Cyberdefence 24

aut. Sylwia Gliwa 08.04.2020

MASOWA KAMPANIA HAKERÓW UDERZYŁA W CHINY

W trakcie pandemii hakerzy powiązani z grupą DarkHotel zaatakowali chińskie instytucje, które posiadają swoje siedziby poza granicami kraju – twierdzi chińska firma zajmująca się cyberbezpieczeństwem. Ataku dokonano przejmując kontrolę nad siecią VPN a ofiarami padły organizacje nawet z 19 krajów z trzech kontynentów.

Chińska firma Qihoo 360 za pośrednictwem swojego bloga twierdzi, że hakerzy z grupy DarkHotel (APT-C-06) powiązani prawdopodobnie z północnokoreańskim rządem, od marca tego roku przejęli ponad 200 serwerów VPN. W ich opinii umożliwiło to atak na wiele chińskich instytucji za granicą. Ataków miano dokonać za pośrednictwem przejętego serwera SangFor VPN. Na początku kwietnia, jak twierdzą Chińczycy, atak rozprzestrzenił się na agencje rządowe w Pekinie i Szanghaju.

Specjaliści z Qihoo 360 zwrócili uwagę, że w ramach globalnej walki z pandemią koronawirusa VPNny odgrywają ważną rolę podczas zdalnej komunikacji przedsiębiorstw, a nawet rządów. W ich opinii, grupa całkowicie kontrolowała serwer VPN zastępując kluczowy program oprogramowania programem zawierający tzw. tylną furtkę – gdy użytkownicy logowali się, hakerzy mieli kontrolę nad każdym urządzeniem końcowym, który zalogował się do sieci.

W komunikacie chińska firma ostrzega, że zaatakowane zostały chińskie instytucje w 19 krajach w Europie, Azji i Afryce. Zdaniem specjalistów z uwagi na fakt, że wiele firm za granicą przeszło na tryb pracy zdalnej a pracownicy tych organizacji nawiązywali kontakt pomiędzy sobą za pośrednictwem sieci VPN przekazując również dane wrażliwe, skutki tego ataku mogą być niewyobrażalne.

Grupa hakerów DarkHotel, na którą wskazują specjaliści z Qihoo 360, na początku marca próbowała włamać się do systemów Światowej Organizacji Zdrowia. Zdaniem ekspertów była to jedna z najpoważniejszych prób tego rodzaju w ostatnim czasie. Do ataku próbowano wykorzystać stronę bliźniaczą podobną do wewnętrznego systemu poczty elektronicznej WHO. Światowa Organizacja Zdrowia potwierdziła, do szło do próby kradzieży haseł od pracowników organizacji.

Również na początku marca, specjaliści z Qihoo 360 twierdzili, że posiadają dowody, na amerykańskie szpiegostwo w sieci. Jak dowodzili na swoim blogu, CIA miało pozyskać wrażliwe informacje odnośnie chińskich przedsiębiorstw w tym z branży lotniczej, ośrodków badań naukowych, przemysłu naftowego, firm IT oraz agencji rządowych. Dowody na szpiegostwo ze strony Stanów Zjednoczonych, specjaliści mieli odnaleźć w dokumentach ujawnionych na portalu WikiLeaks szczegółowe metody ataku, cele, narzędzia a także specyfikacje techniczną grupy hakerów CIA. Chińska firma na ich podstawie prześledziła amerykańskie ataki od września 2008 roku do czerwca 2019 roku i dotarła do celów zlokalizowanych na terenie Chin – skupiły się one w stolicy kraju oraz w prowincjach Guangdong i Zhejiang.

Czytaj też: CIA przyłapana na cyberszpiegostwie w Chinach. WikiLeaks przyczyną porażki?