aut. Szymon Palczewski 25.09.2020

HAKERZY PRZEŁAMALI ZABEZPIECZENIA AGENCJI FEDERALNEJ USA

Hakerzy przeprowadzili skuteczny cyberatak na jedną z amerykańskich agencji federalnych, przełamując jej zabezpieczenia. Cyberprzestepcy, uzyskując dostęp do wewnętrznej sieci, przeglądali zbiory danych, a następnie pobrali interesujące ich pliki.

Amerykańska Cybersecurity and Infrastructure Security Agency (CISA) wykryła cyberatak wymierzony w wewnętrzną sieć jednej z agencji federalnych USA. Podczas operacji hakerzy wykorzystali pozyskane dane uwierzytelniające w celu zainstalowania złośliwego oprogramowania na konkretnych systemach. W ten sposób uzyskali do nich stały dostęp, wykorzystując słabe punkty zapory sieciowej poszkodowanego podmiotu – wynika z komunikatu opublikowanego przez CISA.

Jak wskazuje Agencja, hakerzy posiadali ważne poświadczenia dostępu do kont Microsoft Office 365 wielu użytkowników oraz profilu administratora. Pozwoliło im to na „wejście" do sieci poszkodowanej agencji, której CISA nazwy nie zdradza dla dobra sprawy. „Najpierw cyberprzestępcy zalogowali się na konto użytkownika w usłudze Microsoft Office 365 (…), a następnie przeglądali foldery w celu pobrania plików" – tłumaczy CISA.

Specjaliści Agencji nie byli w stanie określić, w jaki sposób hakerzy uzyskali poświadczenia, aby uzyskać dostęp do sieci. Możliwe, że wykorzystali do tego celu lukę CVE-2019-11510 w Pulse Secure. Eksperci nie mają wątpliwości, że hakerzy przeglądali systemy poszkodowanej agencji, a następnie pobrali interesujące ich pliki.

Po zalogowaniu na koncie administratora sieci cyberprzestępcy łączyli się ze zdalnym serwerem. Zainstalowali również złośliwe oprogramowanie do przenoszenia i podmieniania plików w wybranym systemie. Alarmujący jest fakt, że hakerom udało się „pokonać zabezpieczenia agencji federalnej" – wskazuje CISA w komunikacie.

Czytaj też: USA: postawiono zarzuty irańskim hakerom powiązanym z Gwardią Rewolucyjną