客户端概况

JavaScript 对于实现出色的用户体验至关重要，然而，它也会让您的网站易于受到客户端威胁和最终用户数据窃取的侵扰。

Web 数据窃取、Magecart 和表单劫持会给品牌带来有害后果，包括罚款、信任度下降和收入损失。

感染开始的位置

利用第一方漏洞
安全配置错误、框架漏洞等

第三方供应链攻击
通过已获得授权的第三方提供商注入恶意代码

Web 数据窃取攻击如何窃取最终用户数据

最终用户上网浏览网页

Web 应用程序

最终用户在结账页面中输入**敏感信息**

通过
恶意脚本
注入所窃取的数据

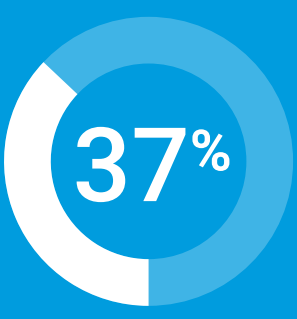
受感染的 JavaScript

由攻击者控制的域**收集**和**泄露的数据**

第三方 JavaScript 导致品牌容易受到攻击

网站中来自第三方来源的 JavaScript 所占百分比

零售和商业[1]



金融服务[2]

对各种规模的企业的威胁

2022 年，有 81% 的大型在线零售商报告其企业遭受过可疑脚本行为的攻击[3]

破坏性影响

445 万美元 2023 年全球范围内平均每次数据泄露造成的总损失[4]

948 万美元 2023 年美国境内平均每次数据泄露造成的总损失[4]

PCI 合规性现在要求实现客户端安全

Security Standards Council

在 2025 年之前，所有处理支付卡数据的企业都必须满足新的 **PCI DSS v4.0 JavaScript 安全要求**以避免受到罚款处罚[5]

要求 6.4.3 | **要求 11.6.1**

Akamai Client-Side Protection & Compliance

Akamai Client-Side Protection & Compliance 可防范 JavaScript 威胁，简化 PCI DSS v4.0 工作流程并确保最终用户数据安全。它提供对 JavaScript 漏洞的监测能力，并分析脚本行为以检测有害和恶意的脚本活动。此外，它还提供切实可行的告警，让安全团队能快速抵御和防范客户端攻击。

如需了解更多信息，请访问我们的产品页面或联系 Akamai 销售团队。

1. 商业行业的威胁趋势分析 | Akamai SOTI 2023
2. 创新遭遇高风险：金融服务业的攻击趋势 | Akamai SOTI 2023
3. 从恶意爬虫程序到恶意脚本：专业防御措施的有效性 | 2023
4. IBM《数据泄露的代价》| 2023
5. PCI DSS v4.0 | 2022

扫码关注，获取最新CDN前沿资讯