[stato di internet] - security

Analisi delle tendenze sulle minacce nel settore del commercio

La continua digitalizzazione delle organizzazioni commerciali dopo la pandemia da COVID-19 ha potenziato la crescita aziendale, ma ha anche introdotto rischi per la sicurezza del perimetro e dei clienti.

Attacchi alle organizzazioni del settore del commercio

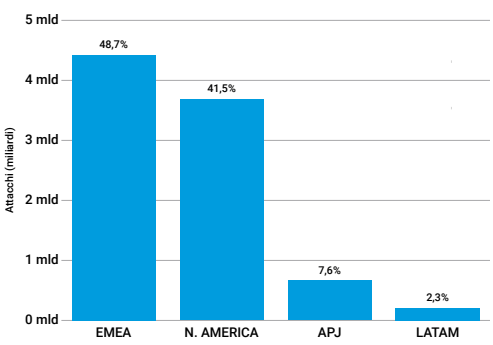
Oltre 14 miliardi

Attacchi alle API e alle applicazioni web nel settore del commercio

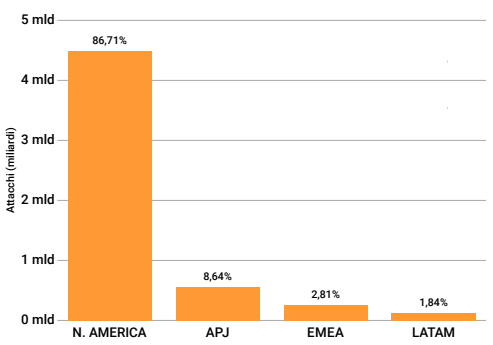
314%

Attacchi LFI (Local File Inclusion) dal terzo trimestre 2021 al terzo trimestre 2022

I vettori di attacco emergenti, come SSRF (Server-Side Request Forgery) e SSTI (Server-Side Injection Template), rappresentano una minaccia significativa per il settore del commercio e per altri segmenti verticali in considerazione del potenziale impatto e dei danni che possono causare attraverso l'esfiltrazione dei dati e l'esecuzione di codice in modalità remota.



L'area EMEA (Europa, Medio Oriente e Africa) ha superato il Nord America per quanto riguarda gli attacchi alle applicazioni web e alle API sferrati contro il settore retail



Il Nord America è il primo per attacchi alle applicazioni web e alle API nella categoria Hotel e viaggi, seguito dall'area Asia-Pacifico e Giappone

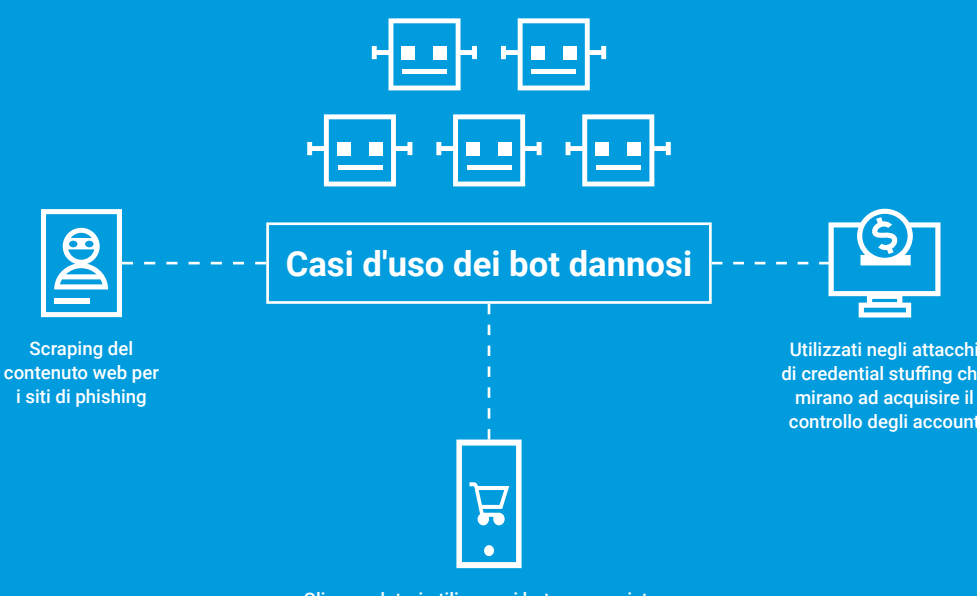
Gli assalti ai clienti del settore del commercio continuano

30,2%

Campagne di phishing che hanno imitato brand commerciali nel 1° trimestre del 2023

> 5 mila miliardi

Richieste di bot dannosi da gennaio 2022 a marzo 2023



Per maggiori informazioni e approfondimenti sulle tendenze degli attacchi a cui è esposto il settore del commercio, leggete il rapporto completo.

Scarica il rapporto completo

 | Supporto | Data di pubblicazione: 06/23