Cyberdefence 24

aut. Szymon Palczewski 13.02.2019

UE PRZECIWKO CHIŃSKIM HAKEROM. PLAN WSPÓLNEJ ODPOWIEDZI

Państwa członkowskie Unii Europejskiej rozważają możliwość wspólnej odpowiedzi na cyberataki przeprowadzone przez chińskich hakerów. Przyczyną takiego stanu rzeczy są dowody przedstawione przez brytyjskich specjalistów dotyczące infiltracji wewnętrznych sieci.

Eksperci z Wielkiej Brytanii podczas styczniowego spotkania technicznego poinformowali przedstawicieli Unii Europejskiej o incydentach. Przedstawili dowody dotyczące zarówno ataków wymierzonych w oprogramowania, jak i infrastrukturę przeprowadzonych przez grupę Advanced Persistent Threat 10 (APT 10).

Skupienie na działalności APT 10 jest przejawem narastających podejrzeń Unii oraz Stanów Zjednoczonych o szpiegostwo oraz kradzież własności intelektualnej przez Chiny. Grupa państwowych hakerów została oskarżona w grudniu przez Departament Sprawiedliwości USA o zorganizowanie kampanii szpiegowskiej, obejmującej infiltrację amerykańskich firm oraz podmiotów z innych państw.

W specjalnym oświadczeniu strony chińskiej skierowanym do UE stwierdzono, że „oskarżenia niektórych państw przeciwko Chinom w sprawie cyberbezpieczeństwa są bezpodstawne”. Równocześnie Pekin wezwał kraje do „zaprzestania zniesławiania Chin, aby nie podważać ich stosunków dwustronnych i współpracy z innymi państwami”.

W przypadku jakiejkolwiek kary wymierzonej w Chiny związanej z cyberatakami, państwa członkowskie UE musiałyby jednogłośnie stwierdzić, że Pekin jest odpowiedzialny za incydenty. Niemniej jednak są kraje nie zgadzające się z oskarżeniami skierowanymi wobec Państwa Środka. W związku z tym, Wspólnota podjęła pracę nad projektem sankcji, które mają być nakładane na konkretną grupę lub pojedynczego cyberprzestępcę w reakcji na złośliwy incydent.

W grudniu brytyjskie MSZ dołączyło do stanowiska Waszyngtonu, oskarżając APT 10 o działalności na rzecz chińskiego rządu „w celu przeprowadzenia złośliwej cyberkampanii ukierunkowanej na własność intelektualną oraz wrażliwe dane handlowe w Europie, Azji i USA”.

Eksperci NATO również zajmą się sprawą chińskich cyberataków. Jak powiedział sekretarz generalny NATO Jens Stoltenberg – „Widzieliśmy raporty sojuszników na temat ich obaw dotyczących chińskiej działalności związanej z infrastrukturą i cyberprzestępczością. Są to raporty, które traktujemy poważnie i będziemy kontynuować konsultacje w tych kwestiach”.

Spear Phishing

Departament Sprawiedliwości USA wskazuje, że grupa APT 10 podczas ataków wykorzystuje metodę spear phishingu. Hakerzy tworzą złośliwe wiadomości e-mail, które mają być wierną kopią treści

pochodzących z legalnych adresów. Następnie zainfekowane maile rozsyłane są wraz z załącznikami oraz plikami zawierającymi szkodliwe oprogramowanie. Po ich otworzeniu cyberprzestępcy uzyskują dostęp do urządzenia, co umożliwia kradzież danych i wrażliwych informacji.

Specjaliści firmy FireEye, śledzącej działalność APT 10 od 2009 roku, twierdzą, że chińska grupa od dawna specjalizuje się w atakach na przedsiębiorstwa z branży telekomunikacyjnej, lotniczej czy inżynieryjnej. Celem hakerów są również systemy rządowe m.in. w Stanach Zjednoczonych, Europie oraz Japonii. W ten sposób APT 10 chce wesprzeć działania chińskich komórek wywiadu.