aut. Andrzej Kozłowski 21.05.2020

CHIŃSCY HAKERZY ODPOWIEDZIALNI ZA ATAKI NA TAJWAN?

Władze Tajwanu sugerują, że chińscy hakerzy stali za atakiem ransomware wymierzonym w państwowego giganta z branży petrochemicznej, który jest kluczowym elementem tajwańskiej gospodarki.

Dane, które zostały pozostawione po ataku takie jak konfiguracja plików czy nazwa domen wskazują na chińską grupę znaną jako Winnti albo ugrupowania blisko z nią związane – wskazuje Ministerstwo Sprawiedliwości Tajwanu. Winnti składa się z dużej liczby hakerów, która zdaniem ekspertów, jest powiązana z chińskim rządem.

Chińscy hakerzy od dawna przeprowadzają operacje przeciwko Tajwanowi, głównie w celu zbierania informacji. Atak na przedsiębiorstwo z branży petrochemicznej, które jest odpowiedzialne za dostarczenie produktów naftowych, w celu jego unieruchomienia stanowi śmielszy krok i eskalację w wzajemnych tajwańsko-chińskich relacjach w cyberprzestrzeni. Atak wprawdzie nie wpłynął na produkcję energii przez CPC's, ale spowodował problemy z płatnościami za gaz przy wykorzystaniu kart CPC Corp. Atak ransomware zmusił również przedsiębiorstwo z sektora petrochemicznego do przebudowania części swojej infrastruktury i wprowadzenia bardziej rygorystycznego systemu zabezpieczeń.

Specjaliści firmy Trend Micro zidentyfikowali kampanię, której celem było tajwańskie przedsiębiorstwo. Eksperci nazwali ją ColdLock. Podkreślili, że podczas cyberataku hakerzy wykorzystali oprogramowanie ransomware. „Złośliwe oprogramowanie wydaje się atakować bazy danych i serwery e-mail w celu szyfrowania" – czytamy w oficjalnym komunikacie Trend Micro. Cyberatak rozpoczął się na początku maja.

Analiza incydentu wykazała podobieństwa między ColdLock a dwiema znanymi wcześniej rodzinami ransomware, w szczególności Lockergoga oraz Freezing. Hakerzy starali się uzyskać dostęp do wewnętrznych serwerów wybranych organizacji, aby następnie zainstalować złośliwe oprogramowanie na danym urządzeniu.

CPC stanowi atrakcyjny cel dla hakerów. Tajwan jest w dużym stopniu uzależniony od importu surowców energetycznych, a firma zainwestowała w wiele morskich projektów naftowych i gazowych.

To jednak nie jedyny przypadek ataku ransomware w ostatnich tygodniach. Ministerstwo Sprawiedliwości Tajwanu poinformowało, że również inne przedsiębiorstwa z sektora energetycznego oraz nowoczesnych technologii stały się ofiarą ataku.

Biorąc pod uwagę sytuację polityczną, która ma miejsce pomiędzy Tajwanem a Chinami trop chińskich hakerów wydaje się być oczywistym. Chińscy hakerzy zostali również oskarżeni o próbę kradzieży wyników badań nad zwalczaniem koronawirusa przez FBI i Departament Bezpieczeństwa

Wewnętrznego. To jednak nie jedyna aktywność Państw Środka w cyberprzestrzeni. Japończycy oskarżają ich o kradzież projektu pocisku hipersonicznego, a Wietnam o atak na swoje bazy danych. Wygląda na to, że obok Bliskiego Wschodu rejon Azji Południowo-Wschodniej staję arenę wymiany ciosów między państwami w cyberprzestrzeni.

Czytaj też: Plany japońskiego pocisku hipersonicznego wykradzione?