2025 年 DDoS 威胁图景：自动化全面掌舵之年

如果您脑海中对 DDoS（分布式拒绝服务）攻击的印象仍停留在那种“持续时间长、动静大、能给团队留出反应时间”的流量洪水，那么 2025 年的现实将彻底打破这一认知。在过去的 12 个月里，我们目睹了 DDoS 攻击从“单纯追求大流量”向一种更令人不安的模式转变：**自动化、多阶段的攻击活动。**它们会主动探测你的防线，实时调整策略，并在任何人加入应急响应会议（Bridge Call）之前便已撤离。

核心信息非常简单：**速度已成为武器。**根据我们的最新数据，78%的攻击在 5 分钟内结束，37%的攻击甚至在 2 分钟内就已停止。这就是为什么网络运营面临一个残酷的真相：如果你的 DDoS 防御系统不能在一分钟内于网络边缘完成检测与缓解，你将错过绝大多数的现代攻击。

以下是定义 2025 年的 DDoS 趋势，以及它们对网络运营商意味着什么。

趋势 1：短时、高冲击力攻击

2025 年，攻击者以攻击时长换取了攻击强度。DDoS 变成了“快准狠”的突袭，且几乎没有任何预警。与此同时，攻击流量的上限不仅在抬升，而且在加速。2025 年 9 月，我们观测到了首个超过 **10 Tbps** 的攻击；随后是 **22 Tbps**；到 10 月，这一记录被刷新至 **33 Tbps**。短短六周内，三项记录被打破。

太比特（Terabit）级的攻击不再是里程碑，而是基准线。

这改变了衡量防御准备度的方式。仅仅询问“我们能否处理 DDoS 峰值？”是不够的，你还必须问：“我们能否全天候、重复性地在数秒内做出反应？”

趋势 2：多目标与多向量成为默认配置

2025 年的 DDoS 攻击不再局限于填满单一链路，而是倾向于“全方位施压”。我们发现 **52% 的攻击同时针对多个主机**（通常被称为“地毯式轰炸”），且 **58% 的攻击结合了两种或更多攻击向量。**

更值得关注的是，攻击者不仅是“选择”多个向量，而是将其“序列化”。在我们的 DDoS 库中，2025 年的一个典型样本显示：攻击者在三分钟内执行了四种截然不同的攻击——TCP 地毯式轰炸、UDP 洪水、DNS 放大以及高频率 SYN 洪水。每当防御方做出响应后，攻击便立即调整，并在每一步都增加带宽。

这绝非乱打乱撞，而是**侦察式攻击。**

趋势 3：住宅代理网络成为 DDoS 基础设施

我们记录到的最重要转变之一是攻击流量源的变化。

住宅代理网络（Residential Proxy Networks）——曾经主要与小型诈骗活动挂钩——现已成为主流基础设施风险。据估计，全球有 **1 亿至 2 亿个 IPv4 终端** 正在隐秘地转发来自日常消费级设备的流量。地理分布也极具规模：约四分之一在巴西，美国则拥有超过 1000 万个节点。

这种看似杂乱的地下市场其实高度集中。我们的研究表明，**单一批发商可能控制着全球约 70%的此类 IP 地址池。**其规模令人震惊：全球总容量现已超过 **250 Tbps**，足以让许多国家级的骨干网承压。

我们还记录到一种可重复的“两阶段”模式：受控 IP 最初充当“干净”的代理出口，一旦其信誉度下降，便立即转变为执行超大规模流量 DDoS 的角色。在巴西和中国等热点地区，住宅代理贡献了约 10%的观测流量。

对于防御者来说，这打破了原有模型。你无法通过防火墙屏蔽家庭流量，因为这些流量在技术层面是“合法的”——它们只是恰好在执行攻击。这模糊了“好”与“坏”流量的界限。

趋势 4：IoT 僵尸网络带着超大规模攻击回归

IoT（物联网）僵尸网络并未消失，而是进化了。

我们追踪到了 Mirai 家族的新一代变种，包括 **Eleven11bot/RapperBot** 和 **Aisuru**，它们瞄准了人们家中和办公室里常见的设备（如 DVR、摄像头和网关设备）。诺基亚 Deepfield 应急响应团队（ERT）于 2025 年 2 月下旬首次观测到该活动，涉及超过 **3 万台** 受损的 IoT 设备。

这些攻击不是缓慢增长的。遥测数据显示，其具备 **30 Tbps** 的体积容量，数据包强度峰值接近 **15 Gpps**，且**从发动到峰值仅需 1-3 分钟**。

令人沮丧的是，这种情况持续发生的原因显而易见：碎片化的 IoT 供应链导致漏洞无人修复，且更新机制常被悄悄禁用以降低支持成本。设备出厂即不安全，且终身不安全。一旦某个僵尸网络被拆除，其他势力会迅速填补真空。2025 年 8 月某大型僵尸网络被取缔后，我们发现相关设备在数日内便被吸纳进新网络并参与攻击。

趋势 5：DDoS 编排实现算法化

2025 年最本质的变化是：**人为编排让位给了算法自动化。**攻击者现在使用的系统能够持续监测防御方的响应时间和阈值，系统性地切换向量，在防御手段激活时自动升级，甚至重新排队僵尸流量以寻找覆盖漏洞。

其含义明确且令人不安：**防御也必须以算法速度运行**，否则攻击者将始终占据优势。

趋势 6：黑客行动主义——低技术依然有效

并非所有的破坏性 DDoS 都很先进。“Eastwood 行动”案例研究表明，技术水平极低的群体——利用租借服务器上的剪贴脚本、通过免费 VPN 隧道——依然能通过攻击资源匮乏、控制薄弱的网站制造头条新闻。

这是一个提醒：韧性不仅是“一级（Tier 1）”目标的需求，最薄弱的公共服务往往定义了你的公众声誉。

2025 年给 DDoS 安全团队的启示

来自真实运营商的数据揭示了实际情况。例如，Bite Latvija 报告称探测并拦截了近 4000 次 DDoS 企图（2024 年数据），峰值达 280 Gbps，平均持续时间不足 15 分钟，其中 69%为多向量攻击。从全球来看，许多流量洪水在带宽上并不巨大——82%低于 50 Gbps——但由于节奏极快，它们依然具有破坏性。