

## 关键见解

34%

### 金融服务机构遭受的第 3 层和第 4 层 DDoS 攻击事件百分比

金融服务业仍然是遭到第 3 层和第 4 层分布式拒绝服务 (DDoS) 攻击事件最多的行业。其后是游戏行业和高科技行业，分别占到 18% 和 15%。这种威胁类型的泛滥可能源于持续上演的地缘政治紧张局势，尤其是巴以冲突和俄乌战争，这些战争促使了全球黑客活动激增。



### API 使用量增长引发了第 7 层 DDoS 攻击的攀升

虽然 Web 应用程序一直以来是网络攻击的主要目标，但在本报告所覆盖的期间内，针对 API 的第 7 层 DDoS 攻击出现了明显的高峰。这很大程度上是因为，为了满足不断变化的监管和合规性要求，金融服务业越来越多地采用 API。由于企业对 API 的依赖程度越来越高，攻击者也在调整攻击手段，这使得 API 安全成为了现代企业的头等大事。



### 流量激增突显了按频率和攻击量评估 DDoS 的必要性

金融服务业中的 DDoS 攻击揭示了一个关键见解：攻击事件频率并非始终与攻击强度存在对应关系。虽然一些月份的攻击次数很少，但对应的 Gbps 数据量表明流量大幅增加，这强调了在评估 DDoS 攻击影响时需要同时考虑攻击频率和攻击量。

36%

### 针对金融机构的可疑域的百分比

网络钓鱼攻击越来越多地针对金融服务客户，这加剧了身份盗窃和帐户接管的风险。这种攻击趋势使得金融机构需要接受监管部门更严格的审查，而数据泄露会引发客户的信任问题。

30%

### 跳转到网络钓鱼和品牌仿冒网站的页面访问量百分比

攻击者模仿合法的金融服务网站和应用程序，从而将流量成功地导向欺诈网站。他们利用网络钓鱼来持续攻击金融机构，以期获取这些企业掌握的大量敏感信息。