腾讯云边缘平台

腾讯云 2024 年
DDoS 与应用安全威胁
趋势报告

2024 年，网络安全领域面临的威胁持续演变，攻击手段更加多

样化和复杂化。基于腾讯云全网的大量数据，我们对过去一年网络攻击的趋势进行了全面分析。本文将详细阐述 2024 年主要的网络攻击趋势、攻击来源、各行业的安全形势，并基于腾讯云 EdgeOne 的防护实践提出相应的防护建议，帮助客户有效识别潜在的风险并应对这些威胁。

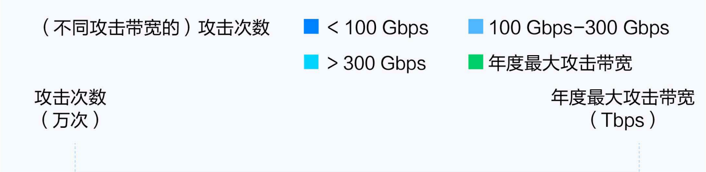
PART1

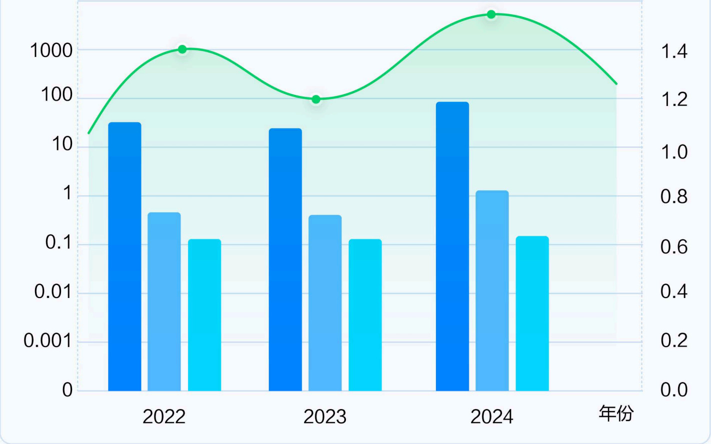
网络层（L3/L4）DDoS 攻击

攻击趋势：小规模攻击常态化，超大型攻击规模显著增加

2024 年，DDoS 攻击依旧呈现出强劲增长态势。流量型攻击次数同比增长 144%，其中小于 100 Gbps 的小规模攻击次数同比激增 146%。攻击者更倾向于通过低强度的持续攻击消耗防御资源，这种策略对防护能力较弱的企业构成了巨大的压力。同时，大于 300 Gbps 的超大型攻击次数同比增长 73%，年内流量峰值突破 1.5 Tbps，表明攻击者在提升单次攻击破坏力方面持续加大投入。

2022-2024 年度 L3/L4 DDoS 攻击规模

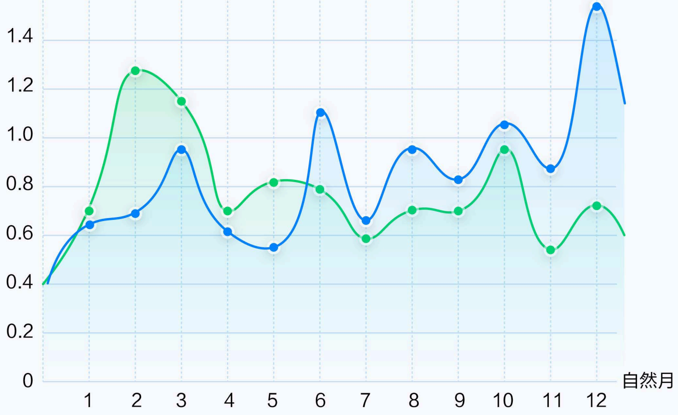




攻击高发时段：节假日成为攻击集中期

月度攻击峰值数据显示，2024 年12 月的攻击带宽规模创历史新高，同比增幅达到 115%。此外，6 月、8 月、10 月等时段的最大攻击带宽也突破了 1 Tbps ，集中在电商大促、暑期流量高峰和年末结算期等关键商业周期。这一趋势显示出攻击者越来越重视利用节假日和业务高峰期发动攻击。因此，企业在这些时期需要更加关注 DDoS 攻击的防护，确保防御能力能应对不同攻击模式。

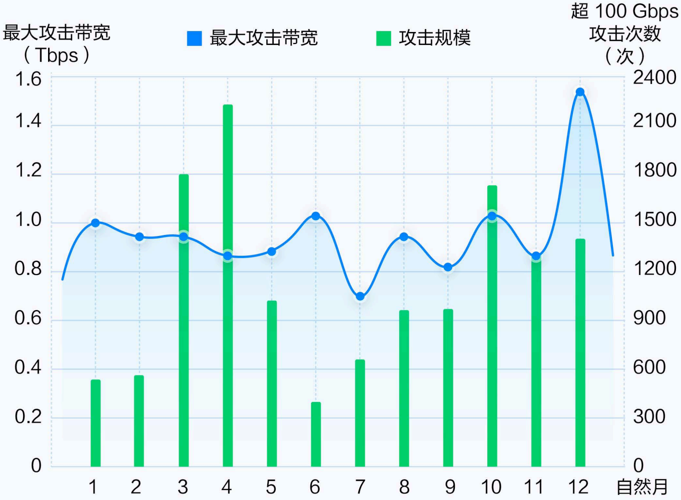
2023-2024 年自然月内最大攻击带宽



攻击呈现脉冲式密集爆发，跨区域协同攻击风险加剧

2024 年 9 月和 12 月，全球攻击流量在全球范围内呈现出“短时集中爆发”态势，攻击密度相比其余月份显著增加。局部地区业务，尤其是欧美和东南亚地区业务成为主要攻击目标，全球多地域协同攻击成为显著趋势。全球化与跨国业务应加强各区域基础设施的本地化拦截能力。

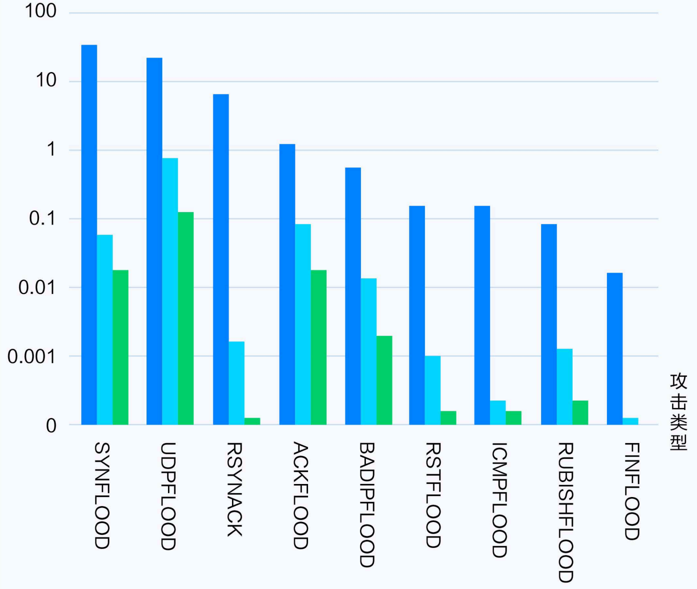
2024 年月度大规模（超 100 Gbps）L3/L4 DDoS 攻击



攻击策略：协议漏洞深度利用

在攻击类型的分布上，SYN Flood 攻击仍然占据低成本攻击的主导地位，特别是在 100 Gbps 以下的规模中占比 58% 。而 UDP Flood 则主导了中等规模的攻击，100–300 Gbps 攻击中占比 91%，大于 300 Gbps 的攻击中占比 69%。对传统协议漏洞的利用仍然是攻击的主要形态，对反射攻击的防护仍然是互联网服务应对 DDoS 防护的核心要求。

2024 年各类型 L3/L4 DDoS 攻击的攻击次数

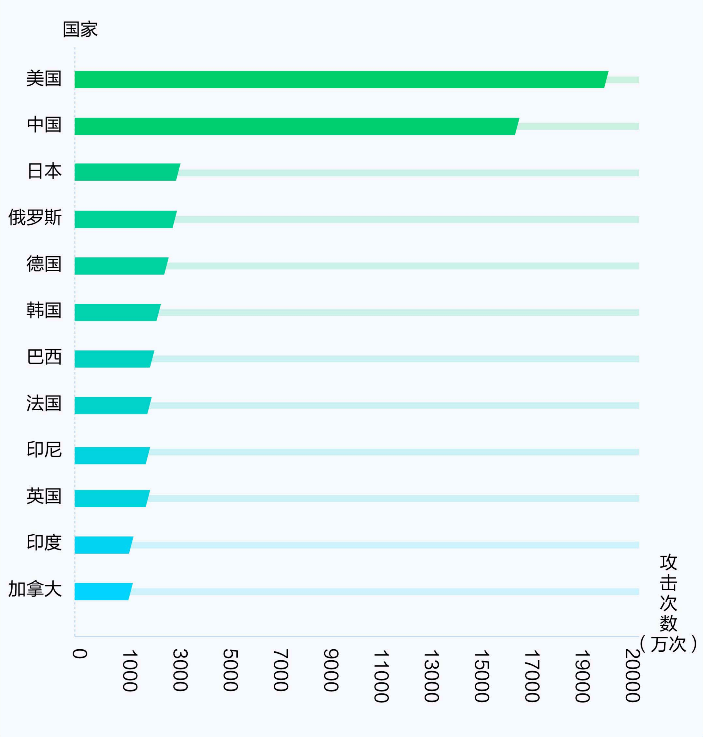


攻击源地域分析

2024 年，攻击流量主要来源于美国和中国等地区，这些地区暴露的基础设施（如未加固的反射源）常被攻击者利用，成为反射 DDoS 攻击的中转站。虽然这些地区的攻击流量较大，但并不意味着攻击行为直接来自这些地区。企业应加强基础设施防护，特别是防止常见反射协议（如 DNS、NTP 等）被滥用，采取措施关闭不必要的端口、加固服务认证，部署必要的流量过滤策略，减少互联网服务成为反射攻击源的风险。同时，对于全球范围部署的应用服

务，建议采用分布式的接入架构和防护机制，本地化处理流量，以尽可能隔离不同区域间的攻击风险。

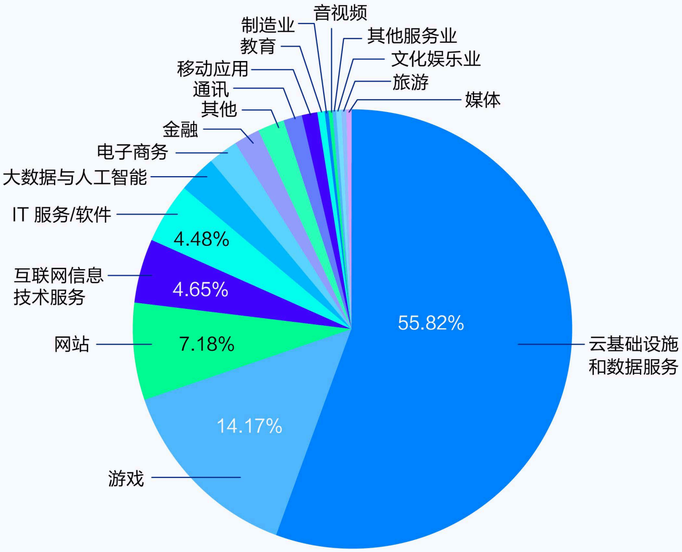
2024 年 L3/L4 DDoS 攻击流量来源 TOP 10



云基础设施和数据服务行业承受最大冲击

云基础设施和数据服务行业成为攻击的主要目标。根据最新数据显示，云基础设施和数据服务领域在各行业中被攻击的次数超 6 万次，远超其他行业。随着企业越来越多地将业务迁移到云端，云基础设施和数据服务的安全防护显得尤为重要。攻击者的目标不仅是获取敏感数据，更是通过对云基础设施和数据服务的攻击来影响企业的运营和声誉。因此，云服务提供商和用户必须加强安全防护措施，提升对潜在威胁的识别和响应能力，以应对日益严峻的网络安全形势。

2024 年 L3/L4 DDoS 攻击行业分布



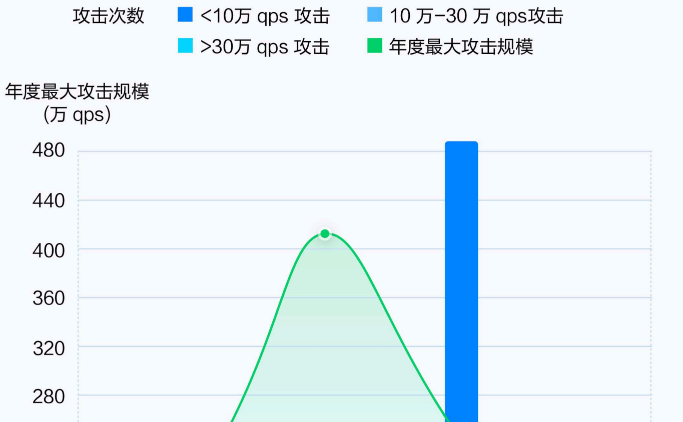
PART2

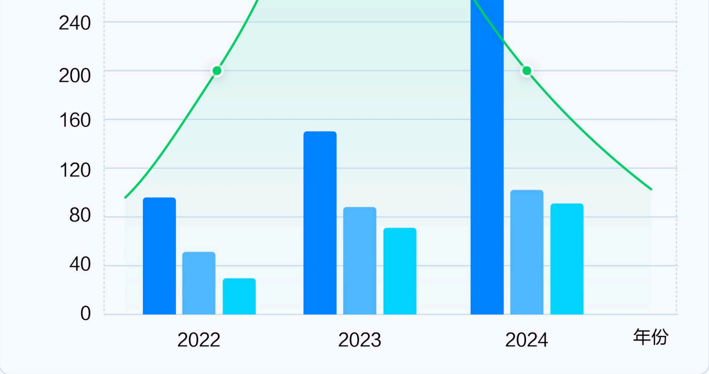
HTTP/S 攻击

HTTP/S DDoS 攻击量级爆发，超大型攻击仍处于高频状态

2024 年，HTTP/S DDoS 攻击展现出更为复杂的攻击模式。小于 10 万 QPS 的小规模 HTTP/S 攻击次数同比增长 491%；大于 30 万 QPS 的超大型攻击增长 187%，并且年度峰值突破 200 万 QPS。攻击者正在通过“海量低强度试探+间歇性高压突破”的策略，集中打击企业的应用层弱点。

2022-2024 年度 HTTP 攻击规模

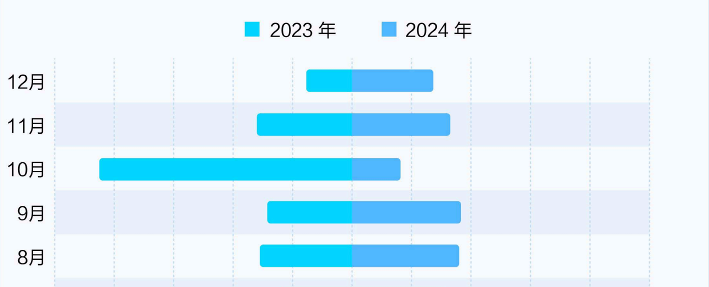


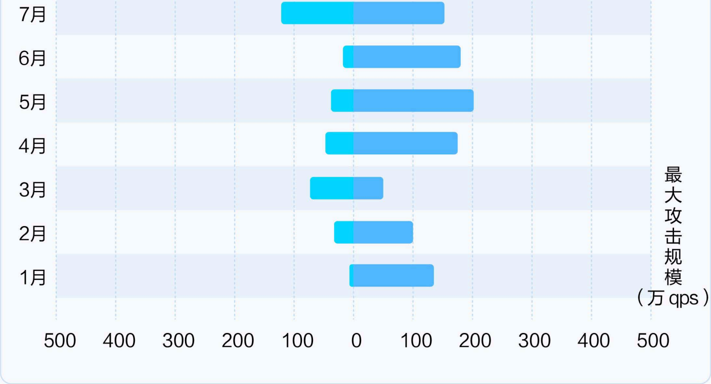


攻击高发时段：业务高峰期依旧是重灾区

2024 年，5 月、9 月和12 月成为 HTTP/S 攻击的主要高峰期，特别是在电商大促、暑期流量高峰和年末结算期，攻击者通过高频请求大量占用服务器资源，导致应用系统受到巨大压力。电商、金融等行业需要特别注意这些时间段的防护策略。

2023-2024 年自然月 HTTP/S DDoS 最大攻击规模

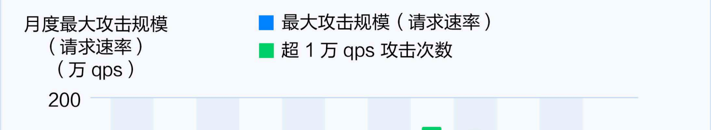


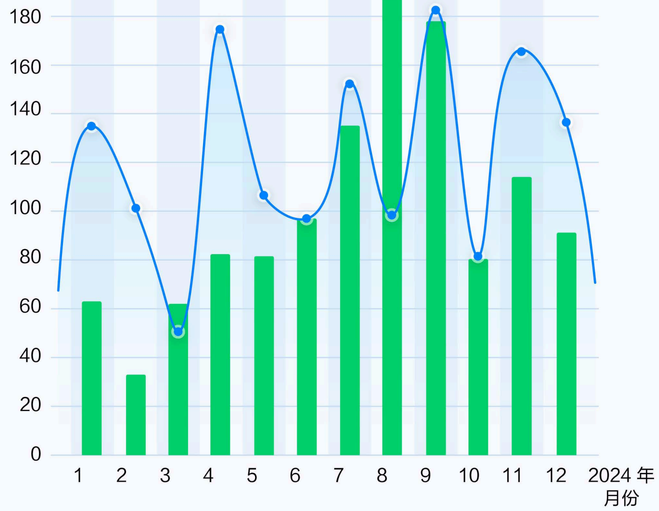


全球攻击暴增，跨域协同防护需求增强

全球 HTTP/S 攻击在 9 月出现了 254% 的增幅，欧美地区受攻击比例超过 60%。这种“跨域攻击”模式表明全球化的业务面临更加严峻的安全挑战，边缘节点的防护能力亟待提升。

2024 年 HTTP/S DDoS 月度攻击规模





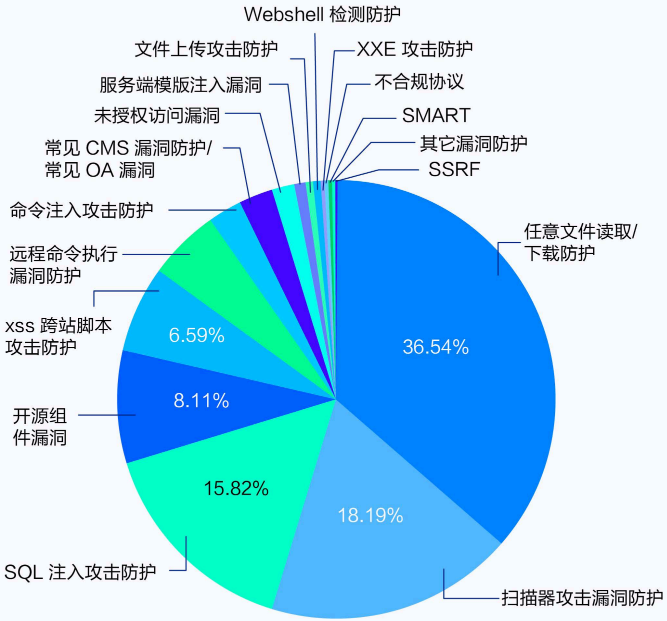
PART3

利用漏洞和应用弱点的攻击

任意文件读取漏洞和漏洞扫描器仍是最大威胁

2024 年，漏洞利用攻击依旧呈现出高发趋势，高危的漏洞攻击总量超过 17 亿次，其中任意文件读取/下载漏洞占比 36.5%，远超 SQL 注入和扫描器攻击等传统攻击类型。攻击者越来越倾向于通过配置错误、权限漏洞等“低技术门槛”的攻击向量进行漏洞扫描，并尝试渗透，企业需要加强权限管控和目录访问控制，防止敏感数据泄露。

利用 Web 服务弱点或漏洞的攻击类型



PART4

新威胁趋势：流量盗刷攻击

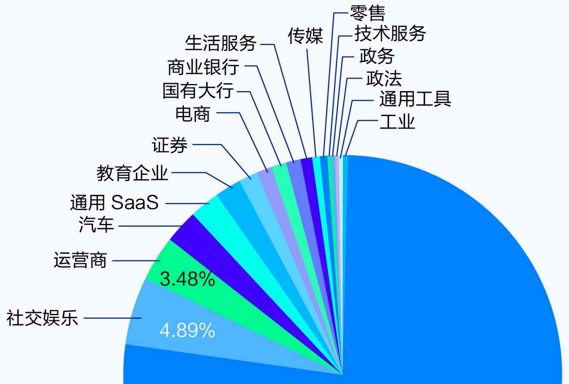
2024 年，下载流量盗刷攻击成为新的安全威胁趋势，尤其在电商、云存储和在线流媒体等行业中。EdgeOne 能够帮助企业有效应对流量盗刷攻击，

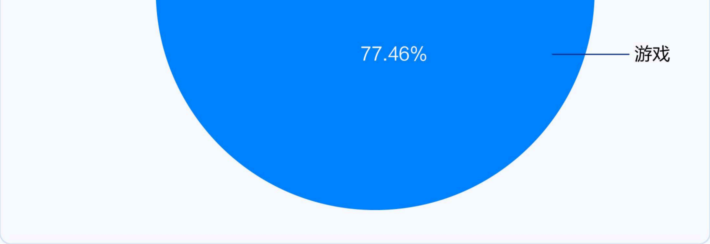
这类攻击通过恶意脚本或模拟用户行为，频繁发起虚假下载请求，消耗带宽资源，导致正常用户无法访问或平台性能下降。攻击者利用平台资源造成经济损失或业务中断，给企业带来严重威胁。

单季度流量盗刷规模突破 2 PB，游戏行业占比超 70%

2024 年 9 月至 12 月，流量盗刷攻击的规模超过 2 PB（含拦截后，未产生的盗刷流量）。其中游戏行业占比达 77%。第四季度盗刷流量较上季度环比增长 134%。攻击者通过反复下载游戏更新包、图片等静态资源，产生巨额流量账单，严重影响企业的带宽成本和系统资源。尤其是在游戏行业，由于游戏安装和更新包文件普遍较大，成为了流量盗刷的主要目标。EdgeOne 为全平台业务免费提供流量防盗刷功能，大幅降低了企业被盗刷的经济损失。

2024 年遭受流量盗刷攻击的业务（行业分布）

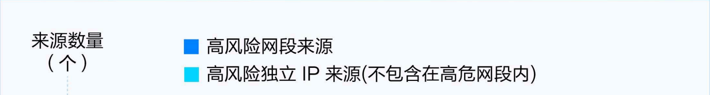


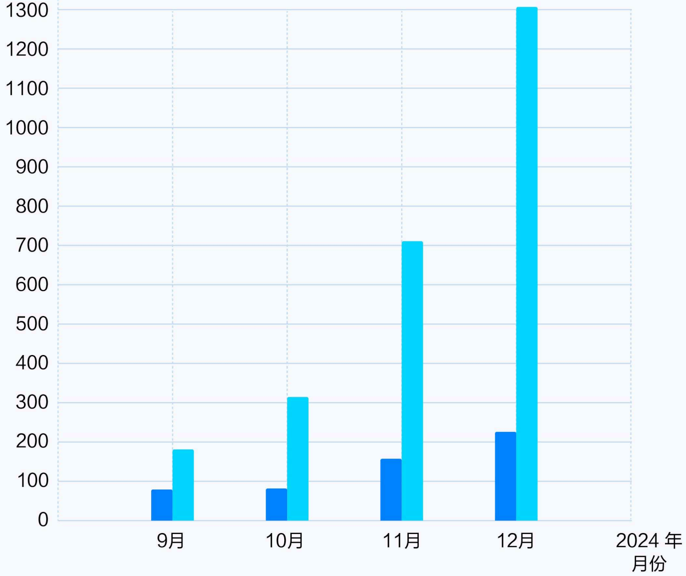


流量盗刷攻击 IP 溯源难度加剧，单季度涉及 IP 超 4.7 万

2024 年第四季度，流量盗刷攻击涉及 IP 数超过 4.7 万个，较 9 月增长 367%。其中，87% 的攻击流量来源的归属网段较分散，表明攻击者通过分布式、低强度的方式进行盗刷，以规避检测。传统的 IP 黑名单机制已难以应对这种复杂的攻击模式。为提升防护效果，企业需要结合设备指纹、用户行为分析等多维度的风控手段，精准识别异常流量并加强防范。EdgeOne 通过全平台情报库对盗刷来源和盗刷客户端指纹进行全平台自动化识别拦截，有效保护企业和个人站点的静态内容。

2024 第四季度流量盗刷攻击趋势





PART5

应用层 HTTPS 攻击案例

某直播服务平台提供全球直播业务，用户通过多个终端（如小程序、APP、Web 等）进行访问。2024 年，该平台遭遇了一次大规模的应用层 DDoS 攻击，此次攻击采用了复杂的手段，攻击者投入大量资源，并实施了多种高隐蔽性的攻击方式：

攻击来自真实的 Bot 网络，具备 JavaScript 执行能力，能够绕过基本的 JavaScript 挑战机制

攻击的并发请求速率非常高，且攻击来源分布广泛

攻击者定制与业务终端非常相似的客户端，并伪造类似的 JA3 指纹

使用新型的 HTTP 2 协议漏洞，持续发起攻击，消耗平台资源

此类应用层攻击结合了多种威胁机制，攻击者不仅深度定制了客户端和请求，还通过 Bot 网络发起大规模分布式攻击，降低了单个客户端的请求频率。由于传统的 IP 限频和头部特征过滤无法有效识别和区分此类攻击，新型混合型攻击对企业防护体系构成了新的挑战。

预计未来 1–2 年，这类攻击将逐步增多。我们建议互联网服务，特别是金融、游戏、电商、零售和互联网 SaaS 服务，提升安全防护基线，以应对这一新的威胁趋势：

使用防护资源更为充足的分布式边缘安全机制（如：腾讯云 EdgeOne），以应对更大规模的 DDoS 攻击

将安全解决方案部署在网络最外围，以更好地应用新型的 TLS 指纹、客户端指纹技术，高效识别攻击来源

基于多项统计指标的限频机制，以缓解整体可用性风险

建立正向防护机制，分析非攻击期客户端指纹和请求特征，并动态加白，建立安全信任基线

使用聚类分析策略，对 TLS 指纹和 HTTP 头部等指标进行聚合分析，提升防护效率

腾讯云 EdgeOne 凭借强大的防护能力，帮助全球企业应对多种复杂的网络安全威胁，保障互联网服务的安全性。

腾讯安全、腾讯云 EdgeOne 团队联合制作