Uno sguardo al lato client

Il linguaggio JavaScript è fondamentale per fornire eccellenti user experience, ma lascia il vostro sito web vulnerabile alle minacce lato client e al furto di dati degli utenti finali.

Gli attacchi di web skimming, Magecart e formjacking possono avere conseguenze dannose per i brand, dalle sanzioni alla perdita di fiducia da parte dei clienti fino al calo del fatturato.

Dove inizia l'infezione

Sfruttamento delle vulnerabilità proprietarie

Errata configurazione della sicurezza, vulnerabilità del framework, ecc.

Attacchi alla supply chain di terze parti

Iniezione di codice dannoso tramite un provider di terze parti autorizzato

Come gli attacchi di web skimming rubano i dati degli utenti finali

L'utente finale naviga online

Applicazione web

L'utente finale accede ad **informazioni sensibili** sulla pagina di pagamento

I dati vengono sottratti mediante l'iniezione di **script dannosi**

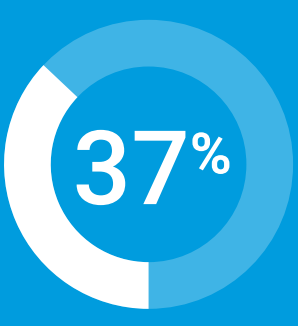
Codice JavaScript violato

I dati vengono raccolti ed **esfiltrati** tramite un dominio controllato dal criminale

Il codice JavaScript di terze parti lascia i brand vulnerabili

Percentuale di codice JavaScript sui siti web che proviene da terze parti

Retail e commercio[1]



Servizi finanziari[2]

Una minaccia per le aziende di tutte le dimensioni

L'81% dei grandi retailer online segnala che le loro organizzazioni sono state prese di mira da comportamenti di script sospetti nel 2022[3]

Un impatto devastante

4,45 milioni di dollari	Costo medio di una violazione dei dati a livello globale nel 2023[4]
9,48 milioni di dollari	Costo medio di una violazione dei dati negli Stati Uniti nel 2023[4]

La conformità al PCI ora richiede un sistema di sicurezza lato client

PCI Security Standards Council

Le organizzazioni che elaborano i dati delle carte di pagamento dovranno conformarsi ai nuovi **requisiti di sicurezza JavaScript del PCI DSS v4.0 entro il 2025** per evitare di incorrere in pesanti sanzioni[5]

Requisito 6.4.3 | **Requisito 11.6.1**

Akamai Client-Side Protection & Compliance

Akamai Client-Side Protection & Compliance protegge dalle minacce JavaScript, semplifica i workflow per il PCI DSS v4.0 e tiene al sicuro i dati degli utenti finali. Inoltre, fornisce visibilità sulle vulnerabilità JavaScript e analizza il comportamento degli script per rilevare eventuali attività dannose e illecite. Infine, genera anche avvisi che consentono ai team addetti alla sicurezza di mitigare e proteggere rapidamente dagli attacchi lato client.

Per ulteriori informazioni, visitate la nostra pagina sul prodotto o contattate il team di vendita di Akamai.

1. Analisi delle tendenze sulle minacce nel settore del commercio | Akamai SOTI 2023
2. L'innovazione e i suoi rischi: tendenze degli attacchi nei servizi finanziari | Akamai SOTI 2023
3. Bot e script dannosi: l'efficacia di sistemi di difesa specializzati | 2023
4. Rapporto IBM sul costo di una violazione di dati | 2023
5. PCI DSS v4.0 | 2022