Akamai

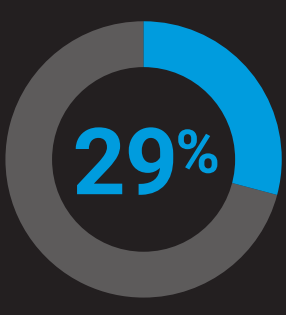
10 YEARS OF SECURITY INSIGHT

潜伏在阴影之中

攻击趋势揭示了 API 威胁

API 的广泛应用在现代企业中激发了创新热潮并提升了效率。但是，这也导致安全团队难以了解这些 API 带来的风险的规模和复杂性。大多数企业甚至无法说明其所有未进行归档的 API 或影子 API 的用途，这导致其网络边界上形成多个可受攻击的入侵点。在我们最新一期的研究报告中，您将看到最新的 API 攻击趋势。

聚焦 API 挑战



的 Web 攻击以 API 为目标（2023 年）

排名前三的 API 攻击媒介

44%
HTTP 攻击

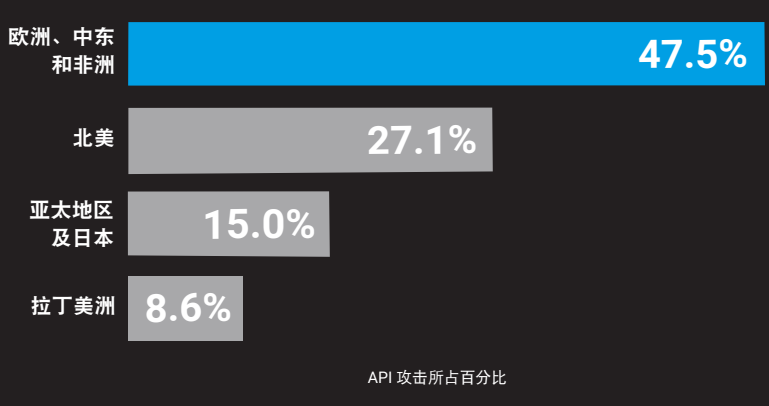
25%
活动会话

14%
结构化查询语言注入

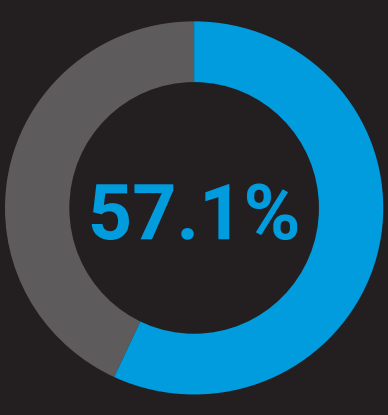
API 环境数据统计

API 攻击（按区域划分）

2023 年 1 月 1 日 – 2023 年 12 月 31 日



在全球范围内，欧洲、中东和非洲 (EMEA) 地区遭受的针对 API 的攻击占比最高，高达 47.5%。



的受访者估计其 API 清单的准确度介于 25% 到 75% 之间

基于 2023 SANS API 安全调查

遭受 API 攻击最多的三个垂直行业

- 商业
- 商业服务
- 其他数字媒体

企业需要回答的三个问题

API 滥用和利用可能超出了 OWASP 十大 API 安全风险清单中概述的漏洞范围。勾选相应的复选框，确保您实施了全面的安全策略：

- ☐ **漏洞**: 对于利用 API 进行的开发工作，您是否遵循了相应的最佳做法?
- ☐ **监测能力**: 您是否采取了适当的流程和技术控制措施来确保自己的安全计划能够保护您的所有 API?
- ☐ **业务逻辑滥用**: 您是否有可判断正常 API 流量的基准值，并以此来识别可疑活动?

为何监测能力很重要

API 漏洞是进入您环境的入侵点。您需要在攻击者之前发现这些漏洞。

保护 API 领域

如何保护您的 API

- ✔ 确保所有 API 都有文档记录并纳入到您的 API 安全控制措施中，以提升监测能力
- ✔ 解决 API 中的错误配置问题，并实施适当的流程以避免未来出现新的漏洞
- ✔ 建立 API 监控和威胁搜寻准则以消除安全漏洞，让攻击者无法再利用这些漏洞来攻击您
- ✔ 选择可以抵御从 OWASP 十大 API 安全风险到传统 Web 攻击的各种威胁的解决方案
- ✔ 利用与编码实践相关的 OWASP 指导来阻止常见攻击
- ✔ 使用提供行为分析的安全解决方案来检测业务逻辑滥用和其他异常情况

您所使用的 API 将需要满足合规性要求

PCI DSS v4.0 包含一些新标准，规定了在系统和软件的开发及维护过程中能够降低数据泄露风险的 API 使用方式。

提前做好防范攻击的准备

编码最佳做法包括先对您的 API 进行测试再将其投入生产环境，以及增强整个 API 生命周期内的安全性。

完整报告揭示了有关 API 攻击趋势和补救措施的更多内容。立即阅读。

下载报告

扫码关注，获取最新CDN前沿资讯