快快网络

快快网络2023年
DDoS全球攻击趋势专项报告

摘要

随着科技创新力量不断迸发，以科技推动产业发展、加快经济社会数字化转型升级已成为全球共识，企业上云、用云也成为趋势。同时，世界经济还在经历疫情带来的阵痛，全球黑产动作频频，引发出更多网络威胁事件，攻击手段更加智能化、隐蔽化，单一的防护策略遭遇瓶颈。攻防对抗将成为常态化，业务安全成为全球关注热点。

通过快快网络 DDoS 团队检测数据显示：游戏行业依然是 DDoS 的重灾区，一旦被盯上，73%的 IP 都会遭受多次的 DDoS 攻击。2022 年更是历年之最，仅快快网络 DDoS 云防平台监测全年超过 1Tbps 的攻击即高达 60 余次。从数据看出，6 月至 7 月以及 12 月是超 1Tbps 的攻击的高发月份。

快快网络带来了 2023 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

01

2021-2022年全球DDoS攻击情况

1 2021-2022 年全球 DDoS 攻击情况

1.1 全球 DDoS 攻击情况

NETSCOUT 威胁情报报告显示，2021 年 DDoS 攻击总次数 975 万，2022 年达到 1053 万次，同比增长 8%。

快快网络监测数据显示,2021 年中国遭受 DDoS 攻击次数达 89.90 万，占全球 9.22%，排名第二，第一为美国占比 39.54%，第三为中国香港占比 7.25%；2022 年中国遭受 DDoS 攻击次数达 116.67 万，占全球 11.08%，同 2021 年排名一致为全球第二，美国稳居第一，占比 43.29%，第三为德国占比 5.53%。

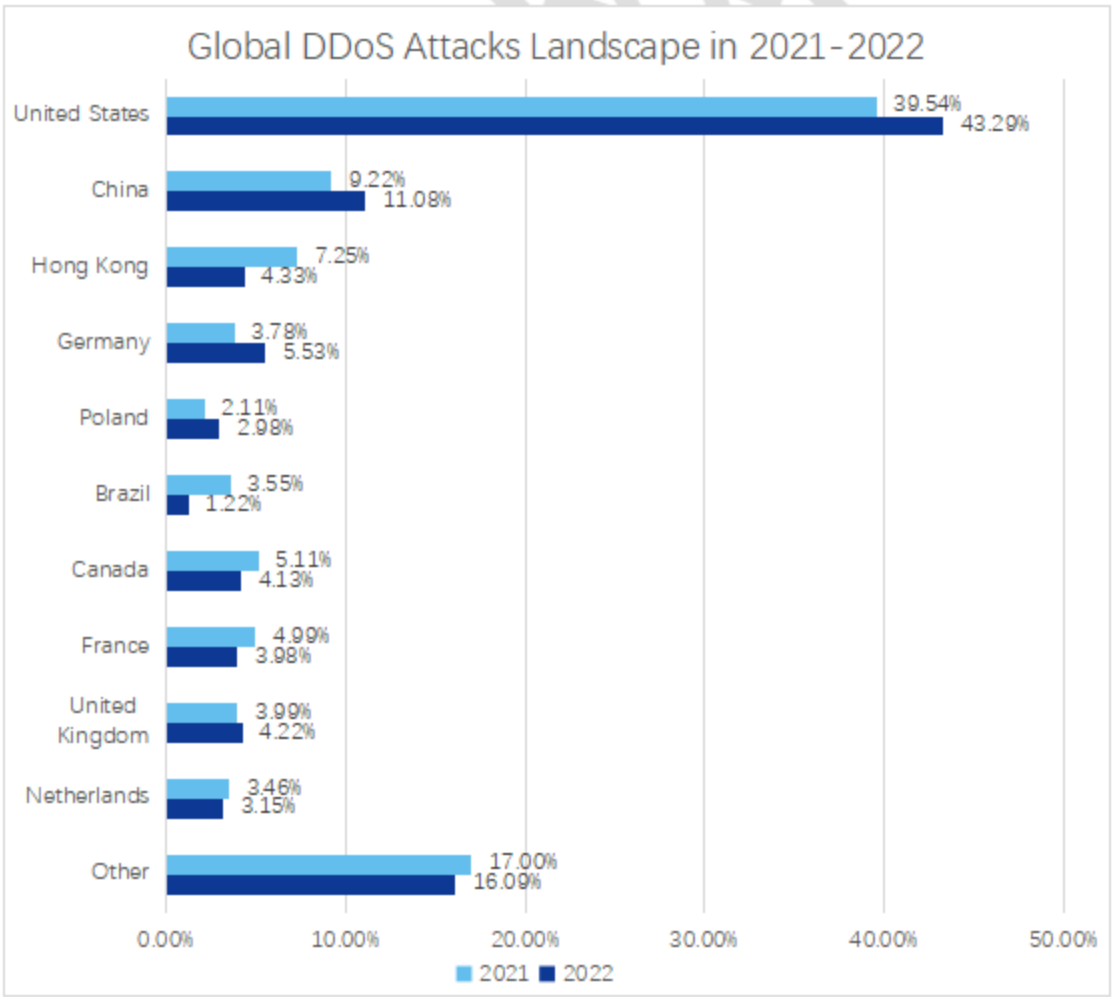

图 1 2021-2022 年全球 DDoS 攻击情况

1.2 攻击高峰期

2021-2022 年，单日最多攻击次数分别发生于 2021 年 8 月 10 日、2022 年 9 月 22 日，攻击次数达 4296 次、2215 次。单日最少攻击次数分别发生于在 2021 年 4 月 1 日、2022 年 8 月 22 日，攻击次数为 915 次、680 次。

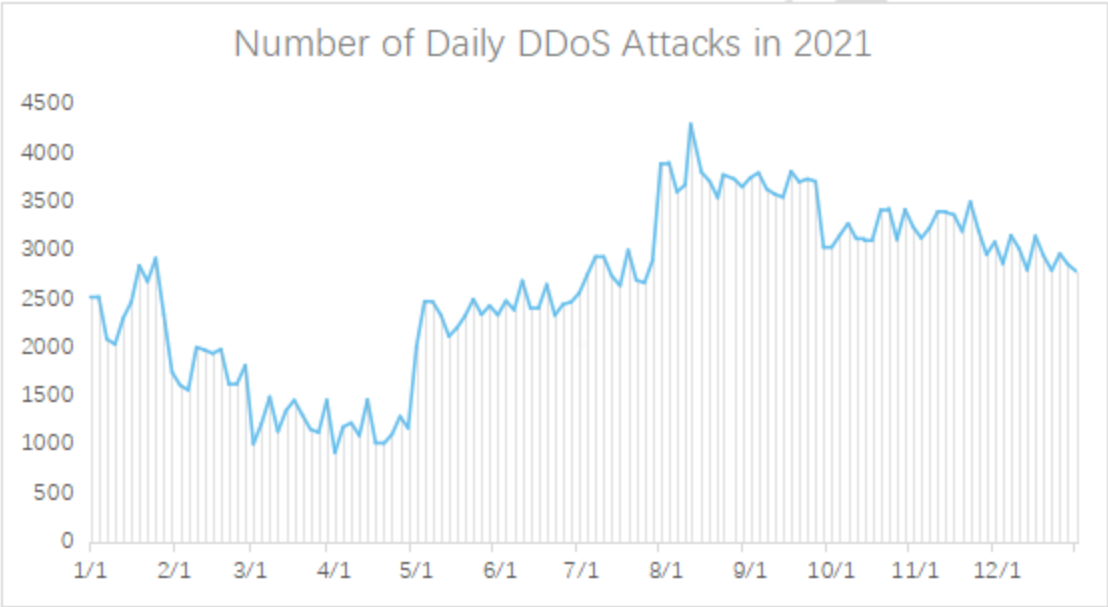

图 2 2021 年每日 DDoS 网络攻击数量

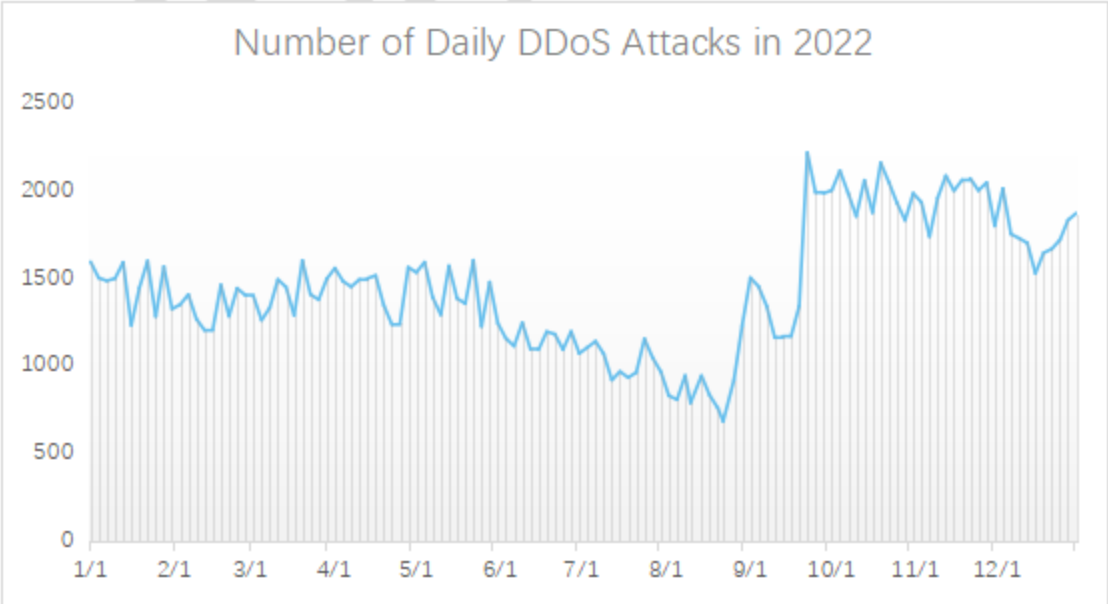

图 3 2022 年每日 DDoS 网络攻击数量

2021-2022 年网络攻击数量情况显示，上半年攻击次数普遍比下

半年少。DDoS 网络攻击数量较低集中在 2021 年 2 月-4 月、2022 年 6 月-8 月，DDoS 网络攻击数量较高集中在 2021 年 8 月-12 月、2022 年 10 月-12 月。2021-2022 年与过去几年中看到的袭击趋势保持一致，高攻击数量集中在假日期间。

2021 年最大峰值发生于 11 月，达 3.47 TBps，2022 年最大攻击峰值发生于 5 月，达 3.25 TBps。

1.3 常见攻击类型

2021 年，SYN Flood、UDP 反射、UDP Flood、ACK Flood、TCP 反射是 TOP5 网络层攻击。其中 ACK Flood 和 UDP Flood 占比较 2020、2019 年明显提升。ACK Flood 突增的主要原因是针对游戏的 ACK Flood 从虚假源泛洪演进成网络层 CC 后，攻击效果提升，成为攻击者惯用手段。

2022 年，SYN Flood、ACK Flood、UDP Flood、UDP 反射、TCP 反射是 TOP5 网络层攻击。其中，ACK Flood 和 UDP Flood 频次占比近三年呈逐年递增趋势。

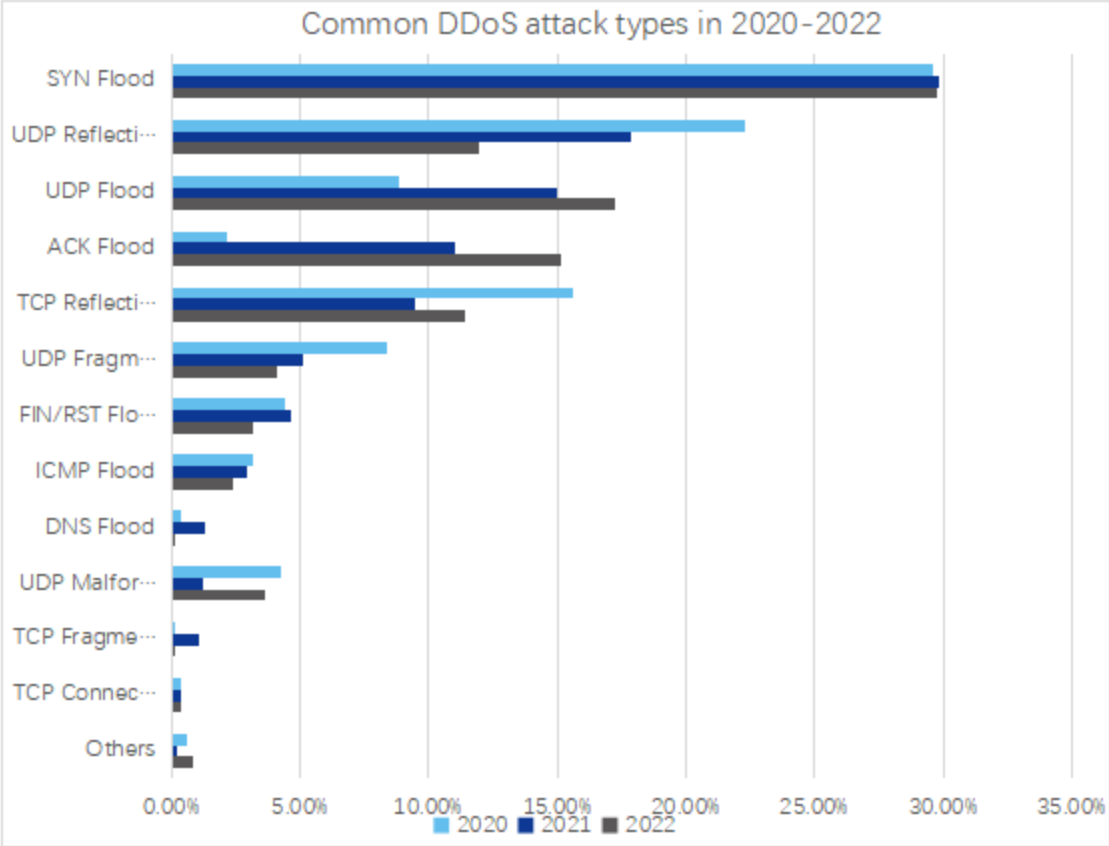

图 4 DDoS 攻击类型

1.4 短时攻击流行

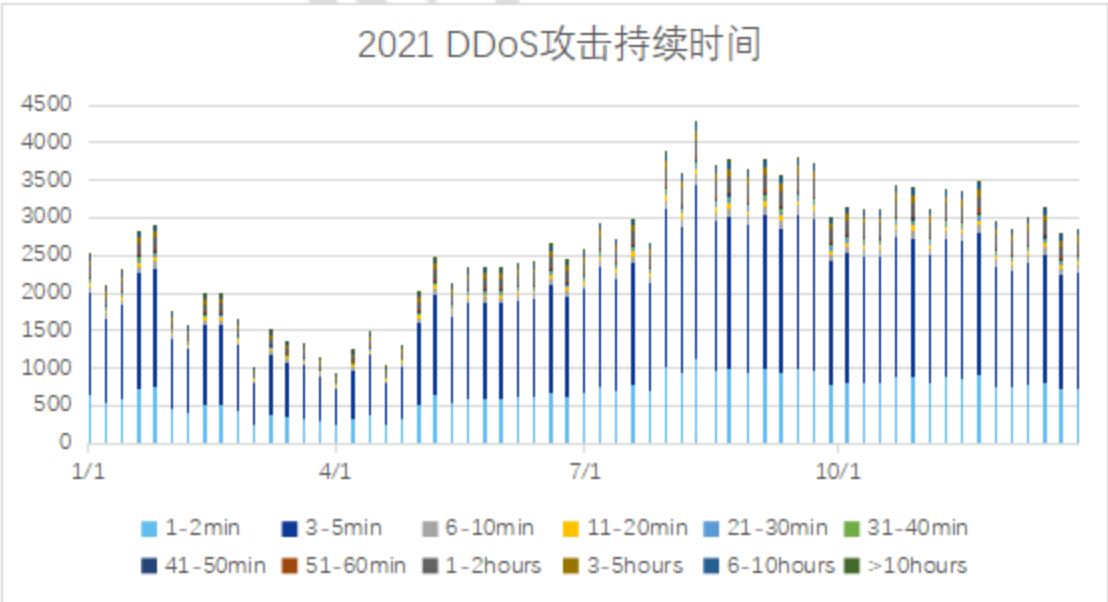

图 5 2021 DDoS 攻击持续时间

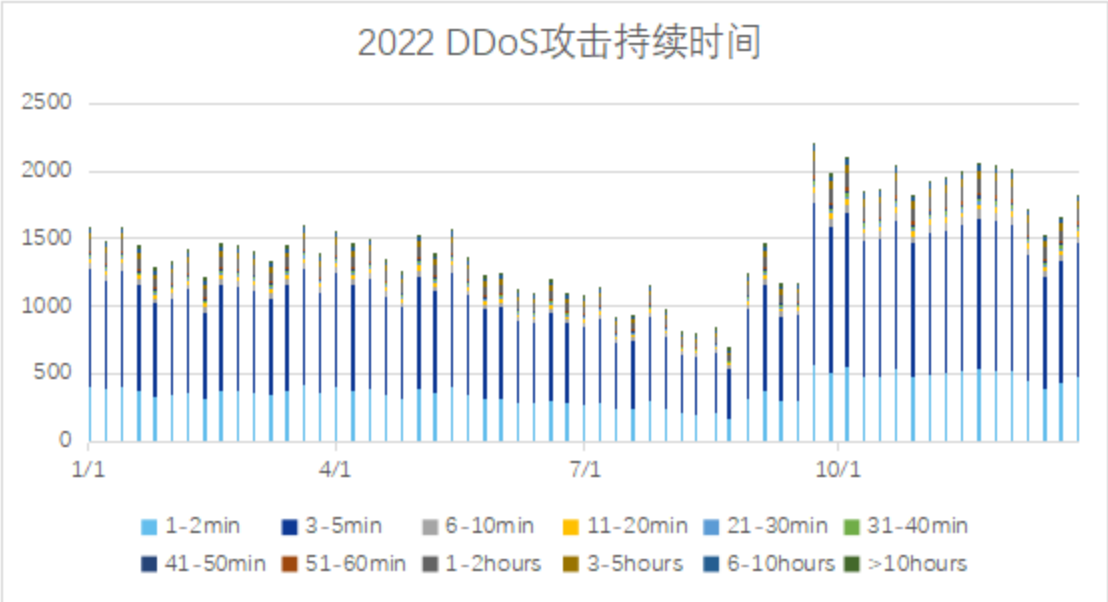

图 6 2022 DDoS 攻击持续时间

2021 年，80%的 DDoS 攻击时长在 5 分钟以内，2022 年，89%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 26%。近两年来，持续时间较短的 DDoS 攻击更为常见，说明攻击者越来越重视攻击成本、效率和技术对抗，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。长远来看，多次瞬时攻击能够严重影响目标的服务质量，有效控制攻击成本，尽快耗尽 DDoS 防御服务人员的精力。

短时攻击利用了系统检测攻击和缓解所需的时间。缓解时间可能只需要一两分钟，但这些短时攻击的信息可能会进入服务后端，影响合法使用。如果短时攻击会导致系统重新启动，那么当每个合法用户同时尝试重新连接时，这可能会触发多个内部攻击。

1.5 攻击源来源

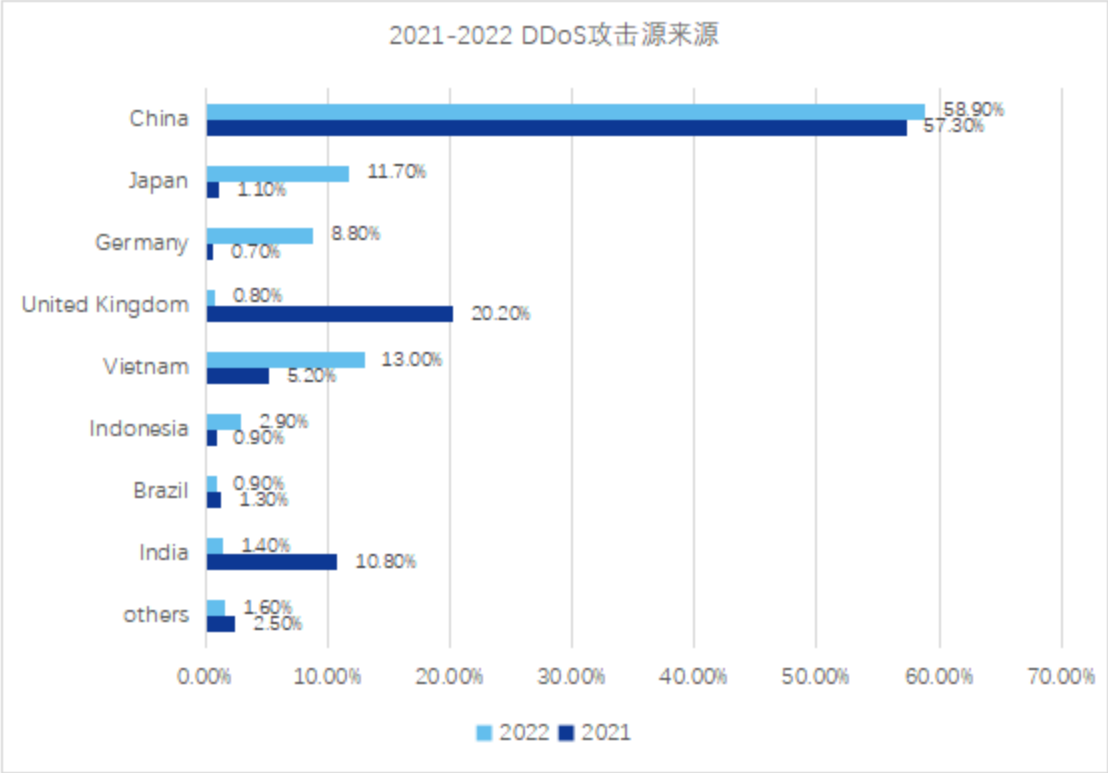

图 7 攻击源来源

中国经济体量大、人口多，互联网产业较发达，一直位居最主要攻击源来源国家的前 2 位。

2021 年，来自中国的攻击源达到 57.3%，2022 年，来自中国的攻击源达到 58.9%。日本、德国、韩国、英国等发达国家，以及越南、印度尼西亚、巴西、印度等发展中国家也是主要的攻击源分布国家。

02

2021-2022年国内DDoS攻击情况

2 2021-2022 年国内 DDoS 攻击情况

2.1 攻击次数情况

DDoS 攻击频率呈逐年倍增趋势。2021 年共监测到 89.90 万次 DDoS 攻击，是 2020 年的 2.5 倍。尽管 2021 年由于出现大型扫段攻击，攻击次数已经处于高位，但是 2022 年全年 DDoS 攻击次数同比 2021 年还是增长 8%，DDoS 威胁维持了 4 年持续增长的态势。

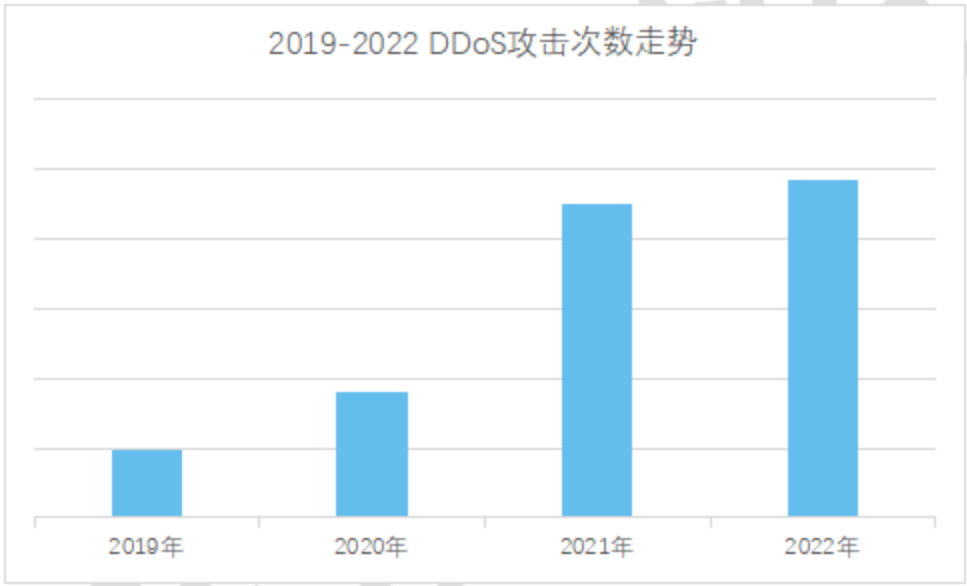

图 8 DDoS 攻击次数走势

2.2 攻击热点行业

2021 年 DDoS 攻击行业分布呈现多元化趋势。游戏行业 DDoS 攻击占比继续保持第一，但是相比往年比率偏低，不再是一家独大的局面。除游戏行业外，云计算、企业官网、视频直播、IT 通信等行业成为 2021 年攻击占比较高的行业。

2022 年，通过对 DDoS 攻击目标的行业属性分析发现，互联网是 DDoS 攻击主要目标，排在第一位的依然是游戏行业，占比达到了 60%

以上。针对游戏的攻击，很大一部分原因与竞品有关，其中手游遭到 DDoS 攻击最为频繁。

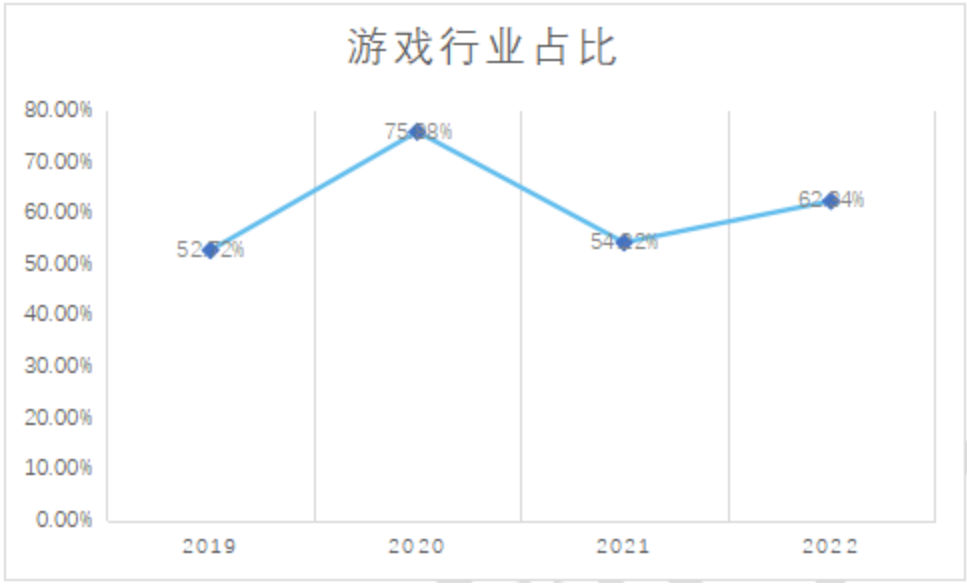

图 9 DDoS 攻击游戏行业占比

2.3 攻击矢量分布

为挑战防御成功率，提升防御成本，混合攻击是主流。2021 年混合攻击占比 85.81%，多于五种矢量的混合攻击占比高达 35.11%。2022 年混合攻击占比较 2021 年有所降低，占比 63.47%。

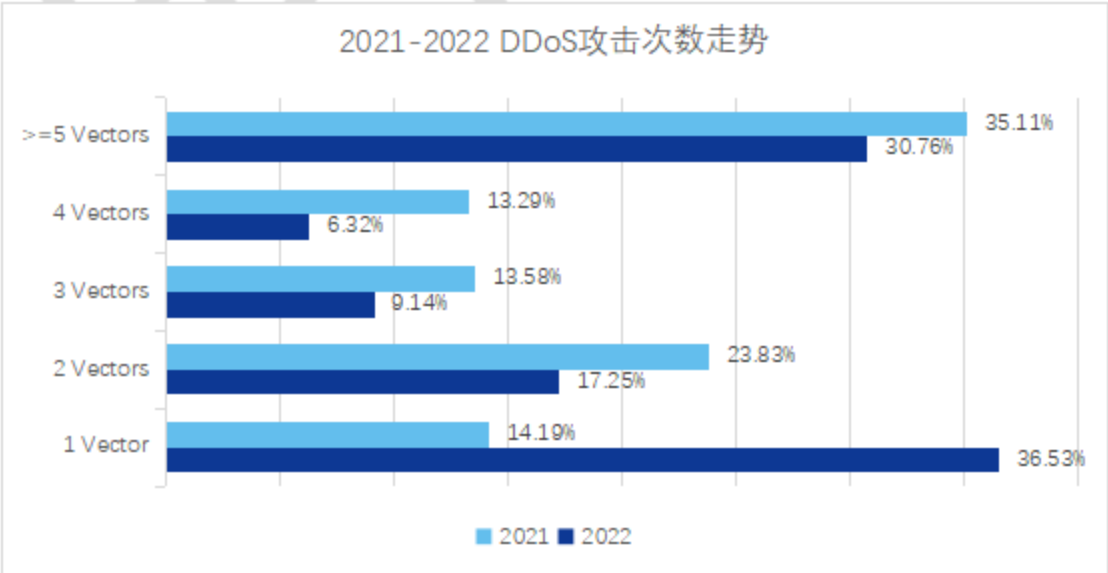

图 10 DDoS 攻击矢量分布

2.4 大流量攻击威胁趋势

2021 年，300G 以上更大规模的 DDoS 攻击在超百 G 的大流量攻击中的占比也明显提升，2021 年有 5 个月（2 月、6 月、7 月、8 月、10 月）占比超过 30%。统计数据显示，相当比例的超百 G 大流量 DDoS 攻击是由 SYN 大包或 UDP 反射之外的手法发起的（包括 TCP 反射、SYN 小包、ACKFLOOD 等），说明超百 G 大流量 DDoS 攻击手法呈明显多元化趋势。

2022 年，DDoS 攻击黑产获得了大量的攻击资源和攻击带宽，导致百 G 以上的大流量攻击越来越普遍，而且呈现明显的大流量攻击增长幅度高于整体威胁增长幅度的态势。2022 年百 G 以上大流量攻击同比增幅超过 5 成，平均下来大约每隔 1 小时就会出现 1 次百 G 以上的大流量攻击。

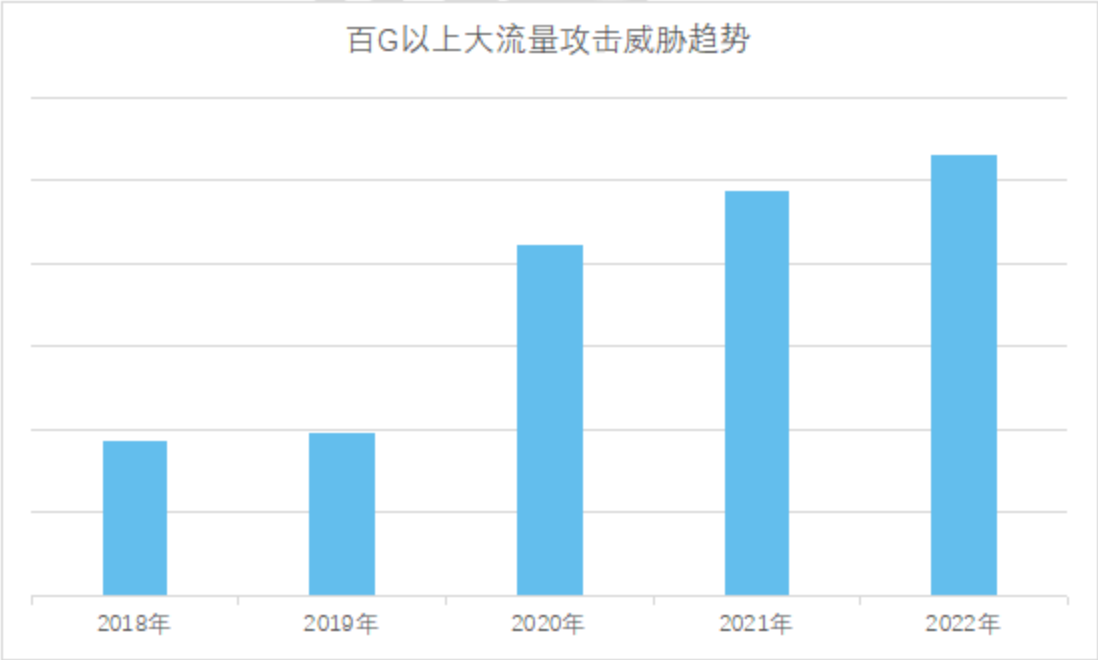

图 11 大流量攻击趋势

2.5 最大攻击峰值

2021 超大流量攻击主要集中在 6-8 月，其中最大攻击发生于 7 月，攻击流量峰值为 1.85Tbps，持续 19 分钟。2022 年的攻击峰值再创新高，最大攻击峰值同比去年增长 11%，达到 2.05Tbps，2022 年也成为攻击峰值最大的一年。

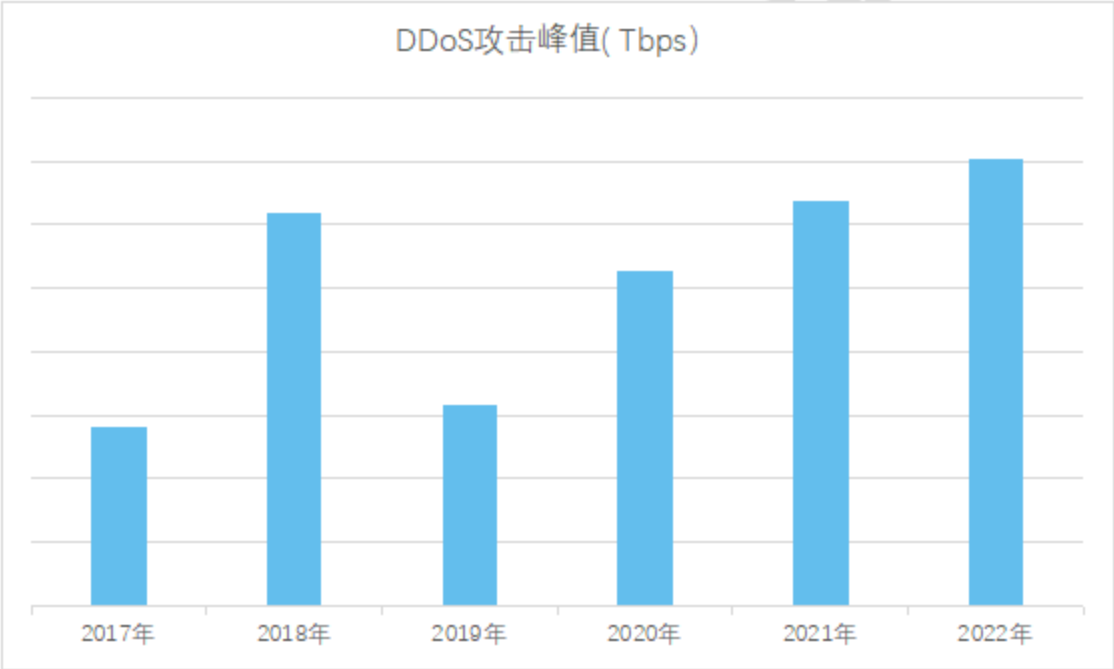

图 12 DDoS 攻击峰值

03

快快网络DDoS攻防态势观察

3 2021-2022 年快快网络 DDoS 态势观察

快快网络 2021-2022 年整体 DDoS 威胁呈上升趋势。

3.1 攻击峰值

2021 年攻击峰值最高值出现在 7 月份，为 1.77 Tbps；2022 年，快快网络攻击峰值突破 T 级高达 5 个月，集中在 6 月-8 月之间。6 月峰值最高，为 1.96 Tbps，同比增长 10.7%。大流量攻击集中在 6 月和 11 月。

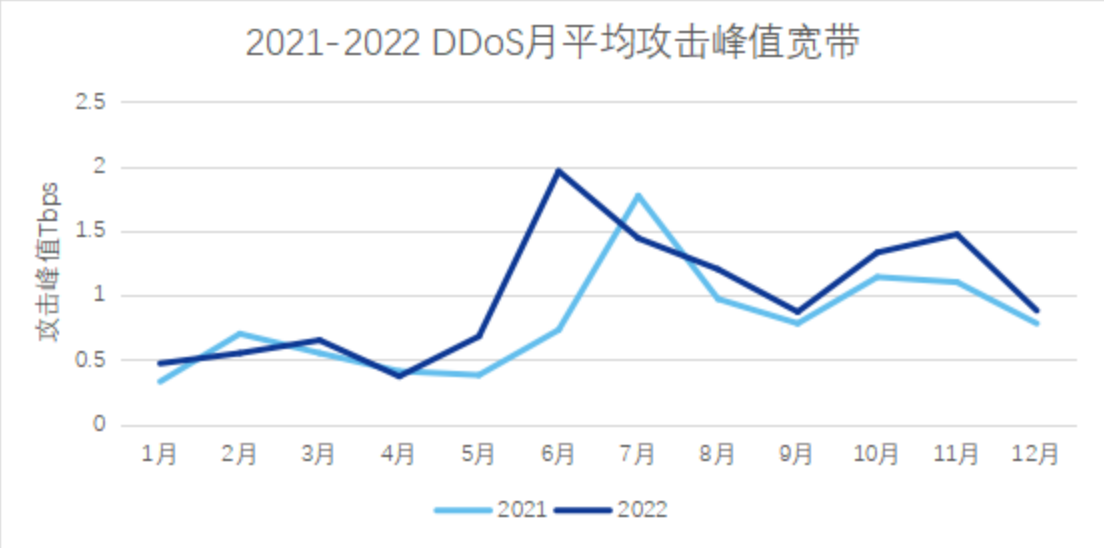

图 13 2021-2022 年 DDoS 攻击峰值

3.2 攻击次数

2021 年-2022 年，快快网络共计成功防护 42.7 万起 DDoS 网络攻击。其中，2021 年 19.5 万起，2022 年 23.2 万起，同比增长 18.9%。1 月-3 月 DDoS 网络攻击次数较低，5 月份、6 月份攻击次数最多，占全年 23%。

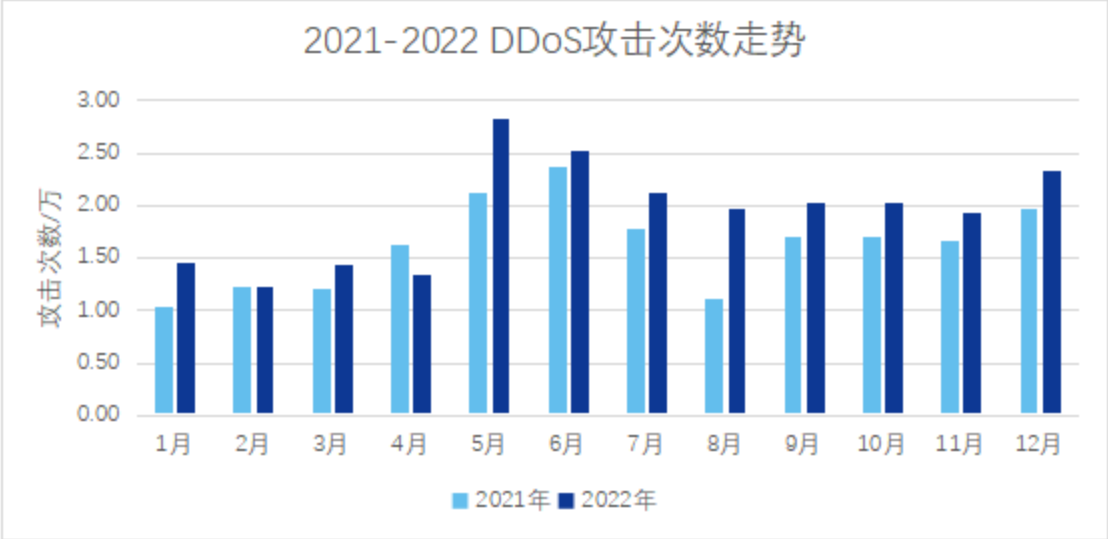

图 14 DDoS 攻击次数走势

3.3 攻击方式

攻击者使用的 DDoS 攻击方式主要包括 UDP Flood、ACK Flood、SYN Flood 等。2021 年 UDP Flood 占比最高，为 27.3%，其次分别为 SYN Flood、ACK Flood，占比为 14.8%、11.9%。2022 年，SYN Flood 占比最高，为 28.2%，其次为 UDP Flood，占 21.3%，ACK Flood 占 11.4%。

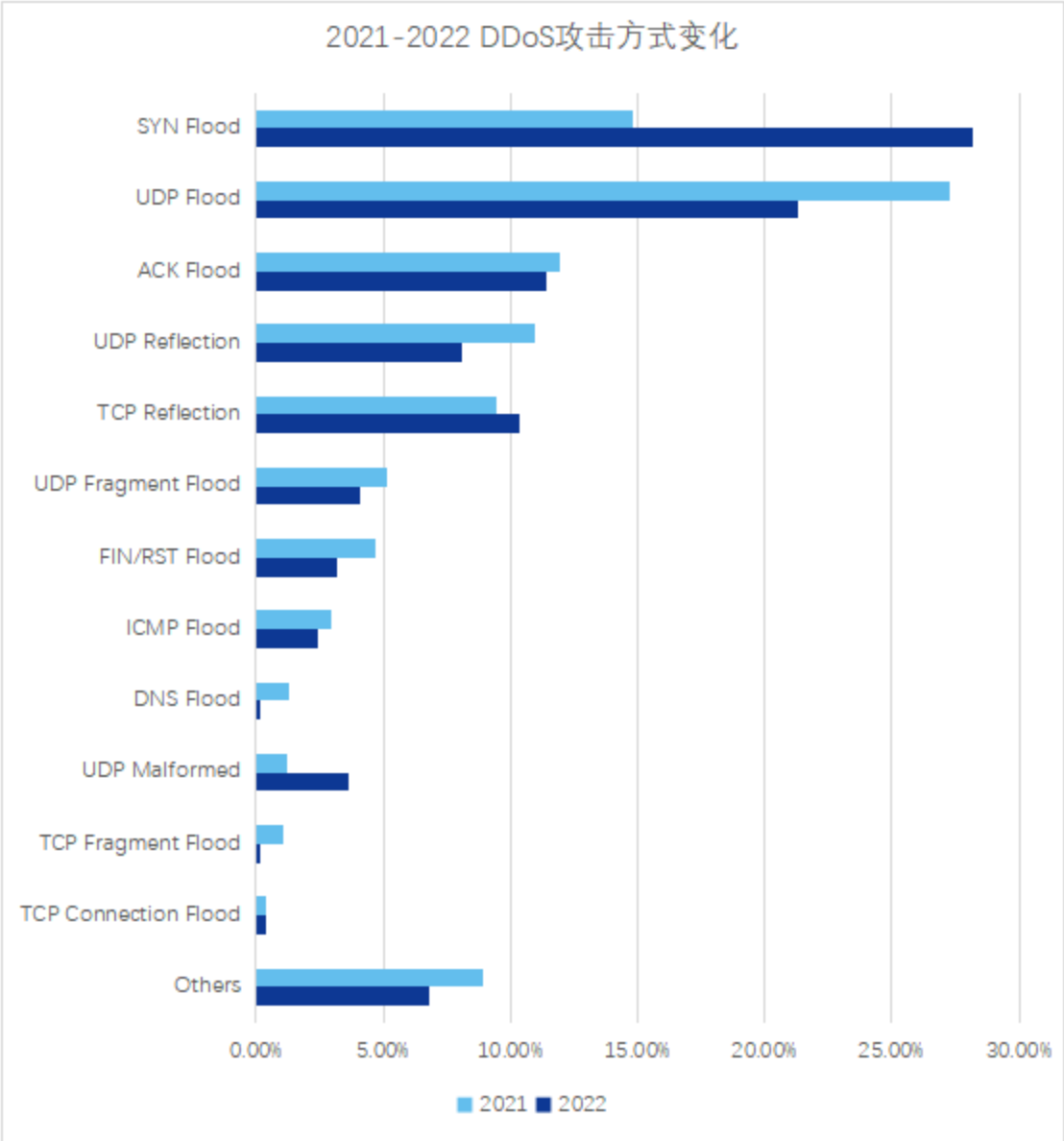

图 15 DDoS 攻击方式变化

3.4 攻击行业

通过对 DDoS 攻击目标的行业属性分析发现，传媒互联网行业仍是 DDoS 攻击的重灾区，包含游戏、电商、互联网金融、社交等分支行业，行业内竞争激烈导致传媒和互联网行业一直是 DDoS 攻击的高地，其中排在第一位的是游戏行业。2021 年游戏行业攻击频次占比达到了 51.19%，2022 年占比达 51.57%。

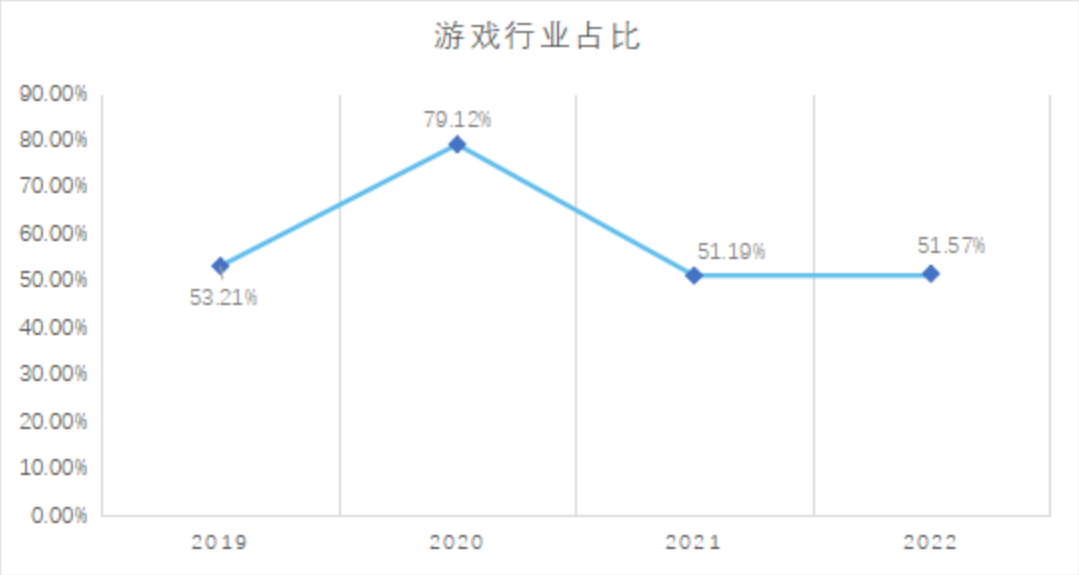

图 16 DDoS 攻击行业

04

攻防对抗案例

4 攻防对抗案例

4.1 案例一：某知名游戏公司

2022 年 6 月，该公司遭遇针对性强的 DDoS、CC 组合式攻击，累计被攻击长达 7 天，流量峰值高达 1.12T，累计 CC 请求数超过 10 亿次，意图使其应用程序处理崩溃。

攻击手法：

使用常规 SYN 大包搭配 UDP 反射包→转用 PSHACK 混合 SYN 小包的专业攻击手法→混合多种攻击数据包、模拟 CC 攻击。

防护难度：

攻击时间过长，混合多种攻击数据包，并针对业务模拟 CC 攻击，意图使用户应用程序处理崩溃。

在面对这场持续多日的攻击时，快快网络快速研究了该公司的业务结构，为其定制相应的 DDoS 防护解决方案，提供全方位保护。

具体应对方案包括：

1. 快快网络 DDoS 防护解决方案提供全面的 4 层/7 层防护。

2. 对所有访问流量进行清洗，经过清洗后再将流量注回该公司的源服务器。

3. 基于 AI 数据算法深度学习该公司业务基线，快速智能地决策下发最佳的防护方案。

4. 为该公司配备专业的 1V1 24 小时无死角在线服务，并对定制

级的需求提供保驾护航调优，确保最高效的防御效果。

快快网络专业的 DDoS 防护解决方案在这次攻击多次证明其高效，为该公司应对 DDoS、CC 攻击提供了有力的保护。

4.2 案例二：某电商平台

该公司使用的源服务器在香港 A3 云，但是遇到了 200-400G 的 DDoS 攻击，同时由于香港国际 A3 云网络不够稳定，所以导致 443 端口的网络连接经常中断；其售后服务响应速度较慢，需要提交工单等待回复，无法实时沟通，给该公司的业务造成严重影响。

针对以上情况，快快网络提供以下应对方案：

1. 针对该公司在 A3 云香港国际网络不稳定的情况，提供全球高防 CDN+专线定制方案，以确保该公司业务的稳定性和持续性。

2. 成功为该公司抵御峰值达到 300G 的 DDoS 攻击，通过专业的抵

御手段和技术方案来保障其业务的稳定性和安全性。

3. 为该公司配备专业的 1V1 7x24 小时无死角在线售后服务，用于解答该公司的业务问题并及时处理。

通过以上方案的实施，快快网络成功地保障了该公司的业务安全，同时提高了该公司对快快网络服务的满意度。

4.3 案例三：某游戏 APP 项目

该公司的新游戏服务器上线后不久就遭遇 DDoS 攻击，使得玩家的访问体验急剧下降、卡顿和掉线问题频发；而由于 A3 云 DDoS 防护成本过高，费用高达上百万，该公司寻求了快快网络的帮助。

防护难度：

该公司遭受有组织、有预谋的 DDoS 攻击，攻击目标主要是游戏的 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，快快网络提供以下应对方案：

1. 提供游戏盾 SDK 产品。通过 SDK 接入到客户的游戏 APP 中，成功为其抵御 DDoS 攻击和百万级 CC 攻击。游戏盾产品具有高效可靠的防护能力和丰富的协议层次识别能力，保障了游戏服务器的稳定和用户体验。

2. 快快安全专家与该公司深度沟通配合和优化。通过 SDK 接入到游戏中，在 DDoS 或 CC 攻击时始终保持玩家无感知，用户能够平稳游戏，不会受到攻击的影响。

3.通过游戏盾 SDK 智能化最优路径决策调度，玩家能够以最优速度登录游戏，为玩家提供了最佳的游戏体验。

通过以上方案的实施，快快网络成功地帮助该公司解决了 DDoS 攻击的问题，同时提高了游戏的稳定性和用户体验；快快网络的游戏盾 SDK 产品和专家支持为该公司提供了高效、可靠的防护能力和完整的服务保障。

05

2023年DDoS攻击发展趋势预测

5 2023 年 DDoS 攻击发展趋势预测

5.1 DDoS 攻击成为网络战的重要手段

研究人员发现，DDoS 攻击已经被大量用于实施网络战。针对银行、能源和医疗等行业部门的 DDoS 攻击在 2022 年已有所增多。而在地缘政治冲突变得更普遍的情况下，针对关键基础设施的攻击也将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。

除了出于政治动机的网络威胁外，近年来还出现了一些新的攻击模式，比如 DDoS 勒索攻击，这些攻击模式在 2023 年也将会继续出现并呈现增长态势。

5.2 DDoS 攻击更猛烈

2022 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：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。

5.3 “地毯式轰炸攻击”模式

为了获取更大的攻击效果，DDoS 攻击者在攻击规模、频率和目标多样化方面不断提高标准，攻击途径也在不断增多。面对受害者的防御策略，攻击者会同时采用多种攻击方法，形成所谓的“地毯式轰炸攻击”模式。这种攻击会对目标区域进行密集轰炸，但各自的数据包可能非常小且很不起眼，因此可以绕过许多防护系统的拦截。在 LSOC 发现的一起攻击中，攻击者使用了多个途径，大量端口和协议在攻击过程中反复变化。因此，传统的 DDoS 防护方案根本无能为力。2023 年，这种 DDoS 攻击模式可能会成为主流。

5.4 攻击媒介多样化

攻击者还在尝试更多的 DDoS 攻击媒介。2023 年，预计会出现更多基于 TCP 或类似协议的洪水攻击和应用程序层攻击。对付这种类型的攻击比对付典型的 DDoS 放大攻击难得多。因此，防御战术需要通过融合机器学习等先进技术加以应对，而不仅仅只是通常用于应对放大攻击的端口或协议封阻。

5.5 攻防双方的较量更激烈

虽然 DDoS 容量耗尽攻击是最广泛的 DDoS 攻击类型之一，但其攻击效果目前已明显减弱，尤其是在基础设施行业领域，因为现有的 DDoS 防护措施可以很有效地检测和挫败这类 DDoS 攻击活动。然而，由于网络基础设施的脆弱性和敏感性，意味着攻防双方的竞争将会持

续并不断加剧。借助人工智能技术，新一代 DDoS 攻击者所采用的方法和攻击种类在不断进化，以造成最大程度的破坏。因此需要同样智能化、自动化的 DDoS 防护解决方案，才可以确保防御者领先一步。

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。