Uma perspectiva do lado do cliente

O JavaScript é essencial para oferecer experiências de usuário avançadas, mas deixa seu website vulnerável a ameaças no lado do cliente e roubo de dados de usuários finais.

Ataques de skimming na Web, Magecart e formjacking podem resultar em consequências prejudiciais para as marcas, desde multas até perda de confiança e receita.

Onde a infecção começa

Exploração de vulnerabilidades internas

Configuração incorreta de segurança, vulnerabilidades de estrutura etc.

Ataques de cadeias de suprimento externas

Injeção de código mal-intencionado por meio de um provedor externo autorizado

Como os ataques de skimming na Web roubam dados de usuários finais

Usuário final navegando online

Aplicação da Web

O usuário final insere **informações confidenciais** na página de finalização de compra

Dados obtidos por injeção de script mal-intencionado

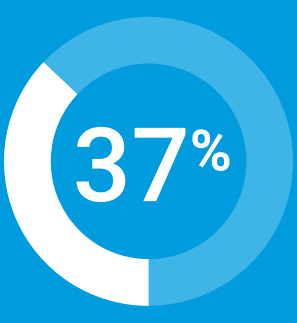
JavaScript **comprometido**

Dados coletados e **exfiltrados** por domínio controlado pelo invasor

O JavaScript externo deixa as marcas vulneráveis

Porcentagem de JavaScript em websites de origens externas

Varejo e comércio[1]



Serviços financeiros[2]

Uma ameaça a empresas de todos os portes

81% de grandes varejistas online relatam que sua organização foi alvo de um comportamento suspeito de scripts em 2022[3]

O impacto devastador

US$ 4,45 M	Custo médio total de uma violação de dados globalmente em 2023[4]
US$ 9,48 M	Custo médio total de uma violação de dados nos EUA em 2023[4]

A conformidade com PCI agora requer segurança no lado do cliente

PCI Security Standards Council®

Qualquer organização que processe dados de cartões de pagamento deve estar em conformidade com os novos **requisitos de segurança de JavaScript do PCI DSS v4.0 até 2025** para evitar sanções[5]

Requisito 6.4.3 | **Requisito 11.6.1**

Akamai Client-Side Protection & Compliance

O Akamai Client-Side Protection & Compliance protege contra ameaças JavaScript, simplifica os fluxos de trabalho do PCI DSS v4.0 e mantém seguros os dados de usuários finais. Ele fornece visibilidade de vulnerabilidades JavaScript e analisa o comportamento de scripts para detectar atividades de script prejudiciais e mal-intencionadas. Ele também fornece alertas práticos que permitem que as equipes de segurança mitiguem e evitem ataques do lado do cliente rapidamente.

Para saber mais, visite a página do produto ou entre em contato com a equipe de vendas da Akamai.

1. Análise de tendências de ameaças no setor comercial | Akamai SOTI 2023
2. Os altos riscos da inovação: tendências de ataque em serviços financeiros | Akamai SOTI 2023
3. De bots mal-intencionados a scripts maliciosos: a eficácia das defesas especializadas | 2023
4. Relatório IBM: Custo de uma violação de dados (em inglês) | 2023
5. PCI DSS v4.0 | 2022