CYBERBROŃ UŻYTA DO ATAKU NA INFRASTRUKTURĘ KRYTYCZNĄ MOGŁA POWSTAĆ W ROSJI

Cyberbroń Triton, która w grudniu 2017 r. posłużyła do ataku na saudyjską petrochemię, mogła powstać w Rosji - stwierdzili eksperci z FireEye. Mało kto posiada zdolności i motywacje do stworzenia podobnego narzędzia - powiedział PAP ekspert dr Łukasz Olejnik.

Ubiegłoroczny atak na Bliskim Wschodzie początkowo budził skojarzenia z aktywnością cyberprzestępców sponsorowanych przez Iran. Podejrzenia te przybrały na sile, gdy ujawniono, że celem hakerów działających z użyciem Tritona była infrastruktura należąca do Arabii Saudyjskiej. Specjaliści z amerykańskiej firmy FireEye ujawnili jednak, że za użyciem cyberbroni może stać inny podmiot. Komponenty narzędzia według nich zostały najprawdopodobniej stworzone w rosyjskim Centralnym Badawczym Instytucie Chemii i Mechaniki zlokalizowanym w Moskwie.

Moskiewska instytucja dotowana jest przez rosyjski rząd. Ma doświadczenie w badaniach z takich dziedzin, jak bezpieczeństwo informacyjne i operacje na systemach kontroli przemysłowej. Współpracuje ona także z innymi rosyjskimi podmiotami badawczymi w zakresie rozwoju nauki, technologii i obronności. Według raportu FireEye rosyjski instytut może być odpowiedzialny za rozwój jednego z komponentów Tritona - nie oznacza to jednak, że nie współpracował z twórcami innych modułów złośliwego oprogramowania.

Triton składa się zarówno z komponentów służących do infekowania celów, jak i narzędzi do manipulacji systemami kontroli infrastruktury przemysłowej. Jego wykorzystanie umożliwia cyberprzestępcom zdalną destabilizację przemysłowych systemów bezpieczeństwa, co może pozwalać nawet na fizyczne zniszczenie obiektu, np. elektrociepłowni czy rafinerii.

Zdaniem niezależnego eksperta ds. cyberwojny i bezpieczeństwa dr. Łukasza Olejnika "specjalistyczne i ofensywne narzędzia zdolne atakować systemy przemysłowe to rzadkość, a przypadek Tritona jest wręcz nadzwyczajny". Jak ocenił Olejnik, w przypadku tego oprogramowania "chodzi o stworzenie i testowanie w warunkach polowych bardzo zaawansowanego narzędzia o charakterze tzw. cyberbroni, będącego niewątpliwie jednym z najgroźniejszych narzędzi tego typu". Ekspert w rozmowie z PAP podkreślił, że "stworzenie go wymagało wiedzy, czasu, środków finansowych i dostępu do specjalistycznego sprzętu" i "nie ma wątpliwości, że mało kto obecnie posiada odpowiednie ku temu zdolności i motywacje".

Badacz podkreślił, że ataki na systemy odpowiedzialne za kontrolę bezpieczeństwa procesów przemysłowych są bardzo groźne. "W tym wypadku nie jest jasne, co było celem atakujących. Powstają jednak wątpliwości, czy w ataku z ubiegłego roku chodziło o kradzież danych" - ocenił ekspert. "Kluczowa funkcja Tritona reprogramująca systemy bezpieczeństwa może zdestabilizować proces przemysłowy. W uproszczeniu jest to wyjęcie bezpieczników, które potencjalnie może prowadzić do zniszczeń fizycznych, takich jak wybuch. W ekstremalnej sytuacji w wyniku takiej katastrofy pojawia się ryzyko utraty życia" - ostrzegł dr Olejnik.