Surveillance du côté client

Bien qu'essentiel pour offrir des expériences utilisateur puissantes, JavaScript laisse votre site Web vulnérable aux menaces côté client et au vol de données des utilisateurs finaux.

Les attaques de web skimming, les attaques de type Magecart et le détournement de formulaire peuvent avoir des conséquences néfastes pour les marques : amendes, érosion de la confiance des clients et perte de revenus.

Où commence l'infection

Exploitation des vulnérabilités internes

Mauvaise configuration de la sécurité, vulnérabilités de la structure, etc.

Attaques de la chaîne d'approvisionnement par des tiers

Injection de code malveillant via un fournisseur tiers autorisé

Comment les attaques de web skimming volent les données des utilisateurs finaux

Utilisateur final surfant sur Internet

Application Web

L'utilisateur final saisit **des informations sensibles** sur la page de paiement

Données dérobées via l'injection d'un **script malveillant**

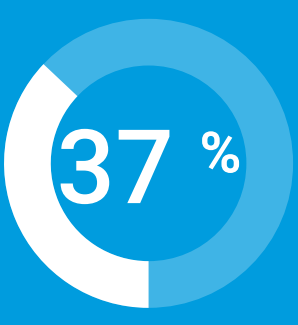
JavaScript **compromis**

Données collectées et **exfiltrées** par un domaine contrôlé par un attaquant

Le JavaScript tiers laisse les marques vulnérables

Pourcentage de codes JavaScript sur les sites Web provenant de sources tierces

Vente au détail et commerce[1]



Services financiers[2]

Une menace pour les entreprises de toutes tailles

81 % des grands détaillants en ligne déclarent que leur organisation a été ciblée par un comportement de script suspect en 2022[3]

L'impact dévastateur

4,45 M $	Coût moyen total d'une violation de données à l'échelle mondiale en 2023[4]
9,48 M $	Coût moyen total d'une violation de données aux États-Unis en 2023[4]

La conformité PCI nécessite désormais une sécurité côté client

Security Standards Council

Toute organisation qui traite des données de carte de paiement devra se conformer aux nouvelles **exigences de sécurité JavaScript PCI DSS v4.0 d'ici 2025** pour éviter des pénalités[5]

Exigence 6.4.3 | **Exigence 11.6.1**

Client-Side Protection & Compliance d'Akamai

La solution Client-Side Protection & Compliance d'Akamai protège contre les menaces JavaScript, rationalise les workflows PCI DSS v4.0 et protège les données des utilisateurs finaux. Elle fournit une visibilité sur les vulnérabilités JavaScript et analyse le comportement des scripts pour détecter les activités de script nuisibles et malveillantes. Elle génère également des alertes exploitables qui permettent aux équipes de sécurité d'atténuer les risques et de se protéger rapidement contre les attaques côté client.

Pour en savoir plus, rendez-vous sur notre page produit ou contactez l'équipe commerciale Akamai.

1. Rapport Analyse des tendances des menaces : attaques dans le secteur du commerce | Rapport État des lieux d'Internet 2023 d'Akamai
2. Les enjeux immenses de l'innovation : tendances des attaques ciblant les services financiers | Rapport État des lieux d'Internet 2023 d'Akamai
3. Des bots malveillants aux scripts malveillants : les défenses spécialisées en action | 2023
4. Rapport IBM sur le coût d'une violation de données | 2023
5. PCI DSS v4.0 | 2022

 | Publication : 12/23