Milano, 27 luglio 2023 - Nel secondo trimestre del 2023 gli attacchi informatici sono aumentati in maniera considerevole rispetto al periodo gennaio-marzo. Secondo i dati pubblicati dal Report Trimestrale di Cisco Talos Incident Response (Talos IR), la più grande organizzazione privata di intelligence al mondo dedicata alla cybersecurity, sul primo gradino del podio troviamo le estorsioni: un tipo di attacco in aumento del 25% rispetto al primo trimestre e particolarmente pericoloso, attraverso cui i criminali informatici sono soliti rubare i dati minacciando di diffonderli a meno che la vittima non accetti di pagare una cospicua somma di denaro, senza la necessità di utilizzare la crittografia. Al secondo posto, con una crescita del 17% - contro il 10% di gennaio-marzo - ci sono invece i ransomware, divisi in diverse famiglie tra cui 8base e MoneyMessage.

I principali target

Il settore della sanità pubblica e privata è quello più colpito di questo trimestre, seguito da quelli dei servizi finanziari e delle utility.

Vettori iniziali

Nella maggior parte degli eventi a cui Talos IR ha risposto in questo trimestre, i criminali informatici hanno ottenuto l'accesso iniziale utilizzando credenziali compromesse per accedere ad account validi. L'uso di account validi è stato osservato in quasi il 40% degli interventi totali, con un aumento del 22% rispetto al primo trimestre del 2023.

In oltre il 50% degli attacchi di questo trimestre, è stata osservata PowerShell, un'utility dinamica della riga di comando che continua a essere una scelta molto frequente per i criminali informatici per una serie di motivi tra cui l'invisibilità, la praticità e le ampie funzionalità di gestione IT.

Punti deboli della sicurezza

La mancanza o un'implementazione impropria dell'autenticazione a più fattori (MFA) nei servizi critici è stata responsabile di oltre il 40% degli eventi a cui Cisco Talos ha risposto in questo trimestre. In quasi il 40% dei casi, i criminali informatici hanno utilizzato credenziali compromesse per accedere ad account validi, il 90% dei quali non disponeva di MFA.

In altri casi, è stato aggirato l'MFA con attacchi di esaurimento che si verificano quando l'aggressore tenta di autenticarsi ripetutamente a un account utente con credenziali valide per sommergere le vittime di notifiche push MFA, sperando che alla fine accettino per poi autenticarsi con successo.