CSE atakuje komputery i podważa reputację radykałów

28 czerwca 2025

Według nowego raportu kanadyjska agencja cyberwywiadu nie tylko atakuje komputery i sieci grup ekstremistycznych, ale także podważa ich reputację i wiarygodność.

W swoim najnowszym rocznym raporcie opublikowanym w piątek, Communications Security Establishment (CSE) przedstawiło nowe szczegóły dotyczące działań podejmowanych w ramach „aktywnej operacji cybernetycznej". W skrócie, raport opisuje sposób, w jaki CSE prowadzi zatwierdzone przez ministra obrony kampanie, których celem jest zakłócanie, wpływanie lub ingerowanie w zagrożenia online stwarzane przez wrogie podmioty, takie jak państwa obce, zorganizowana przestępczość lub grupy ekstremistyczne.

Działania te wykraczają daleko poza stereotypowy obraz technologicznych geniuszy w kapturach, którzy włamują się do komputerów zagranicznych cyberprzestępców i sieją spustoszenie w ich systemach (choć i to się zdarza). W ubiegłym roku CSE przeprowadzało operacje przeciwko organizacjom stosującym przemoc i ekstremizm. „Korzystając z wielopłaszczyznowego podejścia ukierunkowanego na infrastrukturę techniczną i obecność online grup VEO (Violent Extremist Organizations), CSE przeprowadziło aktywne operacje cybernetyczne, aby zaszkodzić wiarygodności i wpływom kluczowych liderów grup, ograniczając ich zdolność do inspirowania i przewodzenia" – czytamy w raporcie. – „Operacje te miały również na celu osłabienie zaufania i zmniejszenie spójności między liderami i zwolennikami, podważając jedność i siłę tych organizacji".

Zapytana w wywiadzie, czy CSE prowadzi internetowe kampanie zniesławiające przywódców organizacji ekstremistycznych, zastępczyni szefa Cyber Centre, Bridget Walshe, odmówiła

podania szczegółów. „Trudno mi wchodzić w szczegóły dotyczące faktycznie stosowanych technik, ponieważ ich ujawnienie wpłynęłoby na ich skuteczność” – powiedziała Walshe. CSE twierdzi, że w ubiegłym roku fiskalnym otrzymała zezwolenie na przeprowadzenie czterech aktywnych lub obronnych operacji cybernetycznych, w tym jednej wymierzonej w 10 największych grup zajmujących się oprogramowaniem ransomware atakującym Kanadę.

W jednym przypadku, pod koniec zeszłego roku, agencja wykryła grupę ransomware atakującą Kanadyjczyków pracujących w sektorze infrastruktury krytycznej. W ciągu 48 godzin, jak czytamy w raporcie, zespoły CSE zidentyfikowały i powiadomiły ofiary oraz przeprowadziły cyberoperację w celu zakłócenia działalności grupy przestępczej. Agencja wywiadowcza poinformowała również, że pomogła zidentyfikować legalne przedsiębiorstwa, które potajemnie wspierały działania militarne, polityczne i handlowe rządów obcych państw, mające na celu osłabienie Kanadyjskich Sił Zbrojnych.

Walshe nie chciała powiedzieć, czy przedsiębiorstwa te były kanadyjskie lub czy miały powiązania z Kanadą, ale zauważyła, że mandat CSE nie pozwala jej podejmować działań przeciwko obywatelom Kanady.

CSE po raz kolejny stwierdza, że Chińska Republika Ludowa jest zdecydowanie największym zagrożeniem dla bezpieczeństwa narodowego Kanady, a jej działania obejmują zarówno szpiegostwo, kradzież własności intelektualnej, jak i represje transnarodowe. Cele Chin są rozległe i obejmują rząd, społeczeństwo obywatelskie, media, przemysł zbrojeniowy oraz sektor badawczo-rozwojowy. „Skala, umiejętności handlowe i ambicje programu cybernetycznego ChRL w cyberprzestrzeni nie mają sobie równych”. Rosja również pozostaje kluczowym aktorem zagrożenia, który kontynuuje działalność szpiegowską, rozpowszechnia dezinformację i przeprowadza operacje wywierania wpływu przeciwko Kanadyjczykom.

W odróżnieniu od lat ubiegłych, w raporcie rocznym za rok 2024–2025 nie wspomniano o Korei Północnej, a jedynie o zagrożeniu cybernetycznym ze strony Iranu. Mimo to Walshe stwierdziła, że oba te reżimy nadal stanowią problem dla Kanady.

Opracowanie: Andrzej Kumor
Źródło: Goniec.net