

NORDVPN: ZOSTALIŚMY ZHAKOWANI

Dostawca jednej z najpopularniejszych usług wirtualnej sieci prywatnej NordVPN przyznał, że w marcu 2018 roku padł ofiarą niezidentyfikowanych do tej pory hakerów - podano w oficjalnym oświadczeniu. Przesłane mieli włamać się do jednego z centrów danych firmy.

Rzeczniczka NordVPN Laura Tyrell powiedziała serwisowi TechRadar, że "jedno z centrów danych w Finlandii, od którego wynajmują serwery, odnotowało nieautoryzowany dostęp".

"Na serwerze nie znajdowały się żadne dane dotyczące aktywności użytkowników (...) w związku z tym loginy i hasła nie mogły być przechwycone" - podkreśliła.

"Jedyną możliwością zakłócenia ruchu strony internetowej jest przeprowadzenie ataku z użyciem spersonalizowanej techniki man-in-the-middle do przechwycenia pojedynczego połączenia z NordVPN" - tłumaczyła przedstawicielka firmy. Man-in-the-middle polega na podsłuchu i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami transakcji czy korespondencji.

Zdaniem TechRadar hakerzy zidentyfikowali zdalny system zarządzania, którego operatorem był dostawca usług centrum danych. Wykorzystując nieaktualny certyfikat TLS mogli uzyskać pełen dostęp do zawartości serwera. Były haker @hexdefined ocenił, że cyberprzestępcy otrzymali "pełną kontrolę nad nim (serwerem)" i mogli obserwować ruch internetowy przebiegający przez tamtejszą sieć.

TechRadar przypomina, że rejestry logowania NordVPN zostały opublikowane przez hakerów na stronie 8Chan. Wraz z nimi zamieszczono także dane dwóch innych dostawców: VikingVPN i Torguard. Może to świadczyć, że te trzy podmioty korzystały z tego samego centrum danych - podaje TechRadar.