**Linie lotnicze i dane pasażerów celem hakerów Scattered Spider**

**W lipcu 2025 roku świat obiegła niepokojąca wiadomość: dane 6 milionów klientów australijskich linii lotniczych Qantas zostały wykradzione w wyniku wyrafinowanego cyberataku. Śledztwo szybko skierowało uwagę specjalistów ds. cyberbezpieczeństwa na grupę znaną jako Scattered Spider – nowego i niezwykle groźnego gracza w cyberprzestępczym podziemiu. W ciągu zaledwie kilku miesięcy ich ofiarą padły również Hawaiian Airlines oraz WestJet. Eksperci firmy Check Point Research (CPR) alarmują: sektor lotniczy znalazł się w centrum nowej fali ataków.**

Ataki na linie lotnicze nie są przypadkowe – sektor ten, z racji skomplikowanej infrastruktury i licznych partnerów zewnętrznych (np. call center, dostawców IT), staje się idealnym celem. Eksperci podkreślają, że wiele naruszeń bezpieczeństwa miało swoje źródło w tzw. "łańcuchu dostaw" – słabych punktach u partnerów, których systemy miały dostęp do głównej infrastruktury przewoźników.

**Kim są Scattered Spider?**

Scattered Spider to grupa działająca co najmniej od 2022 roku, składająca się głównie z młodych ludzi w wieku 19–22 lat z USA i Wielkiej Brytanii. Motywacją grupy jest zysk finansowy, a ich działania koncentrują się na wyłudzaniu danych uwierzytelniających, włamywania się do struktur chmurowych oraz żądaniu okupów w ramach tzw. ransomware-as-a-service, m.in. z użyciem oprogramowania **BlackCat/ALPHV**.

Ich działania charakteryzują się wysokim poziomem wyrafinowania, a głównym narzędziem są zaawansowane metody inżynierii społecznej: podszywanie się pod pracowników wsparcia technicznego, voice phishing (vishing), MFA fatigue(„push bombing”), a także nakłanianie pracowników do instalowania złośliwego oprogramowania.

- S*cattered Spider działa w sposób oportunistyczny – nie ograniczają się do jednej branży, lecz dynamicznie adaptują swoje ataki do najbardziej podatnych na zagrożenia sektorów* – ostrzegają analitycy Check Point Research.

**Nowa taktyka: phishing domenowy na szeroką skalę**

Jednym z najnowszych odkryć CPR jest zidentyfikowanie ponad 500 domen phishingowych wykorzystywanych (lub przygotowywanych) przez Scattered Spider. Domeny te wiernie imitują portale logowania do systemów korporacyjnych i są tworzone według powtarzalnego schematu:

l nazwa-firmy-sso.com

l nazwa-firmy-servicedesk.com

l nazwa-firmy-okta.com

Przykłady zidentyfikowanych domen to m.in.:

l chipotle-sso[.]com

l gemini-servicedesk[.]com

l hubspot-okta[.]com

Chociaż nie wszystkie z tych domen zostały jednoznacznie uznane za aktywnie szkodliwe, to ich zgodność z metodami działania grupy (TTPs – tactics, techniques and procedures) wskazuje na wysokie prawdopodobieństwo ich użycia w przyszłych kampaniach.

Jak firmy lotnicze powinny zabezpieczyć się przed zagrożeniem? Eksperci wskazują przede wszystkim na analizę ryzyka dostawców usług dla sektora – szczególnie pod kątem bezpieczeństwa danych pasażerów i dostępu do systemów rezerwacji. Niezbędne jest również wprowadzenie wielowarstwowej weryfikacji tożsamości – przy resetach haseł i obsłudze klientów. Oraz ustalenia wektorowych procedur reagowania na incydenty – gotowych scenariuszy działania na wypadek wycieku danych.

Eksperci są zgodni,Scattered Spider to przykład nowego pokolenia cyberprzestępców: młodych, technicznie uzdolnionych, operujących z poziomu internetu, lecz uderzających realnie – w klientów, dane i reputację wielkich korporacji. Lotnictwo, z jego międzynarodową skalą, rozbudowanymi systemami i krytycznymi usługami, stało się kolejnym frontem tej cyfrowej wojny. *- Scattered Spider nie przestanie atakować – to firmy muszą przestać być łatwym celem* – podsumowuje Wojciech Głażewski, dyrektor firmy Check Point Software Technologies w Polsce.