Triton zaatakował na Bliskim Wschodzie

17 grudnia 2017

Cyberprzestępcy wykorzystali oprogramowanie Triton do ataku na instalacje przemysłowe na Bliskim Wschodzie. Jak donosi należąca do FirstEye firma Mandiant, podczas ataku zmanipulowano systemami służącymi do awaryjnego wyłączania krytycznej infrastruktury. Triton to jedno z kilku znanych narzędzi, które powstało z myślą o zaburzaniu procesów przemysłowych.

Pierwszym głośnym atakiem tego typu były działania robaka Stuxnet użytego przeciwko Iranowi w roku 2010. W 2014 atak przeprowadzono na elektrownię atomową w Korei Południowej, a w 2016 na system zasilania Kijowa.

Triton atakuje specyficzny system kontroli przemysłowej o nazwie SIS (safety instrumental system), produkowany przez Triconex. Celem ataku padają kontrolery, które są zarządzane za pomocą Windows. Przestępcy wstrzykują do urządzeń SIS kod, który pozwala im na kontrolę ich zachowania.

Podczas najnowszego ataku instalacje przemysłowe zostały wyłączone, jednak nie to było celem napastników. Zdaniem ekspertów włamywacze chcieli doprowadzić do fizycznego uszkodzenia infrastruktury przemysłowej, jednak zadziałały zabezpieczenia i instalacje zostały wyłączone. „Śledztwo wykazało, że kontrolery SIS rozpoczęły procedurę wyłączania gdy kod aplikacji kontrolnej nie przeszedł testu sprawdzającego jego autentyczność" – stwierdzili eksperci Mandianta. Uważają oni, że atak został przeprowadzony przez jakieś państwo, na co wskazują umiejętności, wytrwałość napastników, zasoby jakimi dysponowali oraz fakt ataku na krytyczną infrastrukturę. „Ataki mające na celu zakłócenie czy zniszczenie krytycznej infrastruktury są typowe dla ataków i

prób rozpoznania prowadzonych na skalę globalną przez Rosję, Iran, Koreę Północną, USA oraz Izrael i wspierane przez nie grupy. Tego typu włamanie nie muszą oznaczać natychmiastowej chęci doprowadzenia do zniszczeń czy zakłóceń, mogą być powodowane chęcią posiadania tego typu możliwości na przyszłość, gdyby zaszła taka potrzeba.”

Przed dwoma miesiącami FBI i amerykański Departament Bezpieczeństwa Wewnętrznego ostrzegły przed rosnącą liczbą ataku przeciwko przedsiębiorstwom z sektora energetycznego. Na podwyższone ryzyko narażone są też firmy z sektorów atomowego, lotnictwa, zasobów wodnych i lotniczego.

Autorstwo: Mariusz Błoński
Na podstawie: ZDNet.com
Źródło: KopalniaWiedzy.pl