创新遭遇高风险

金融服务业的攻击趋势

在这个正在经历前所未有的数字化转型的时代，金融服务业站在了创新与风险的十字路口。技术在重塑金融交易环境的同时，也让这个新时代危机四伏，各种企图破坏经济稳定的威胁无处不在。

针对金融服务业及其客户的攻击

90 亿
针对金融服务业的 Web 应用程序和 API 攻击的数量

排名第一
金融服务业是遭受 DDoS 攻击最多的垂直行业，甚至超过了游戏行业

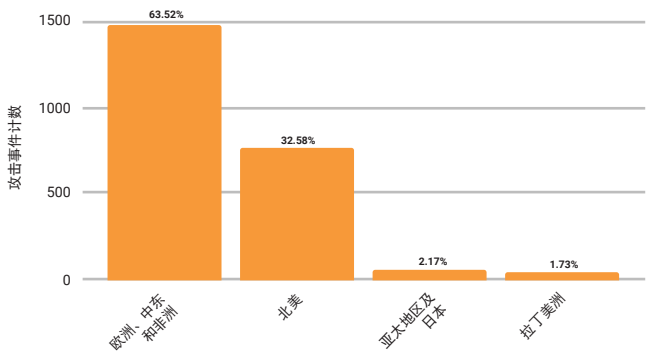
50.6%
2023 年第二季度，金融服务业中的网络钓鱼攻击受害者数量最多

1 万多亿次
恶意爬虫程序请求数量

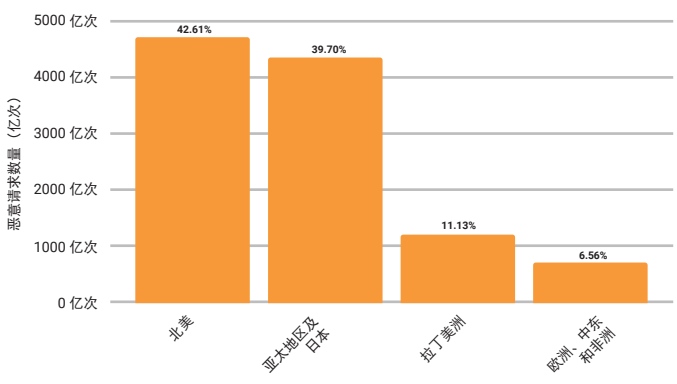
区域概况

欧洲、中东和非洲 (EMEA) 的第 3 层和第 4 层 DDoS 攻击的数量几乎是北美地区的两倍

按地区划分的 DDoS 攻击事件：金融服务业
2022 年 1 月 1 日 — 2023 年 6 月 30 日



按地区划分的恶意爬虫程序请求：金融服务业
2022 年 1 月 1 日 — 2023 年 6 月 30 日



亚太地区及日本 (APJ) 是恶意爬虫程序请求的第二大攻击目标区域

需要注意的潜在安全风险

影子 API
无文档记录也不进行跟踪的 API 会给公司带来监测问题，让公司无法知晓谁在使用以及以何种方式使用这些 API。

第三方脚本
攻击者会利用客户端漏洞或者将恶意代码注入到网站所加载的第三方脚本中。这会导致金融服务业面临 Web 数据窃取的风险，从而造成客户数据被窃取或用在未经授权的交易中。

金融聚合器
金融聚合器与数据收集方式之间的安全漏洞可能为攻击者带来新的可乘之机，导致发生身份盗窃。

安全建议和最佳实践

- 了解您的攻击面，以制定抵御策略并建立安全控制措施
- 部署用于检测和监控恶意 API 的 API 安全工具
- 使用 OWASP API 十大安全漏洞和 MITRE ATT&CK 框架为红队/渗透测试小组制定培训和测试计划
- 采用多层防御策略，其中包括定期进行安全审核及实施高级检测和抵御措施
- 采用能够缓解客户端攻击所带来的风险的解决方案，例如 Client-Side Protection & Compliance（以前称为 Page Integrity Manager）
- 构建基于边缘的治理模式，提供对爬虫程序/API 流量的监测能力
- 如果您在过去三个季度里没有遭遇 DDoS 攻击，不妨进行一次实战演练；根据当前能力验证您的行动手册，并跟踪规模和速度趋势以进行风险评估

有关金融服务业攻击趋势的更多信息和见解，请阅读我们的完整报告。

下载报告

 | 发布时间：2023 年 10 月

扫码关注 · 获取最新CDN前沿资讯