Cyberdefence 24

aut. Szymon Palczewski 07.04.2020

ROSYJSKI TELEKOM PRZEJMUJE RUCH INTERNETOWY. BŁĄD CZY CELOWE DZIAŁANIE?

Rosyjski dostawca usług telekomunikacyjnych odpowiada za incydent wymierzony w system służący do kierowania ruchu internetowego między sieciami internetowymi na całym świecie (BGP). Nie jest to pierwszy przypadek, w którym Rosja ukierunkowuje swoje złośliwe operacje w BGP.

Ruch przeznaczony dla ponad 200 największych sieci na świecie sieci dostarczania treści (CDN) i dostawców hostingu w chmurze został podejrzanie przekierowany do Rosji przez Rostelecom, czyli rosyjskiego państwowego dostawcy usług telekomunikacyjnych – donosi serwis ZDNet.

Incydent dotknął ponad 8800 tras ruchu internetowego z ponad 200 sieci i trwał około godziny. Wśród firm, które odczuły tego skutki należy wskazać między innymi na Google, Amazon, Facebook, Akamai, Cloudflare, GoDaddy, Digital Ocean, Joyent, LeaseWeb, Hetzner czy Linode.

Jak wskazuje ZDNet, incydent to klasyczny przykład na „przejęcie BGP". Skrót ten oznacza *Border Gateway Protocol* i jest de facto systemem służącym do kierowania ruchu internetowego między sieciami internetowymi na całym świecie. W przeszłości, zanim HTTPS był szeroko stosowany, incydenty wymierzone BPG umożliwiały hakerom przeprowadzenie cyberataków typu Man-in-the-middle (MitM) oraz przechwytywanie i modyfikowanie ruchu internetowego.

We współczesnym świecie ingerencja w BGP jest nadal niebezpieczna, ponieważ pozwala zewnętrznym podmiotom rejestrować ruch, analizować oraz odszyfrowywać go w przyszłości, gdy szyfrowanie użyte do jego zabezpieczenia osłabnie z powodu postępu w dziedzinie kryptografii.

ZDNet podkreśla, że niektóre podmioty regularnie zajmują się porwaniami BGP, a także incydentami, które wielu ekspertów określa jako „podejrzane". China Telecom jest obecnie uważany za najbardziej agresywny w tym aspekcie. Jednak Rostelecom również słynie z przeprowadzenia wielu incydentów. Ostatni tak poważny ze strony rosyjskiego podmiotu miał miejsce w 2017 roku, gdy ingerowano w trasy BGP dla niektórych największych światowych podmiotów finansowych, w tym Visa, Mastercard czy HSBC.

Czytaj też: Elita rosyjskich hakerów uderza w Armenię