Bitdefender

Irańscy cyberprzestępcy wykorzystują fałszywe poświadczenia związane z kluczowymi infrastrukturami

18.10.2024

Amerykańska Agencja Bezpieczeństwa Cybernetycznego i Infrastruktury Bezpieczeństwa (CISA) wydała ostrzeżenie, że irańscy cyberprzestępcy przenoszą swoją działalność ze szpiegostwa na pośrednictwo w uzyskiwaniu wstępnego dostępu. Zgodnie z ostrzeżeniem opublikowanym przez wiodące agencje ds. cyberbezpieczeństwa w USA, Kanadzie i Australii, osoby atakujące dokonują włamań do organizacji z sektora energetycznego, rządowego, służby zdrowia i innych ważnych sektorów, a następnie sprzedają dane dostępowe na forach dark webu.

Irańscy cyberprzestępcy w natarciu

Od października 2023 r. irańscy cyberprzestępcy stosują techniki siłowe,

w tym ataki polegające na rozsyłaniu haseł i ataki polegające na zmęczeniu uwierzytelnianiem wieloskładnikowym (MFA), aby zmusić swoje ofiary do nieumyślnego udzielenia im dostępu.

Po włamaniu się do systemu osoby atakujące starają się zachować wytrwałość, co pozwala im na zbieranie danych uwierzytelniających, eskalowanie uprawnień i przeprowadzanie rozpoznania naruszonych sieci.

Sektory o wysokim profilu na celowniku

Eksperci uważają, że irańscy napastnicy zamierzali sprzedać dostępy temu, kto da najwięcej na forach cyberprzestępczości. W ten sposób ułatwili ataki kolejnym gangom ransomware. Innymi słowy, irańscy hakerzy przeszli od szpiegostwa do działania jako pośrednicy dla innych cyberprzestępców.

Wyraźne skupienie się hakerów na sektorach opieki zdrowotnej, energetycznym i rządowym może skutkować poważnymi zakłóceniami w świadczeniu podstawowych usług, zagrożeniem bezpieczeństwa publicznego i naruszeniem poufnych danych.

Wykorzystanie zmęczenia MFA i samodzielnego resetowania hasła

„Według ostrzeżenia atakujący stosują metodę „push bombing" MFA, czyli bezwzględną taktykę polegającą na przytłaczaniu użytkowników powtarzającymi się prośbami o zalogowanie, dopóki nie udzielą dostępu,

czasami przypadkowo lub z czystej frustracji. Dlatego to niezwykle istotne, abyś nigdy automatycznie nie klikał zgód w komunikatach, które wyświetlają się na ekranie" – mówi Krzysztof Budziński z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Inna taktyka preferowana przez sprawców polega na uzbrojeniu samoobsługowych narzędzi do resetowania haseł połączonych z publicznymi katalogami w celu resetowania wygasłych haseł. Pozwala to atakującym zarejestrować własne urządzenia w systemie MFA celu.

Rola Iranu w cyberprzestępczości sponsorowanej przez państwo

Eksperci ds. bezpieczeństwa uważają, że te działania mogą być powiązane z cyberatakiem sponsorowanym przez państwo. Odrębny poradnik rządu USA wskazuje na irańską grupę zagrożeń działającą pod pseudonimami Br0k3r, Fox Kitten i Pioneer Kitten, która prawdopodobnie jest wspierana przez Iran.

Grupa cyberprzestępcza jest powiązana z wieloma naruszeniami bezpieczeństwa na całym świecie, w trakcie których sprzedała pełną kontrolę nad domeną i uprawnienia podmiotom powiązanym z ransomware i innymi podmiotami stanowiącymi zagrożenie.

Oznaki kompromisu i łagodzenie

Aby ograniczyć ryzyko takich ataków, organizacje i osoby prywatne powinny zwracać uwagę na następujące sygnały ostrzegawcze:

- Nieoczekiwane rejestracje MFA lub próby z nieznanych urządzeń, lub nieznanych lokalizacji.
- Podejrzana aktywność wiersza poleceń, która może wskazywać na zrzucanie poświadczeń.
- Uprawnione korzystanie z konta po zresetowaniu hasła lub złagodzeniu zagrożeń dla konta użytkownika.
- Nagła aktywność na kontach, które wcześniej były uśpione lub na kontach, na których zwykle nie ma żadnej aktywności lub jest ona niewielka.

Źródło:https://bitdefender.pl/iranscy-cyberprzestepcy-wykorzystuja-falszywe-poswiadczenia-zwiazane-z-kluczowymi-infrastrukturami/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 18.10.2024
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim

korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.