LUKA W BEZPIECZEŃSTWIE USŁUGI VPN UMOŻLIWIŁA ATAK NA SIEĆ KANTORÓW

Atak z użyciem oprogramowania szyfrującego na sieć kantorów Travelex był możliwy przez lukę bezpieczeństwa usługi Pulse Secure VPN, z której korzystano w tej firmie - wynika z analizy wykonanej przez badacza cyberbezpieczeństwa Kevina Beaumonta. Do incydentu doszło w Nowy Rok.

Cytowany przez serwis Ars Technica specjalista stwierdził, że sieć kantorów Travelex korzystała z siedmiu serwerów usługi Pulse Secure VPN, które obarczone były podatnością cyberbezpieczeństwa. Informacje o luce, z której skorzystali hakerzy działający w ramach grupy Sodinokibi, dostępne były na forach internetowych od sierpnia 2019 roku, aktualizacja zabezpieczająca przed nią natomiast została wydana przez dostawcę usługi VPN w kwietniu.

Istotą działania podatności jest pozwolenie cyberprzestępcom na uzyskanie zdalnego dostępu do serwera bez konieczności podawania danych do logowania. Następnie wykorzystujący lukę hakerzy mogą swobodnie wyłączyć uwierzytelnianie dwuskładnikowe, przeglądać logi i dane do logowania innych użytkowników sieci zapisane w pamięci podręcznej serwera usługi. Zdaniem eksperta, podatność w wypadku ataku na Travelex posłużyła hakerom nie tylko do infiltracji sieci firmy, ale także do wykradzenia danych oraz zainstalowania złośliwego oprogramowania szyfrującego REvil.

Aktywność grupy Sodinokibi atakującej z użyciem tego wirusa została zaobserwowana po raz pierwszy w kwietniu ubiegłego roku przez ekspertów z firmy Cisco Talos. Hakerzy wykorzystali wówczas podatność serwerów usługi Oracle WebLogic. Złośliwe oprogramowanie REvil wysyła do hakerów zwrotne informacje na temat systemu, który zainfekowało, jednakże - jak podkreślają specjaliści - nie ma zdolności samorozprzestrzeniania się do innych sieci, przez co cyberprzestępcy korzystający z niego zmuszeni są do wykorzystania różnych metod jego rozpowszechniania w atakowanych strukturach, np. z użyciem spamu.

O wszczęciu dochodzenia ws. cyberataku na Travelex informował w środę dziennik "Financial Times". Hakerzy domagają się od firmy okupu za nieujawnianie wrażliwych danych klientów kantorów, które wykradli z zaatakowanej sieci.