Cambiano i tipi di attacco: aumentano i web-shell ma diminuiscono i ransomware. Colpiti anche i settori immobiliare e della vendita al dettaglio

Milano, 4 maggio 2023 - Quasi il 30% delle minacce informatiche avvenute nel primo trimestre del 2023 sono state di tipo web-shell, quella particolare categoria di attacchi che sfrutta la vulnerabilità di server e applicazioni per eseguire comandi, spostare file, accedere ai log ed eseguire query malevole.

Di minore percentuale invece gli attacchi ransomware e pre-ransomware - quelli cioè utilizzati per entrare in un dispositivo e chiedere un riscatto per restituirne l'accesso - passati nei primi tre mesi dell'anno dal 20% a circa il 10%. Questi i primi elementi messi a fuoco dal Report Trimestrale di Cisco Talos, la più grande organizzazione privata di intelligence al mondo dedicata alla cybersecurity.

Secondo
il Report gennaio-marzo la maggior parte di questi attacchi sono inoltre
riconducibili a gruppi hacker di spicco come, ad esempio, Vice Society, mentre

altro fattore preoccupante è rappresentato dall'abilità dei criminali informatici nel combinare diversi metodi di accesso e strumenti flessibili e adattabili, per aumentare la probabilità di distribuire ulteriori malware (malicious software) o per ottenere informazioni sensibili e private.

I principali target

La sanità pubblica e privata è stato il settore più colpito di questo trimestre, seguito da quelli della vendita al dettaglio, del commercio, del settore immobiliare e dell'ospitalità.

I principali punti deboli

Il 45% degli attacchi ha sfruttato le applicazioni utilizzate dagli utenti, un aumento significativo rispetto al 15% del trimestre precedente. A ciò si aggiungono la compromissione di account che hanno utilizzato password troppo semplici e con una sola autenticazione.

La mancanza dell'autenticazione a più fattori (MFA) rimane uno dei maggiori ostacoli alla sicurezza aziendale: quasi il 30% delle vittime non ha abilitato l'MFA o lo ha fatto solo su pochi account e servizi critici, permettendo così al criminale informatico di accedere e autenticarsi.