클라이언트 측 조치

자바스크립트는 강력한 사용자 경험을 제공하는 데 필수적이지만, 웹사이트가 클라이언트 측 위협과 최종 사용자 데이터 유출에 취약해질 수 있습니다.

웹 스키밍, Magecart, 폼재킹 공격은 벌금과 신뢰도 하락, 매출 손실 등 브랜드에 해로운 결과를 초래할 수 있습니다.

감염이 시작되는 곳

퍼스트파티 취약점 악용
보안 설정 오류, 프레임워크 취약점 등

써드파티 공급망 공격
권한 있는 써드파티 공급업체를 통한 악성 코드 인젝션

웹 스키밍 공격이 최종 사용자 데이터를 훔치는 방법

최종 사용자 온라인 브라우징

웹 애플리케이션

최종 사용자가 결제 페이지에 **민감한 정보** 입력

악성 스크립트 인젝션에 의한 데이터 스키밍

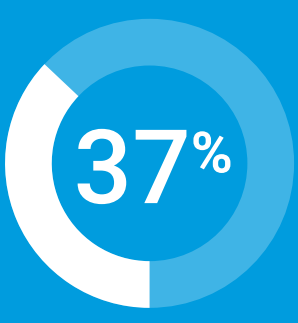
감염된 자바스크립트

공격자가 제어하는 도메인에 의한 **데이터 수집 및 유출**

브랜드를 취약하게 만드는 써드파티 자바스크립트

웹사이트 내 써드파티 소스로 제공되는 자바스크립트의 비율

리테일 및 커머스[1]



금융 서비스[2]

모든 규모의 기업에 대한 위협

대형 온라인 리테일 기업의 81%가 2022년에 의심스러운 스크립트 행동의 표적이 된 적이 있다고 답했습니다.[3]

파괴적인 영향

445만 달러 2023년 전 세계 데이터 유출로 인한 총 평균 비용[4]

948만 달러 2023년 미국 내 데이터 유출로 인한 총 평균 비용[4]

PCI 컴플라이언스를 위해 필요한 클라이언트 측 보안

Security Standards Council®

결제 카드 데이터를 처리하는 모든 기업은 과태료 처분을 피하기 위해 2025년까지 새로운 **PCI DSS v4.0 자바스크립트** 보안 요구사항을 준수해야 합니다[5]

요구사항 6.4.3 | **요구사항 11.6.1**

Akamai Client-Side Protection & Compliance

Akamai Client-Side Protection & Compliance는 자바스크립트 위협을 방어하고, PCI DSS v4.0 워크플로우를 간소화하며, 최종 사용자 데이터를 안전하게 보호합니다. 이 솔루션은 자바스크립트 취약점에 대한 가시성을 제공하고, 스크립트 행동을 분석해 유해한 악성 스크립트 활동을 탐지합니다. 또한 보안팀이 클라이언트 측 공격을 신속하게 방어하고 보호할 수 있도록 실행 가능한 알림을 제공합니다.

자세한 내용은 제품 페이지를 방문하거나 Akamai 영업 담당자에게 문의하시기 바랍니다.

1. 커머스 업계의 위협 트렌드 분석 | Akamai SOTI 2023
2. 혁신의 중대성: 금융 서비스 업계의 공격 트렌드 | Akamai SOTI 2023
3. 악성 봇에서 악성 스크립트로: 전문적인 방어 전략의 효과 | 2023
4. IBM 데이터 유출 비용 보고서 | 2023
5. PCI DSS v4.0 | 2022

 | 2023년 12월 발행