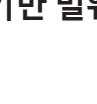


2025년 앱 및 API 보안 현황

AI가 디지털 환경을 변화시키는 방법

기업이 AI 기반 애플리케이션에 지속적으로 투자하면서 새로운 취약점이 발생하고 있습니다. 동시에, 공격자들은 AI를 활용해 공격의 전체 킬 체인을 자동화하고 있습니다. 그 결과, 웹 애플리케이션과 API를 노리는 공격은 규모가 커지고 정교함도 높아졌습니다.

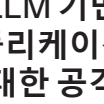
AI가 공격자에게 힘을 실어주는 6가지 방식



AI 기반 멀웨어



AI를 활용한 취약점 스캔



LLM 기반 애플리케이션에 대한 공격
(프롬프트 인젝션, 데이터 포이즈닝, 제일브레이킹 기술)



정교한 웹 스크레이핑



자동화된 DDoS(Distributed Denial-of-Service) 공격



로우 앤 슬로우 공격

웹 공격



33%

전 세계 웹 공격의 연간 증가율



영향

공격 급증을 촉진하는 AI

공격 급증은 클라우드 서비스, 마이크로서비스, AI 애플리케이션의 빠른 도입과 직접적으로 연관되어 있으며 이에 따라 공격 표면이 확장되고 새로운 보안 과제가 등장하고 있습니다.

웹 공격 업계 트렌드

2300억 건 이상
웹 공격

커머스 업계는 웹 공격으로 가장 큰 피해를 입었으며, 두 번째로 많은 공격을 받은 첨단 기술 업계보다 약 3배 더 많은 공격이 발생했습니다.

API 공격



32%

OWASP API 보안 상위 10대 취약점 관련 인시던트 증가율*



영향

더 취약한 AI 기반 API

대부분의 AI 기반 API는 외부에서 접속할 수 있으며, 불충분한 인증 메커니즘에 의존하는 경우가 많습니다. 이러한 취약점은 해당 API를 노리는 AI 기반 공격 유형이 점점 다양해지고 있는 상황에서 더욱 심각해지고 있습니다.

30%

MITRE 보안 프레임워크 관련 보안 알림 증가율*



영향

MITRE 프레임워크는 API를 표적으로 삼는 공격자의 기법에 대한 인사이트를 제공하는 데 여전히 중요한 역할을 합니다

공격자가 자동화와 AI를 활용해 API를 악용하는 상황에서, MITRE 프레임워크는 보안팀 직원이 이러한 공격을 더 빠르고 정확하게 식별하는 데 도움을 줄 수 있습니다.

레이어 7 DDoS 공격



94%

상위 10개 관련 인시던트에서 월간 레이어 7 DDoS 공격 규모 증가율



영향

공격의 정교함과 강도가 모두 증가하고 있습니다

공격자가 웹 애플리케이션 로직이나 API의 특정 취약점을 악용하기 위한 기술을 정교화하면서 레이어 7 DDoS 공격이 급증했습니다. 한편, 점점 더 정교해진 봇 기반 공격은 트래픽 패턴까지 정상적인 API 사용을 유사하게 모방하고 있습니다.

레이어 7 DDoS 공격 업계 트렌드

7조

2023년 1월부터 2024년 12월까지 가장 많이 영향을 받은 첨단 기술 업계를 표적으로 한 레이어 7 DDoS 공격 건수

방어 전략

- 시프트-레프트 및 DevSecOps API 보안 계획 수립
- 적응형 보안 엔진 사용
- API 테스트 툴 적용
- OWASP 보안 지침 구축
- 특화된 DDoS 방어 기술 개발
- 보안 프레임워크 모니터링
- 계층형 랜섬웨어 방어 체계 도입
- AI 기반 방화벽 및 봇 방어 솔루션 활용

*30일 기준 통계

전체 보고서를 다운로드해 공격 트렌드에 대한 독점 인사이트를 확인하세요.

보고서 다운로드

