Cyber 669 w infowojnie w Czechach?

#Strategia i polityka 21 maja 2020

W Izraelu mówi się nieoficjalnie, że za najnowszym epizodem informatycznej wojny w cyberprzestrzeni z Iranem – zablokowaniem komputerów portu Szahid Radżaji (używamy perskiej fonetycznej pisowni) w północnej części Cieśniny Ormuz – może stać supertajna tzw. Jednostka 669 Cyber.

Port Szahid Radżaji – najnowocześniejszy irański terminal kontenerowy w północnej części Cieśniny Ormuz został sparaliżowany na ponad 10 dni za pomocą cyberataku Izraelczyków / Zdjęcie: ARSANG

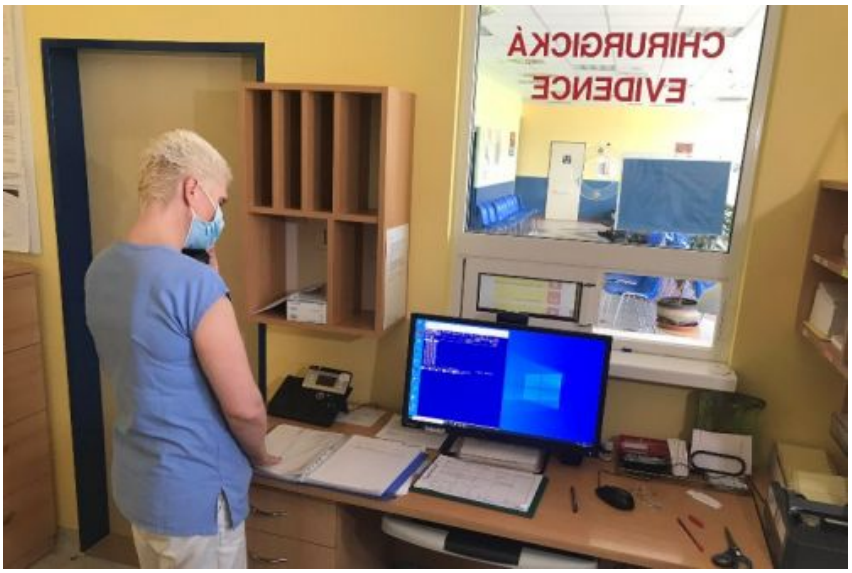
Jest to nieformalna, popularna nazwa formacji odpowiedzialnej za obronę i kontrataki w sieci, utworzona w nawiązaniu do symbolu Oddziału 669 Chejl ha-Awir (izraelskich wojsk lotniczych) przeznaczonego do zadań ratownictwa bojowego. Podobnie, w sytuacjach nadzwyczajnych w cyberprzestrzeni do akcji wkraczać mają eksperci 669 Cyber.

Irańczykom dopiero teraz, po ponad 10 dniach od ataku na sieć komputerów zawiadujących ruchem w porcie i terminalu kontenerowym Szahid Radżaji udało się przywrócić nad nimi kontrolę. Szahid Radżaji to przede wszystkim nowoczesne morskie centrum przeładunku kontenerów, położone 14,5 km na zachód od wielkiego portu i ośrodka stoczniowego Bandar Abbas, zajmujące obszar 2400 ha. Przez jego 23 nabrzeża przepływa rocznie ponad 70 mln t ładunków.

9 maja 2020 komputery nadzorujące ruch w porcie zostały sparaliżowane. Dziennik *Washington Post* podał powołując się na swoje źródła, że była to akcja bojowa Izraelczyków w odpowiedzi na próbę irańskiego cyberataku na dwie izraelskie sieci dystrybucji wody na rolnicze tereny wiejskie – co w przypadku sukcesu miałoby daleko idące skutki dla rolnictwa i gospodarki izraelskiej – podjętą 24 kwietnia 2020. Została ona podobno zawczasu wykryta i udaremniona. W Państwie Hebrajskim mówi się, że za obie akcje – tę obronną i tę zaczepną – odpowiada właśnie 669 Cyber.

Według *Washington Post* irańskim hakerom udało się jednak wniknąć do systemu zarządzającego uzdatnianiem i chlorowaniem dwóch sieci wody (odsolonej z morza) w Izraelu i układu odprowadzającego ścieki. Szybko to jednak dostrzeżono i straty były minimalne. Tymczasem kontratak na port Szahid Radżaji spowodował wielodniowy przestój najnowocześniejszego w Islamskiej Republice Iranu terminalu kontenerowego. Co prawda w oficjalnym komunikacie irańskiej agencji prasowej czytamy, że syjonistyczny atak na port nie spowodował przestojów, jednak zdjęcia satelitarne ukazujące wielodniowe, ogromne korki na drogach dojazdowych oraz zagęszczenie statków czekających na redzie na rozładunek, do których dotarł *Washington Post*, świadczą same za siebie.

Irańskie media poinformowały, powołując się na generalnego dyrektora zarządu portów irańskich Mohammada Rastada, że cyberatak na Szahid Radżaji objął jedynie prywatne systemy zarządzania niektórymi strefami portu, a napastnikom nie udało się przeniknąć do jądra sterującego całością operacji. Irańskie agencje przypomniały także, że już 15 grudnia 2019 minister łączności i technologii informatycznych Dżawad Azari-Dżahromi ujawnił, że Iran odkrył próby instalacji wrogich oprogramowań w swoich serwerach rządowych. Zostały one jednak wykryte i udaremnione.



Komputery centrum medycznego Brnie zostały w kwietniu 2020 sparaliżowane, podobnie jak systemy wielu innych czeskich szpitali i lotnisk. Pomoc mieli przynieść specjaliści z izraelskiej 669 Cyber / Zdjęcie: PNbrno

Sprawa ma jednak także wymiar środkowoeuropejski. W Izraelu mówi się, że Jednostka 669 Cyber weszła do akcji w kwietniu 2020 na naszym gruncie, pomagając specjalistom Republiki Czeskiej w odpieraniu cyberataku na serwery szpitali, ośrodków zdrowia zajętych walką z pandemią. Uderzenie objęło także lotniska, miedzy innymi centralny praski port lotniczy. Według czeskich mediów za atakiem stali rosyjscy hakerzy operujący także za pomocą chińskich serwerowni. W kraju naszych południowych sąsiadów wiązano to z konfliktem politycznym na linii Praga – Moskwa i wojną słów po usunięciu na początku kwietnia 2020 przez praskie władze pomnika sowieckiego marszałka Iwana Koniewa (stał od 1980).

Ponieważ liczba zainfekowanych i zneutralizowanych systemów informatycznych czeskich szpitali rosła, według nieoficjalnych informacji wezwano na pomoc specjalistów izraelskich z 669 Cyber, którzy po kilku godzinach mieli odzyskać kontrolę nad sytuacją. Istotne jest to, że w 2017 Republika Czeska i Izrael zwarły porozumienie o wzajemnej pomocy w działaniach w cyberprzestrzeni. Wszystko na to wskazuje, że z niego skorzystano…
