają eksperci. Według nich operacje hakerskie z użyciem Tritona prowadzone są od 2014 roku, zatem liczba zaatakowanych z użyciem tego złośliwego oprogramowania podmiotów prawdopodobniej jest większa niż dwa znane obecnie przypadki - podaje Motherboard.

Specjaliści uważają, że celem hakerów, którzy włamali się do sieci, nie były działania szpiegowskie - nie wykryto bowiem aktywności narzędzi do wykradania danych z komputerów i przejmowania informacji służących do logowania się w systemach. Większość działań prowadzonych przez cyberprzestępców opierała się na użyciu narzędzi do rozpoznawania ruchu sieciowego i utrzymania stałej obecności w zainfekowanym środowisku - oceniają.

Serwis Ars Technica zwraca uwagę, że informacje firmy FireEye nie precyzują, kiedy doszło do ataku, ani jak długo on trwał. Nie podano również, czy atak spowodował dalsze zagrożenie. Rzeczniczka FireEye odmówiła komentarzy w tej sprawie.

SZP/PAP