PRODUKTY USŁUG POCZTOWYCH W RĘKACH HAKERÓW. LUKA WYKORZYSTANA DO NAMIERZANIA KLIENTÓW

Hakerzy złamali certyfikaty wydane przez Mimecast - dostawcę usług pocztowych i wykorzystali je do namierzania klientów - poinformowała firma w oświadczeniu. Sprawę może mieć związek z tzw. hackiem dekady.

Mimecast został zaalarmowany przez ekspertów Microsoftu, którzy poinformowali, że podmiot o zaawansowanych umiejętnościach złamał certyfikat używany do uwierzytelnienie produktów Mimecastu (Sync and Recover, Continuity Monitor i IEP) do serwisu chmurowego Microsoft 365 Exchange. W swoim oświadczeniu firma oświadczyła, że 10% klientów używało tych produktów, z czego ofiarą padło zaledwie kilku z nich. Biorąc pod uwagę, że takie ataki hakerskie należą do tych bardziej zaawansowanych można wnioskować, że celem były konkretne, wcześniej wytypowane osoby.

Mimecast skontaktował się z ofiarami i zarekomendował jak najszybsze zaprzestanie używania połączenia opartego na złamanych certyfikatach i ponownego nawiązania połączenia przy użyciu certyfikatu zastępczego. Firma zapewniła, że w żaden sposób nie wpłynie to na przepływ poczty przychodzącej ani wychodzącej.

Mimecast jest międzynarodową firmą zajmującą się zarządzaniem pocztą elektroniczną w chmurze Microsoft Exchange i Microsoft Office 365 w tym w usługach bezpieczeństwa, archiwizacji i ciągłości w celu ochrony poczty biznesowej. Firma oferuje wiele narzędzi zwiększających cyberbezpieczeństwo, takich jak blokowanie linków ze złośliwym oprogramowaniem, prób phisingu czy używania przez atakujących fałszywych tożsamości, aby wyłudzić od ofiar informacje.

W rozmowie z Reutersem, trzech ekspertów ds. cyberbezpieczeństwa wskazało, że grupa, która dokonała ataku na Mimecast wcześniej stała za tzw. hackiem dekady, czyli włamaniem do twórcy oprogramowania SolarWinds. Amerykański rząd wskazał, że stoi za nim Rosja, a Kaspersky zidentyfikował liczne podobieństwa pomiędzy rosyjską grupą Turla a sprawcami ataku na SolarWinds. Turla według zachodnich wywiadów jest związaną z FSB.