EKSPERT: PRZEJĘCIE RUCHU SIECIOWEGO NIE BYŁO PRZYPADKOWE

Ataki takie jak przejęcie przez rosyjskiego operatora ruchu sieciowego wielu firm na kilka minut mają miejsce regularnie. Przypadki czy awarie, które powodują takie efekty, zdarzają się dość rzadko. Prawdopodobieństwo, że przejęcie ruchu nastąpiło przez przypadek jest, ale niskie, prawie tak jak wygrana piątki w lotto - mówi Tomasz Wodziński, kierownik I i II linii SOC, Biuro zarządzania usługami bezpieczeństwa Exatel.

Zdaniem Wodzińskiego, nie mając dowodów na celowe działanie, możemy tezę o ataku rozważać. - Jest prawdą, że obecnie najbardziej spektakularne efekty cyberprzestępcy osiągają za pomocą celowych, kierunkowych, dobrze przygotowanych pod kątem danego celu ataków. Tu mieliśmy do czynienia raczej z działaniem szerokim, pozornie nie wymierzonym w konkretną organizację, lecz mającym skopiować realny ruch w internecie - mówi ekspert Exatel.

- Czy te terabajty danych, które przez siedem minut operator mógł sobie zapisać, zawierają krytyczne informacje? Nie wiemy, ale teoretycznie mogą. Na przykład, jeśli akurat w tym czasie były zestawiane połączenia VPN między placówkami banków, to zapis tego procesu jest na dyskach hakerów. Teraz na tych danych można uruchomić automatyczną analizę, poszukiwać ciekawych danych, być może śladów źle skonfigurowanych zabezpieczeń - mówi Tomasz Wodziński.

Czytaj też: Ponad 1000 przypadków WannaCry w Polsce

Jego zdanie, analizując dane można zorientować się, jakie usługi i protokoły są używane w komunikacji danej organizacji. – Jeśli w grę wchodzi rynek finansowy (VISA, Mastercard, HSBC, Fortis Bank, BZ WBK), to sprawę automatycznie trzeba traktować podejrzliwie. Jak mówi powiedzenie – jeśli nie wiadomo, o co chodzi, chodzi o pieniądze - dodaje Wodziński.