aut. Sylwia Gliwa 02.03.2021

INDYJSKO-CHIŃSKI CYBERKONFLIKT. GRUPA REDECHO UDERZA W ENERGETYKĘ I PORTY MORSKIE

Od początku 2020 roku eksperci Recorded Future zaobserwowali duży wzrost podejrzanych działań ukierunkowanych na włamania przeciwko indyjskim organizacjom. Atakujący zostali zidentyfikowani jako chińska grupa sponsorowana przez państwo.

Celem działań stał się indyjski sektor energetyczny, a także dwa porty morskie. Ataki na infrastrukturę krytyczną wskazują, że głównym motywem działań nie jest szpiegostwo przemysłowe – twierdzi Recorded Future, który zidentyfikował i opisał wykryte działania chińskich hakerów.

Ataki na infrastrukturę krytyczną zdaniem badaczy nie stanowią jednak zasadniczego celu działań kontrolowanej przez państwo grupy. Eksperci przewidują, że są one jedynie wstępem do pozycjonowania dostępu do sieci w na rzecz wsparcia chińskich celów strategicznych w przyszłości.

Czytaj też: Pierwszy atak na sieci energetyczne w USA. Czy było to celowe działanie?

Wykorzystywane przez RedEcho narzędzia, które zostały zidentyfikowane przez Recorded Future są rozpowszechnione pośród chińskich grup powiązanych z ministerstwem Bezpieczeństwa Państwowego oraz Chińską Armią Ludowo-Wyzwoleńczą - działalność grupy RedEcho oraz używane przez nich narzędzia pokrywają się z innymi chińskimi grupami, w tym APT41 oraz Tonto Team.

Członkowie grupy APT41 oskarżeni zostali przez Departament Sprawiedliwości USA o ataki na podmioty niemal z całego spektrum branż, w tym m.in. firmy programistyczne, producentów sprzętu komputerowego, dostawców usług telekomunikacyjnych, media społecznościowe, firmy gamingowe, organizacje non-profit, uniwersytety, think tanki i zagraniczne rządy, a także prodemokratycznych polityków i działaczy w Hong Kongu.

Kryzys na linii New Delhi-Beijing stopniowo narasta, a kolejnym polem, na który zostały przeniesione działania jest cyberprzestrzeń. Indie banują kolejne chińskie aplikacje. Na przestrzeni ostatnich miesięcy zdecydowano się wpisać na czarną listę ponad 170 apek – od gier wideo, poprzez popularne serwisy randkowe aż po aplikacje gigantów sprzedażowych jak AliExpress. Jak wskazywały indyjskie media w listopadzie ubiegłego roku po dokonaniu kolejnej już serii banów, na liście 500 najbardziej popularnych aplikacji w Indiach nie ma ani jednego chińskiego produktu.

Czytaj też: Ban za banem. Indie blokują kolejne chińskie aplikacje

W oficjalnym komunikacie do sprawy, który został opublikowany w listopadzie ubiegłego roku, indyjski rząd wskazał, że podstawą do podjęcia działań była m.in. dbałość o suwerenność, bezpieczeństwo państwa oraz zachowanie porządku publicznego. „Rząd zobowiązuje się do ochrony interesów obywateli oraz suwerenności i integralności Indii na wszystkich frontach i podejmie wszelkie możliwe kroki, aby to zapewnić" – wskazano w komunikacie.

Rząd indyjski wykorzystuje cyberprzestrzeń do prowadzenia działań w ramach konfliktu z Pakistanem. W lutym br. opisywaliśmy sprawę działań oraz oprogramowania przypisanym grupie Confucius, która, jak wskazują eksperci, jest dobrze znana z podszywania się pod legalne służby, aby zatrzeć ślady i zmylić swoje ofiary. Wykryte przez ekspertów narzędzia, wykorzystywane są, jak twierdzą badacze, do prowadzenia działań wymierzonych w personel powiązany z pakistańskimi władzami wojskowymi, członkami administracji związanej z badaniami nuklearnymi oraz indyjskimi urzędnikami wyborczymi w Kaszmirze.

Czytaj też: Cyberkonflikt indyjsko-pakistański. New Delhi wystawiło grupę do zadań specjalnych?