快快网络 | 新一代云安全引领者

快快网络2024年 DDoS攻击趋势白皮书

摘要

就分布式拒绝服务（DDoS）攻击趋势而言，2023 年是具有里程碑意义的一年。网络犯罪集团、出于地缘政治动机的黑客活动分子和恶意行为者利用物联网（IoT）设备构建的大规模僵尸网络以及协议级零日漏洞，对企业、政府机构以及关键但脆弱的公共基础设施（包括医院）发起了破纪录的 DDoS 攻击。

在整个 2023 年，DDoS 攻击变得更加频繁、持续时间更长、复杂程度更高。其中，银行和金融服务行业是最具针对性的垂直行业。针对这些行业的攻击通常旨在造成声誉损害，或分散安全专业人员的注意力，以发动 DDoS+勒索软件混合攻击。DDoS 攻击事件愈演愈烈，成为互联网最大的网络安全威胁之一，让企业面临的网络安全风险与日俱增。

通过快快网络 DDoS 团队检测数据显示：2023 年中国遭受 DDoS 攻击次数达 146 万，占全球 11.74%，游戏行业仍然是受影响最严重的行业，遭受了 46% 的攻击。金融行业位居第二，占 22%。电信（18%）、基础设施服务行业（7%）和计算机软件公司（3%）也成为重点目标。

快快网络带来了 2024 年 DDoS 全球攻击趋势专项报告，与您分享 DDoS 攻防态势的最新趋势。

CONTENTS 目录

01

2023年全球DDoS攻击情况

1. 2023 年全球 DDoS 攻击情况

1.1 全球攻击情况

2023 年 DDoS 攻击总次数 1246.61 万次，同比增长 18.1%。

快快网络监测数据显示，2023 年中国遭受 DDoS 攻击次数达 146 万，占全球 11.74%，排名第三，第一为美国占比 41.22%，第二为荷兰。在欧洲、中东、非洲（EMEA）和亚太（APAC）地区，DDoS 攻击的数量和规模已经与北美不相上下。

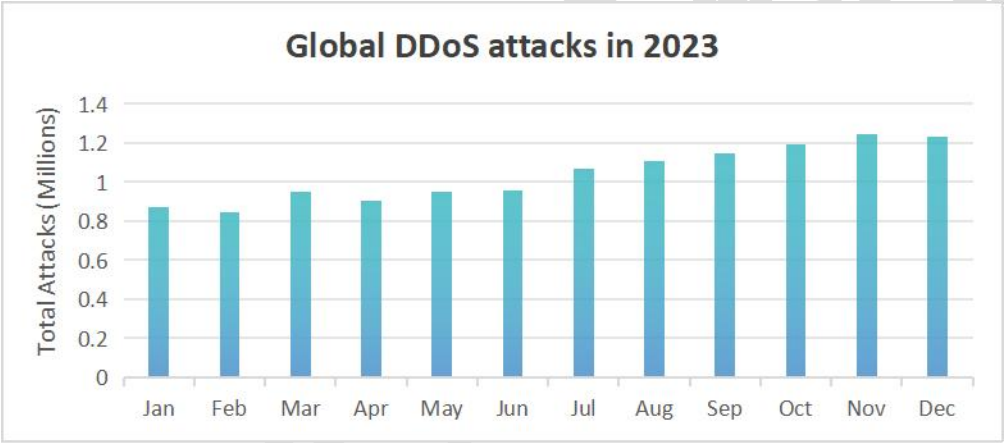

图 1 2023 年全球 DDoS 攻击情况

数据显示，攻击者越来越多地瞄准关键基础设施和服务，包括物流服务、支付处理中心和银行系统，试图影响更多的用户。平均攻击强度达到 1.4Tbps 的峰值，最长的攻击持续了 7 天。

越来越多的 DDoS 攻击开始使用僵尸网络，超过 38%的 DDoS 攻击利用了感染僵尸网络的设备。此外，与上一年相比，作为多向量攻击的烟幕弹/诱饵的 DDoS 攻击增加了 28%。

更具破坏性的 HTTP 攻击正变得越来越容易实施。82.3%的 DDoS 攻击针对 OSI 模型的应用层（L7），11.7%针对 OSI 模型的传输（L4）和网络（L3）层。2.3%的攻击针对 DNS，其余 3.7%针对其他目标。

1.2 攻击规模

DDoS 攻击的规模和复杂程度都在不断增长，但 2023 年以不可预见的速度加速了这一趋势。甚至连安全供应商及其各自的网站也受到了攻击。2023 年 7 月，出现高达 1990 Gbps（1.99 Tbps）和 710 Mpps 的超大规模 DDoS 攻击。9 月份，快快网络发现并阻止了一场大规模 DDoS 攻击。在这起攻击中，网络犯罪分子使用了 ACK、PUSH、RESET 和 SYN 洪水攻击向量的组合，峰值为 1.6 Tbps。事实证明，这些攻击与 2022 年开始的“震慑式”DDoS 攻击趋势非常一致。

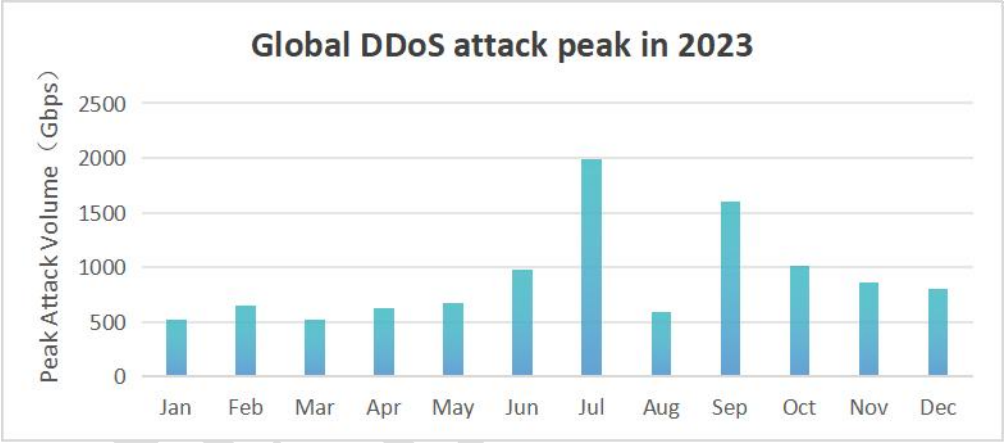

图 2 2023 年全球 DDoS 攻击峰值

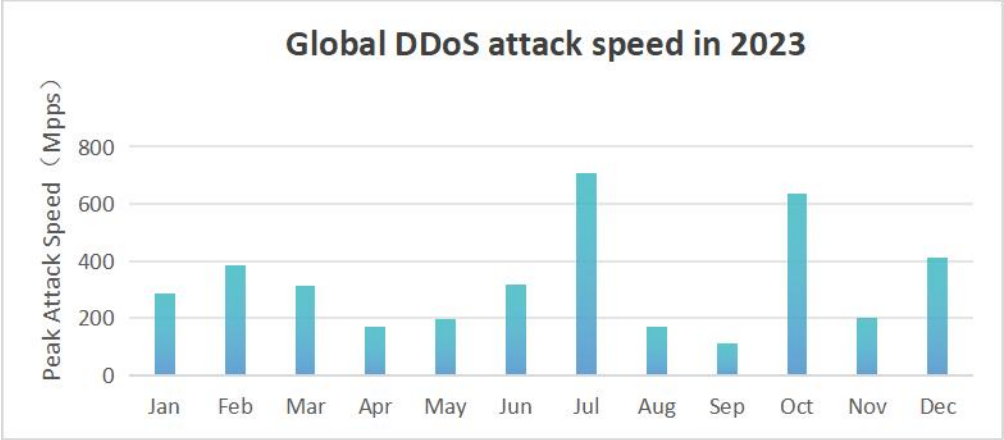

图 3 2023 年全球 DDoS 攻击速度

2023 年，快快网络就曾检测到一起创纪录的 DDoS 攻击，其最

高攻击速度为 704.8 Mpps。快快网络缓解的 10 次最大 DDoS 攻击中有 8 次都发生在过去 18 个月内。

1.3 攻击类型

在主要攻击类型中，UDP flood 继续占据主导地位，占 DDoS 攻击的 62%。TCP flood 和 ICMP 攻击也仍然很流行，分别占总数的 16% 和 12%。所有其他 DDoS 攻击类型，包括 SYN、SYN+ACK Flood 和 RST Flood，合计仅占 10%。虽然一些攻击者可能会使用这些更复杂的方法，但大多数攻击者仍然专注于提供大量数据包来摧毁服务器。

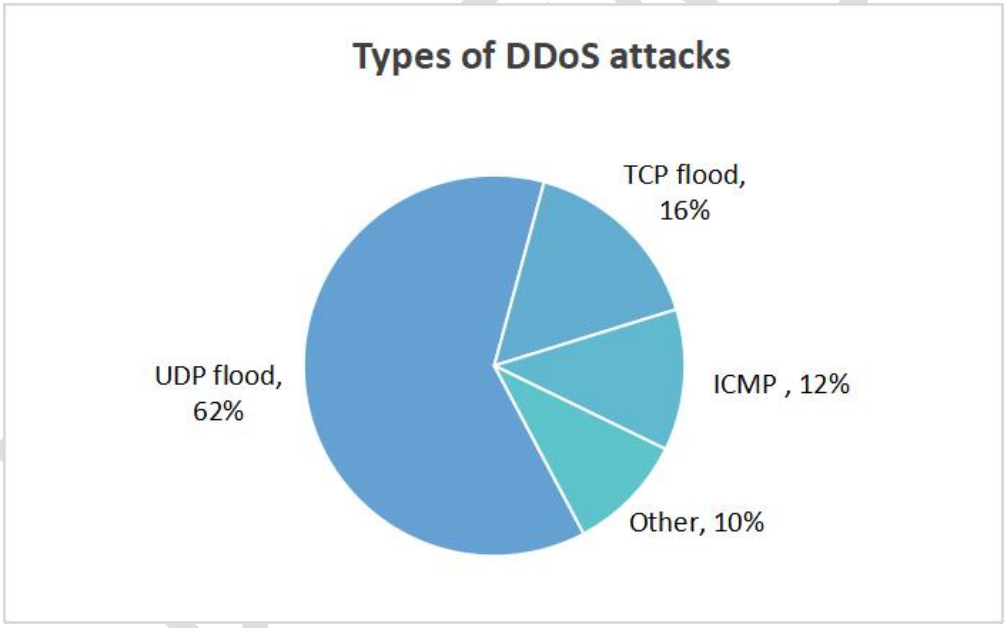

图 4 DDoS 攻击类型

1.4 攻击源分布

攻击源的全球传播表明了网络威胁的无国界性质，攻击者可以跨越国界进行操作。其中美国位居第一，占 53.4%。德国（26%）、英国（25.8%）、荷兰（24.8%）、法国（23.9%）位列前 5。

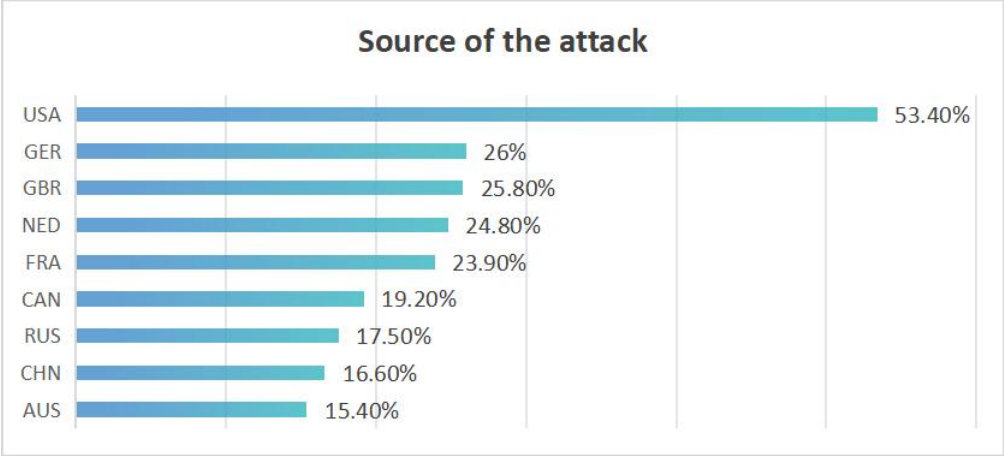

图 5 攻击源地理位置占比

DDoS 攻击源的地理分布为制定有针对性的防御策略，以及制定旨在打击网络犯罪的国际政策提供了重要信息。然而，由于使用 IP 欺骗等技术以及分布式僵尸网络的参与，确定攻击者的真实位置具有一定难度。

1.5 目标行业

与 2022 年游戏行业占据第一不同的是，2023 年，金融机构经历了近 30%的攻击活动，排在第一。但互联网依然是 DDoS 攻击的重灾区，占所有 DDoS 攻击的 22.2%。其他成为 DDoS 攻击目标的行业包括医疗保健(14.2%)、政府(11.5%)、运输和物流(8.64%)以及游戏(3.09%)。

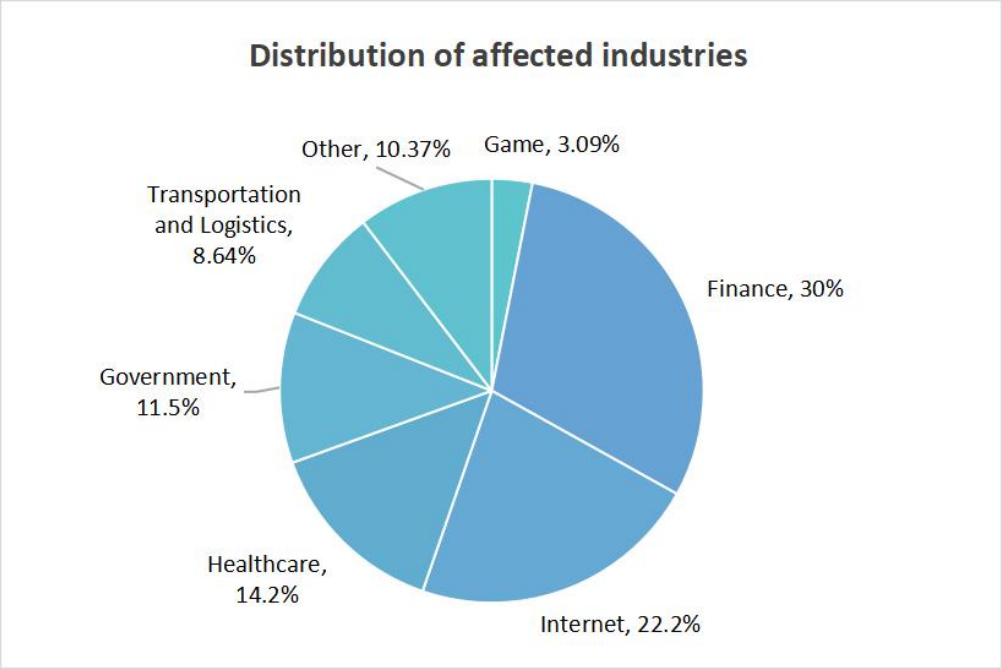

图 6 受影响行业占比分布

02

2023年国内DDoS攻击情况

2. 2023 年国内 DDoS 攻击情况

2.1 国内攻击情况

2023 年，攻击频次逐年增长，大流量攻击频次保持高位，2023 年全年 DDoS 攻击次数同比 2021 年增长 80%，以关键信息基础设施为目标的高烈度 DDoS 攻击已跃升成为国家级网络安全威胁之首。

图 7 国内攻击情况

2.2 攻击目标地域分布

密集型扫段攻击导致攻击目标地域发生聚集。2023 年中国遭受 DDoS 攻击最多的地域为浙江，占全国 33.17%，其次为广东、湖南、江苏、福建、山东、湖北、河南、陕西、四川。

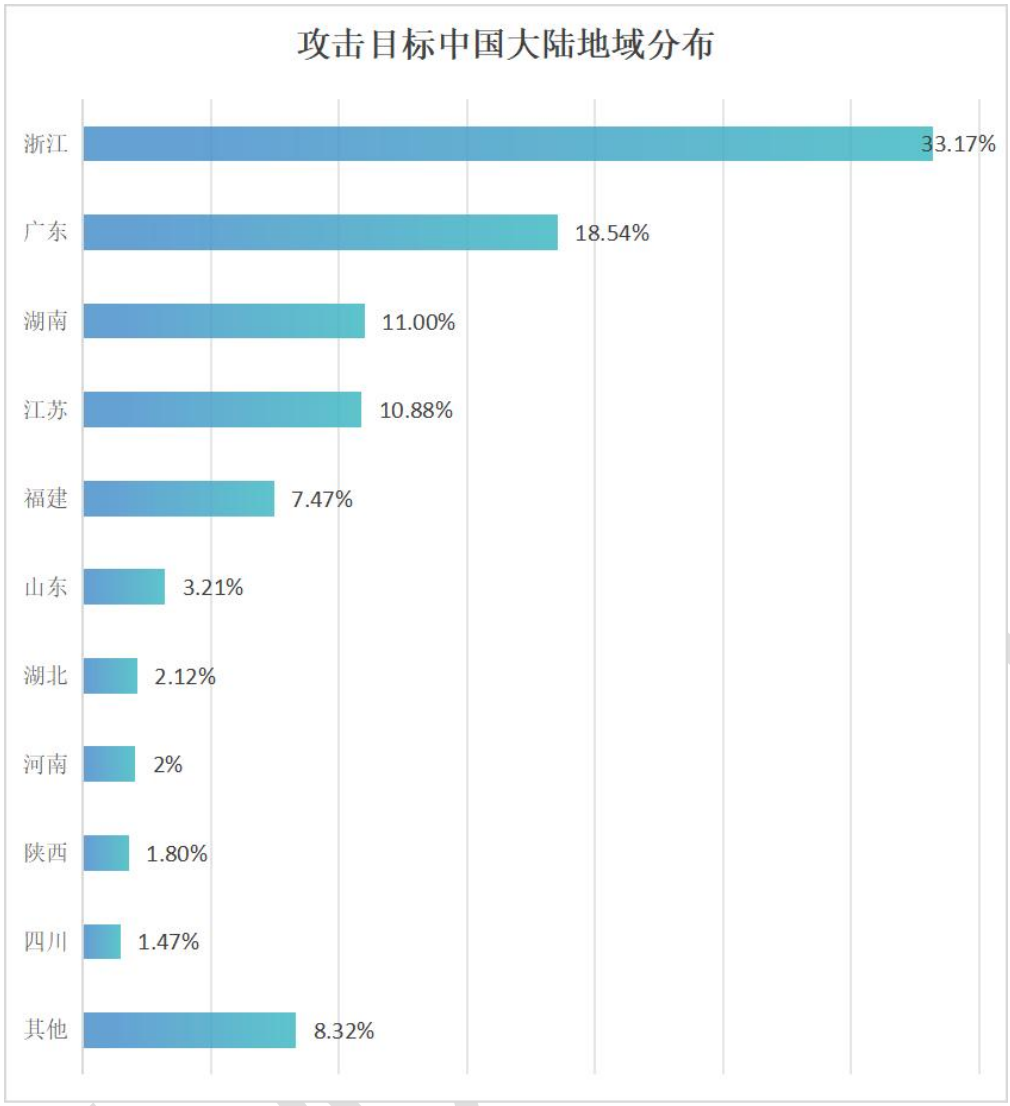

图 8 攻击目标中国大陆地域分布

2.3 瞬时攻击速度攀升

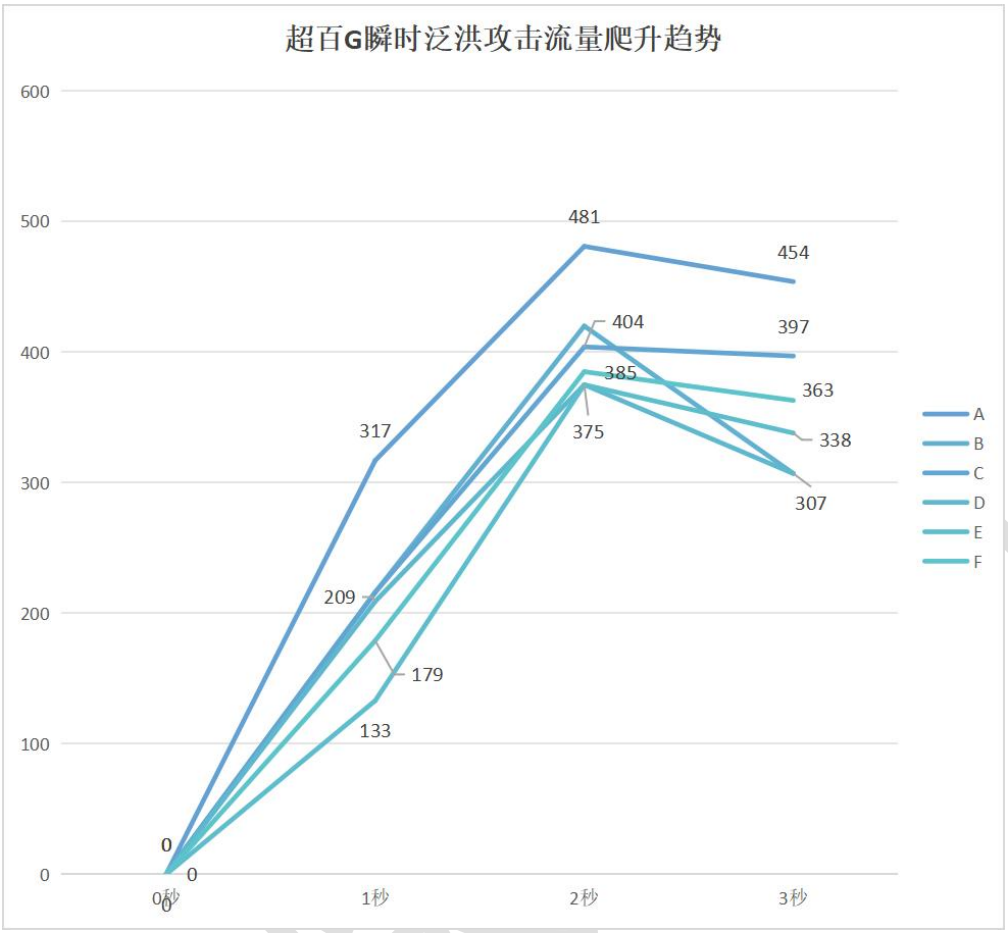

图 9 超百 G 瞬时泛洪攻击流量爬升

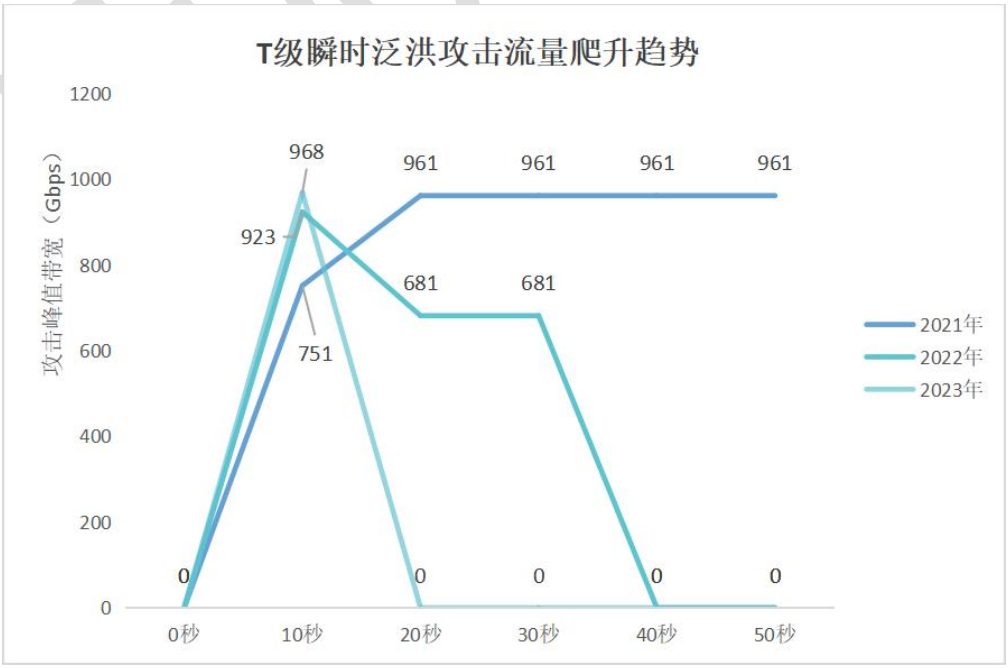

图 10 T 级瞬时泛洪攻击流量爬升趋势

2023 年，从攻击时长来看，短时攻击依然常见。86%的攻击持续时间不到 1 小时，1-2 分钟的攻击占全年攻击的 23.44%。攻击者倾向于在短时间内，以极大的流量导致目标服务用户掉线、延时和抖动。从瞬时泛洪攻击速度来看，近几年瞬时泛洪攻击爬升速度持续攀升。瞬时泛洪攻击 2 秒流量即可爬升至近 500G，10 秒即可爬升至 T 级，大流量攻击爬升速度再创新高，挑战防御系统响应速度。

2.4 扫段攻击

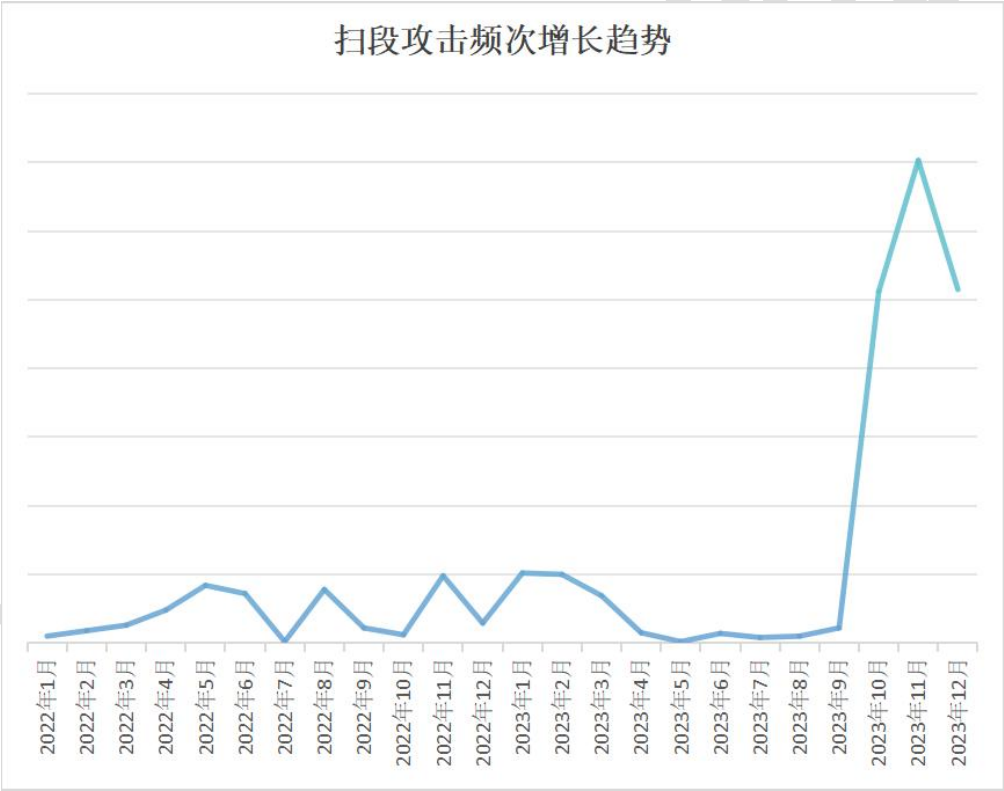

图 11 扫段攻击频次快速增长

2023 年 H2 扫段攻击频次激增，攻击手法持续演进，成为网络基础设施最大威胁。

从扫段速率来看，低速扫段占比 73.91%，低速扫段单 IP 流量低，挑战传统检测算法有效性；单个 C 段攻击持续时间占比中，扫段攻击多采用“短平快”战术<5 分钟的攻击占比 43.26%，挑战防御

系统响应速度；扫段攻击手法中，86.96%的扫段攻击采用混合攻击手法，防御困难；从扫段攻击类型分布来看，反射攻击提升带宽拥塞威胁，虚假源泛洪攻击加大防御难度。

扫段攻击因威胁范围广，扫段攻击的频次、复杂度持续攀升，攻击者惯用“短平快”战术，导致检测难、引流难、防御难、防御成本高，已成为攻击网络基础设施的惯用手段。

03

快快网络DDoS态势观察

3. 快快网络 DDoS 态势观察

通过分析快快网络所保护的各个行业和地区的客户所经历的多个威胁检测，整体 DDoS 威胁呈上升趋势，且增长惊人。

3.1 攻击情况

2023 年，快快网络共计成功防护 58.4 万起 DDoS 网络攻击，同比增长 151.7%。1 月-3 月 DDoS 网络攻击次数较低，6 月份、8 月份攻击次数最多，占全年 22.7%。

2023 年，攻击流量峰值 Q1-Q2 季度增至 800 Gbps，2023 年 Q3-Q4 季度增至 1600 Gbps（1.6 Tbps），越来越多的 DDoS 攻击开始使用僵尸网络，超过 38%的 DDoS 攻击利用了感染僵尸网络的设备。此外，与上一年相比，作为多向量攻击的烟幕弹/诱饵的 DDoS 攻击增加了 28%。

图 12 快快网络 2023 年攻击流量峰值

3.2 攻击类型

UDP 是迄今为止在大流量 DDoS 攻击中利用最多的协议。由于其无状态特性，UDP 允许合法服务被滥用，通过反射和放大攻击向受害者发送大量未经请求的流量。TCP SYN 和状态外数据包也被用于

大容量攻击，但 TCP 协议通常作用是旨在耗尽设备和服务器上资源的攻击。

在流量攻击中，使用最多的攻击向量是 UDP fragment flood(43%)，其次是 UDP flood(19.2%)和 TCP flood(14.4%)。

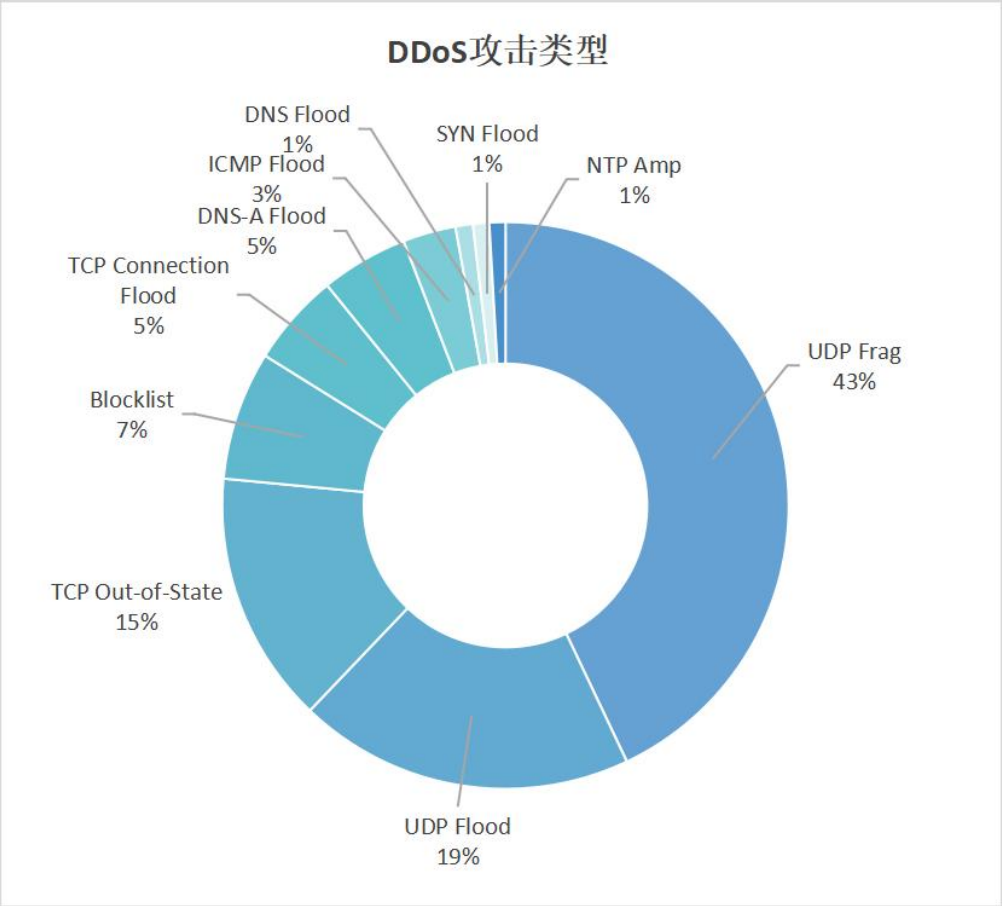

图 13 DDoS 攻击类型

3.3 攻击来源

攻击源的全球传播表明了网络威胁的无国界性质，攻击者可以跨越国界进行操作。其中美国位居第一，占 24%。印度尼西亚（17%）、荷兰（12%）、泰国（10%）、哥伦比亚（8%）、俄罗斯（8%）、乌克兰（5%）、墨西哥（3%）、德国（2%）和巴西（2%）位列前十，这说明全球面临着广泛的威胁。

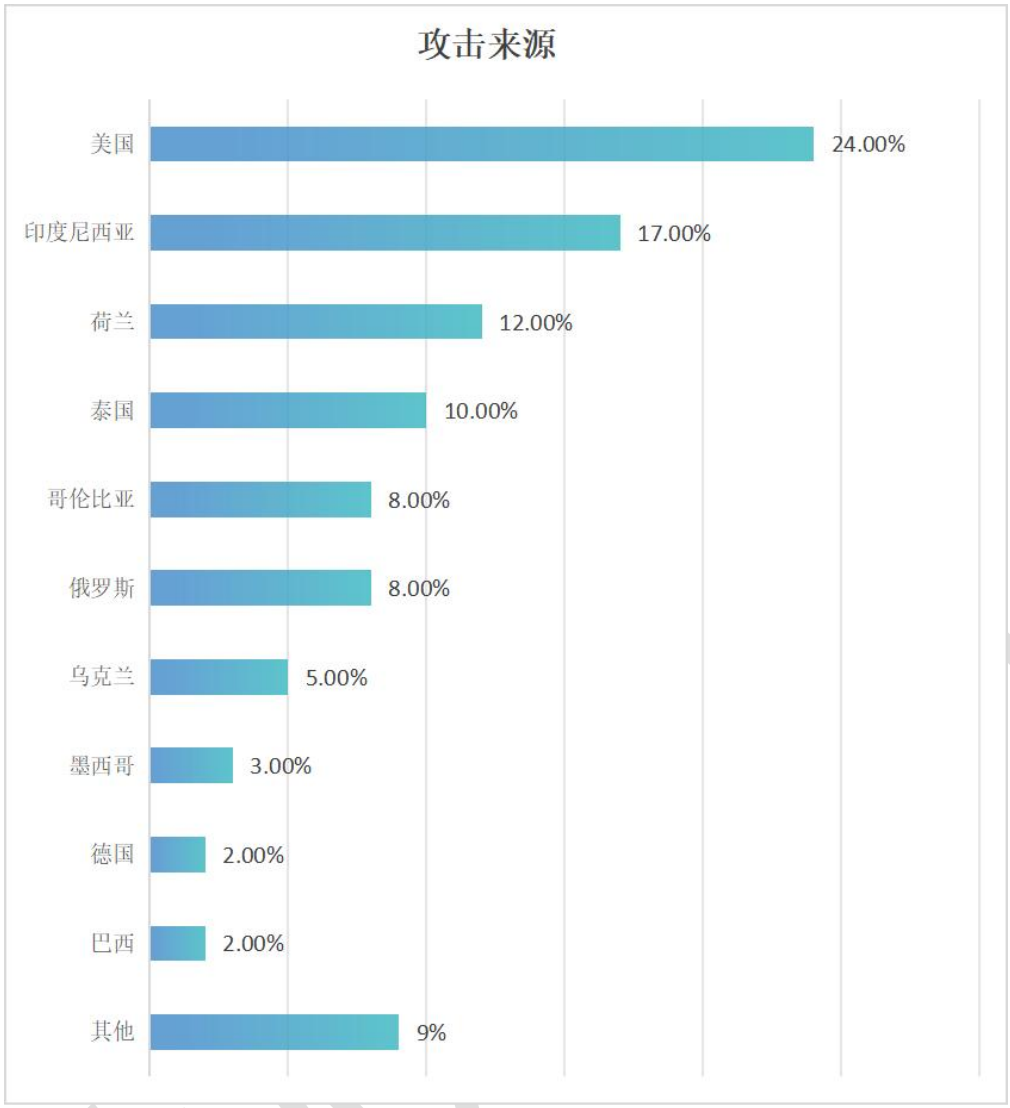

图 14 攻击来源

DDoS 攻击源的地理分布为制定有针对性的防御策略，以及制定旨在打击网络犯罪的国际政策提供了重要信息。然而，由于使用 IP 欺骗等技术以及分布式僵尸网络的参与，确定攻击者的真实位置具有一定难度。

3.4 攻击行业

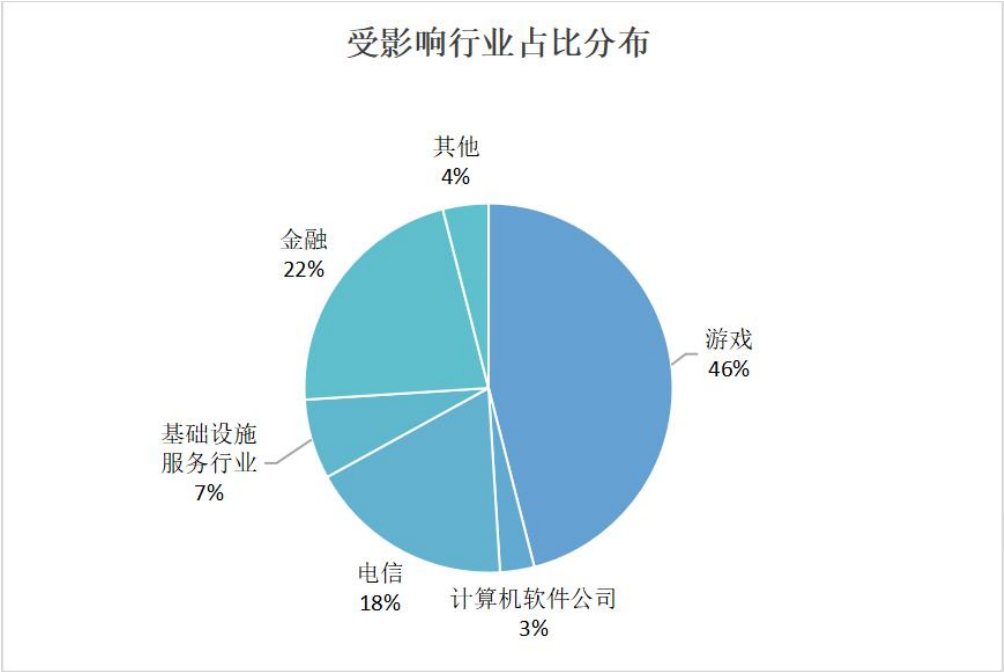

图 15 受影响行业占比分布

游戏行业仍然是受影响最严重的行业，遭受了 46% 的攻击。金融行业位居第二，占 22%。电信（18%）、基础设施服务行业（7%）和计算机软件公司（3%）也成为重点目标。

攻击者对游戏和金融领域特别感兴趣，这些行业一般具有较好的经济收益和用户基础，同时凸显了在受打击最严重的行业中需要有针对性网络安全策略的必要性。

04

典型攻防对抗案例

4. 典型攻防对抗案例

4.1 接口攻防案例

快快网络安全团队接到某数藏平台应急响应请求，平台存在流量访问异常，用户无法登录或无法在平台进行购买下单操作现象，导致客户资产流失和声誉受损。

防护难度：

该平台遭受有组织、有预谋的 DDoS 攻击，攻击目标主要是平台的 API 接口，支付接口等，攻击者通过 SYN Flood、ACK Flood、CC 等多种类型攻击技术手段不断变换攻击形式。

针对以上情况，快快网络提供以下解决方案：

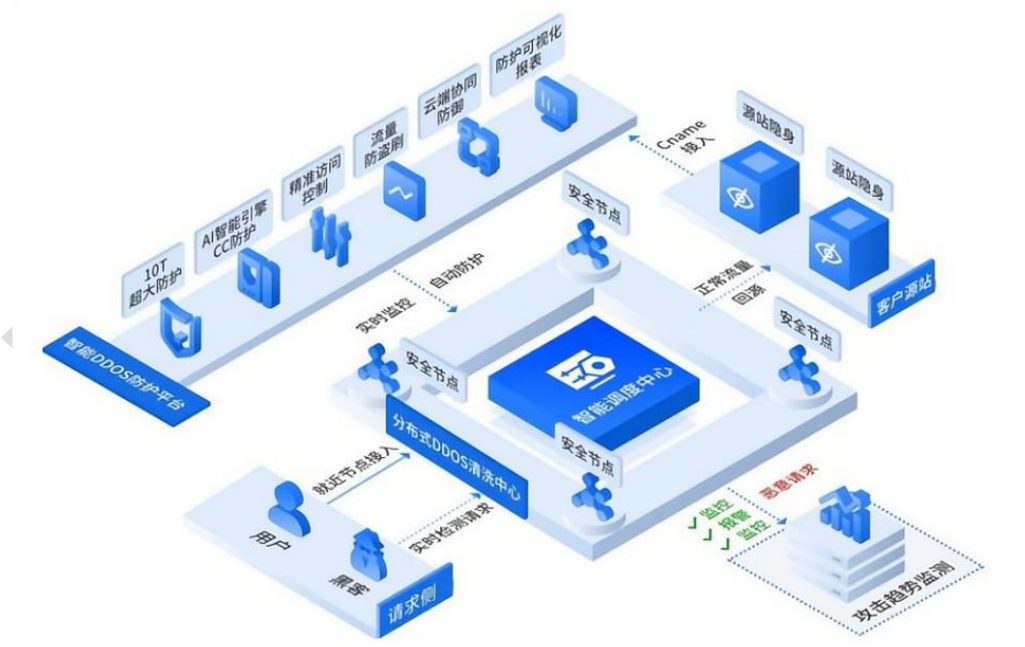

图 16 DDoS 安全防护架构部署图

1、建立完善的监测预警机制，部署使用快快网络 DDoS 安全防护产品。结合快快网络自研 ADS 系统，加持机器学习及特征处置联动能力，扩大攻击可能性的捕捉范围，实时检测阻断各类 DDoS 攻击，

并启动应急预案及时对攻击行为进行防护，为客户成功抵御 125G 的 DDoS 攻击及百万级 CC 攻击。

2、快快网络安全专家与该公司深度沟通配合和优化。定制 CC 防护策略与智能防刷策略，实时检测并拦截攻击，终端用户无感知。

4.2 大流量攻防案例

某知名游戏公司在其运营期间遭受了大型 DDoS 流量攻击，导致游戏玩家在游玩过程中频繁遇到掉线、延迟、卡顿等问题，网络波动严重，严重影响了玩家的游戏体验。不仅如此，长时间的网络不稳定还可能导致玩家数据丢失、账号被盗等更严重的后果。

防护难度：

DDoS 流量攻击规模高达 1.6T，攻击者使用了 ACK、PUSH、RESET 和 SYN 洪水攻击向量的组合。面对如此大规模复杂攻击时，快快网络安全团队快速响应，为其定制相应的 DDoS 防护解决方案，提供全方位保护。

针对以上情况，快快网络提供以下解决方案：

图 17 游戏盾架构部署图

1、提供游戏盾 SDK 产品。通过 SDK 接入到客户的游戏 APP 中，采用分布式高防御节点作为防御网关，抵御大流量 DDoS 攻击，可牵引至云堤清洗防御更大攻击。SDK 端与安全网关建立加密通信隧道，仅放行经过 SDK 和游戏安全网关鉴权的流量，彻底解决 TCP 协议层的 CC 攻击。在 CC 攻击期间，CC 流量直接被防御网关拦截，未透到客户的源服务器，查看防御网关节点 CPU 使用率为 25-30%，并未达到警戒线 60%。CC 新建连接并发量达到 30w 时，无玩家反馈异常。

2、基于 SDK 的网络链路诊断功能，智能选取优质网络传输路线，保证游戏时延最低，并创建断线重连机制，哪怕玩家本地 4G/wifi 网络异常，也不会导致游戏掉线。

05

2024年可操作性策略

5. 2024 年可操作性策略

5.1 2023 年总结

从所有指标来看，情况正在迅速恶化。

- 自 2020 年初以来，全球 DDoS 攻击增加了 130%。
- 每 3 秒就会发生一次新的网络攻击。
- 全球每天大约发生 34153 次 DDoS 攻击。
- DDoS 攻击对任何企业来说都是昂贵的，但未受保护的企业每次攻击的平均成本为 20 万美元。
- 即使是小型企业也受到了严重的打击——平均一次 DDoS 攻击的恢复成本为 12 万美元。

全球数字化程度的不断提高、政治动荡以及居家工作的广泛采用，都导致了一个容易受到 DDoS 攻击的环境。随着攻击数量和频率的增加，它们的规模、复杂程度以及最终的成功程度也在增加。当 DDoS 攻击成功时，会给企业带来时间、金钱、客户和声誉损失。

5.2 2024 年 DDoS 攻击趋势

趋势一：DDoS 攻击持续增长

通过近几年从快快网络监测中心记录的大量 DDoS 攻击事件中可以发现：针对关键基础设施的攻击呈现数字化发展的特点，以 DDoS 为代表的网络攻击预计会与日俱增，同时新型 DDoS 攻击从开始到攻击顶峰的时间已大幅缩短。攻击流量在短时间内达到峰值，而不是持续指数级增长。由于非常快地投放攻击载荷，这种“增强版攻击”会在常规保护措施发挥功效前就已导致网络系统瘫痪。这个趋势仍会持续，这类迅速爆发的 DDoS 攻击会越来越多。同时，

DDoS 攻击继续会有更大的体量（每秒比特数和每秒数据包数）、持续时间也更长，这主要是由于物联网设备数量激增，加上网络犯罪分子可以调用托管云上更多不安全的计算能力和容量。

趋势二：恶意生成式 AI 将进一步加剧攻防不对等

2024 年，恶意生成式 AI 或将引发大规模网络攻击活动。生成式 AI 全面降低网络攻击的门槛，并更广泛地用于提高钓鱼邮件和社会工程攻击的专业化水平，使得勒索软件更容易进到企业。同时，生成式 AI 的攻击内容更加难以被辨别，尤其是借助 Bot 自动化攻击手段，让攻击者可以更快速、准确地扫描漏洞或对网络发起攻击，大幅增加网络攻击的波及面和有效性。这给原本处于攻防弱势的防护方以更大的管理和技术挑战，安全企业、厂商、服务商需要更多的创新、共享、协同，来应对这一巨大挑战。

趋势三：构建整体全面的网络安全韧性将是企业重要战略之一

随着地缘政治、新冠疫情、技术变革等诸多因素的演变，“韧性”成为高频词，出现在各种复杂问题解决方案中。网络安全韧性是指企业组织在面临包括网络安全攻击、服务中断等在内的各种网络安全事件不利影响的局面下，能够继续企业业务运营并保持增长的能力。换句话而言，网络安全韧性是数字连续性在网络安全方面的具体展现，是属于企业整体数字连续性（以及业务连续性）的其中一部分。

塑造一个既能够有效抵御风险，又可以实现快速恢复，具有更强韧性的网络安全架构事关重大。企业组织应该在战略层面上思考如何加强其关键系统、IT 基础设施和数据中心的数字连续性，以便在面对业务中断、网络安全威胁攻击、人为错误等不利局面时保持韧性。

5.3 防护策略

如果说 2023 年是企业、政府机构和关键公共基础设施被高度复杂的网络攻击无情锁定的一年，那么可以肯定的是，网络犯罪分子将在 2024 年设定更高的目标。可被感染并变成僵尸网络的数字设备的激增，EMEA 和 APAC 地区数字基础设施的快速普及，以及欧洲和中东地区持续的地缘政治紧张局势，将继续营造一个混乱的环境，这对有动机的网络罪犯来说无疑是有利的。

在这种情况下，快快网络建议企业采取以下三个可行策略：

积极准备 DDoS 防护态势

发动 DDoS 攻击的成本相对较低，特别是随着 DDoS 服务的普及，这使它们成为恶意行为者手中强有力的网络犯罪武器。虽然无法阻止 DDoS 攻击，但采取以下步骤可以最大限度地保护组织的数字资产免受此类攻击：

- 检查组织所有的关键子网和 IP 空间，确保具备适当的缓解控制措施。
- 以“始终在线”的防护态势部署 DDoS 安全控制措施作为第一层防御，以避免紧急集成场景，并减轻事件响应者的负担。
- 主动指定一个危机响应小组，并确保运行手册和事件响应计划是最新的。当真的受到攻击时，不至于感到猝不及防。
- 使用混合保护平台备份本地 DDoS 保护，该平台可防止使本地设备过载的攻击。
- 通过网络云防火墙设置主动安全控制，将组织的安全态势扩展到基本 DDoS 保护之外。
- 最后，利用知名和久经考验的 DDoS 团队的专业知识和经验来减轻来自关键内部资源的压力。

保护 DNS 基础设施

DNS 基础设施重新成为 DDoS 攻击的主要目标。如果组织的 DNS 出现故障，那么在线状态也会出现故障。攻击可能并不总是以使 DNS 名称服务器瘫痪为目标。相反地，它可能只是希望实现资源耗尽，并降低全局服务器负载平衡性能，从而致使合法请求受到影响。

在某些情况下，保护 DNS 基础架构的安全性和性能可能具有挑战性。很多时候，传统的 DNS 防火墙不能提供足够的保护。最优的解决方案应该是具备以下特征的混合平台：

- 保护本地和云中的 DNS 区域免受各种攻击，包括 DNS 水刑（DNS water torture）、DNS 洪水等；
- 直观、轻松地管理策略和 IP 允许列表，并实时提供可操作的分析，帮助组织采取主动的安全态势；
- 通过使用高度分布式的物理访问点（point-of-presence）基础设施来从最近的位置响应用户，从而提高 DNS 性能。

结语

在当前互联网形势下，DDoS 攻击呈现出攻击威力逐渐增强、攻击频率不断上升、攻击方式日趋多样化等趋势，在可预见的未来，DDoS 依然是流行的网络犯罪手段，为保障网络环境的安全性，急需采用有效的防御策略，不断加强网络安全意识教育，提高设备管理和容灾能力，以应对日益增长的 DDoS 攻击威胁。