2025 年应用程序与 API 安全现状

AI 如何改变数字格局

随着企业持续在 AI 赋能的应用程序上进行投资，由此带来新的漏洞，攻击者也趁机利用 AI 实现整个杀伤链的自动化。 这导致针对 Web 应用程序和 API 的攻击在数量和复杂程度上均有所增加。

攻击者利用 AI 的 6 种方式

- AI 增强型恶意软件
- AI 赋能的漏洞扫描
- 针对基于 LLM 的应用程序的攻击（提示注入、数据投毒、越狱技术）
- 先进的网络内容抓取
- 自动分布式拒绝服务 (DDoS) 攻击
- 低速缓慢攻击

Web 攻击

33%

全球 Web 攻击同比增幅

⚠ 影响

AI 正在加剧攻击激增

攻击激增与云服务、微服务和 AI 应用程序的快速普及直接相关，这些技术扩展了攻击面并带来新的安全挑战。

Web 攻击的行业趋势

超过 2300 亿次

Web 攻击

商业成为受 Web 攻击影响最严重的行业，所遭受的攻击数量几乎是排名第二的行业（高科技）的三倍。

API 攻击

32%

OWASP 十大 API 安全风险相关事件增幅*

⚠ 影响

AI 赋能的 API 安全性较低

大多数 AI 赋能的 API 可通过外部访问，且许多 API 依赖不完善的身份验证机制，这一漏洞随着 AI 驱动的攻击数量不断增加而加剧。

30%

与 MITRE 安全框架相关的安全告警增幅*

⚠ 影响

MITRE 框架对于深入了解攻击者针对 API 的技术仍然至关重要

随着攻击者使用自动化和 AI 来利用 API，MITRE 框架可以帮助防御者更快、更准确地识别这些攻击。

第 7 层 DDoS 攻击

94%

与十大风险相关事件关联的每月第 7 层 DDoS 攻击数量的增幅

⚠ 影响

攻击的复杂程度和强度不断增加

随着攻击者不断完善其利用 Web 应用程序逻辑或 API 中特定漏洞的技术，第 7 层 DDoS 攻击数量出现了激增。与此同时，日益复杂的爬虫程序驱动攻击的流量模式能够逼真地模仿合法的 API 用途。

第 7 层 DDoS 攻击的行业趋势

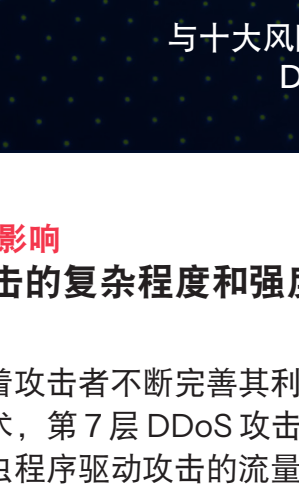
7 万亿次

2023 年 1 月到 2024 年 12 月，针对高科技行业的第 7 层 DDoS 攻击数量达到 7 万亿次，使其成为受影响最严重的行业。

抵御策略

- 采用左移和 DevSecOps API 安全计划
- 使用 Adaptive Security Engine
- 应用 API 测试工具
- 实施 OWASP 安全准则
- 开发专门的 DDoS 防护措施
- 监控安全框架
- 采用分层勒索软件防御措施
- 采用 AI 驱动的防火墙与爬虫程序防御解决方案

*在 30 天内



查看完整报告，获取对攻击趋势的独家见解。

下载报告