L'innovazione e i suoi rischi:

tendenze degli attacchi nei servizi finanziari

In un'epoca caratterizzata da una trasformazione digitale senza precedenti, il settore dei servizi finanziari si trova al crocevia tra innovazione e rischi. Riplasmando lo scenario delle transazioni finanziarie, la tecnologia apre le porte ad una nuova epoca di minacce che mirano direttamente al cuore della stabilità economica.

Attacchi contro i servizi finanziari e i suoi clienti

9 miliardi

Numero di attacchi alle applicazioni web e alle API nei servizi finanziari

Numero 1

I servizi finanziari sono il primo settore maggiormente preso di mira dagli attacchi DDoS, sorpassando persino il gaming

50,6%

I servizi finanziari contano il maggior numero di vittime degli attacchi di phishing nel 2° trimestre 2023

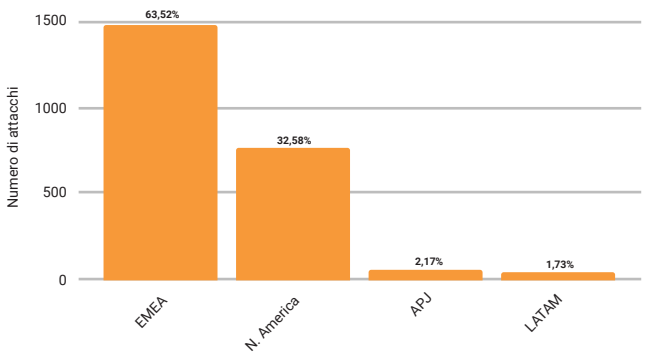
Oltre mille miliardi

Numero di richieste di bot dannosi

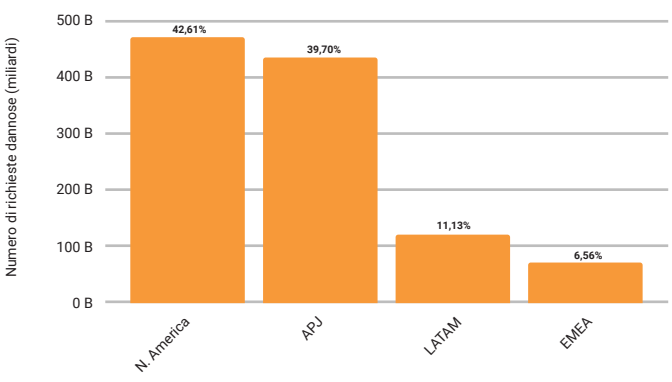
Panoramiche locali

Il numero di attacchi DDoS di livello 3 e 4 che hanno colpito l'area EMEA (Europa, Medio Oriente e Africa) è quasi raddoppiato rispetto a quello del Nord America

Attacchi DDoS per area geografica: i servizi finanziari
1° gennaio 2022 - 30 giugno 2023



Richieste di bot dannosi per area geografica: i servizi finanziari
1° gennaio 2022 - 30 giugno 2023



La regione APJ (Asia-Pacifico e Giappone) è la seconda area più colpita per numero di richieste di bot dannosi

Potenziali rischi alla sicurezza da monitorare

API ombra

Le API non documentate e non tracciate possono creare problemi di monitoraggio per le aziende che non sanno chi e come le utilizza.

Script di terze parti

I criminali possono sfruttare le vulnerabilità lato client o iniettare codice dannoso negli script di terze parti, che vengono caricati come parte di un sito web. Questo approccio mette i servizi finanziari a rischio di attacchi di web skimming, il che può condurre al furto dei dati dei clienti o al loro utilizzo in transazioni non autorizzate.

Aggregatori finanziari

Le falle nella sicurezza tra aggregatori finanziari e metodi di raccolta dei dati possono dare potenzialmente adito a nuovi tentativi di sfruttamento da parte dei criminali, conducendo ad episodi di furto di identità.

Consigli e best practice sulla sicurezza

- Conoscere la propria superficie di attacco per elaborare appropriate strategie di mitigazione e stabilire adeguati controlli di sicurezza
- Implementare appositi strumenti per la sicurezza delle API in grado di rilevare e monitorare le API non autorizzate
- Utilizzare l'OWASP API Security Top 10 e il framework MITRE ATT&CK per sviluppare corsi di formazione e piani di test per red team/gruppi di test di penetrazione
- Adottare una strategia di difesa multilivello, che include l'esecuzione di regolari controlli di sicurezza e l'implementazione di avanzate procedure di rilevamento e mitigazione
- Utilizzare soluzioni come Client-Side Protection & Compliance (in precedenza, Page Integrity Manager) in grado di mitigare i rischi posti dagli attacchi lato client
- Creare un modello di governance basato sull'edge per fornire visibilità sul traffico di bot/API
- Condurre un esercizio dal vivo se non si sono subiti attacchi DDoS negli ultimi tre trimestri; convalidare i playbook e monitorare le tendenze degli attacchi sia per dimensioni che per velocità per valutare il rischio in base alle funzionalità correnti

Per maggiori informazioni e approfondimenti sulle tendenze degli attacchi nel settore dei servizi finanziari, leggete il nostro rapporto completo.

Scarica il rapporto

 | Supporto | Data di pubblicazione: 10/23