2021
DDoS攻击态势报告

中国电信 CHINA TELECOM 云堤 SECURITY

NSFOCUS 绿盟科技

关于绿盟科技

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 50 余个分支机构，为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和办事处，深入开展全球业务，打造全球网络安全行业的中国品牌。

天翼安全科技有限公司

天翼安全科技有限公司（以下简称中国电信安全公司）是中国电信集约开展网络安全业务的科技型、平台型专业公司，以研发运营一体化方式，整合全集团云网、安全、数据等优势资源和能力，进行统一运营，为内外部客户提供云网安全、数据安全、信息安全等各类安全产品和服务。公司始终坚持以传承红色基因守护安全中国为使命，致力于成为数字经济时代最可靠的网络安全运营商！

截至目前，公司已斩获国家级、省部级、行业级优秀项目奖百余项，授权专利 10 项，软件著作 12 项，入选国资委重大科技创新成果和年度网络安全优秀解决方案奖，工信部“网络安全试点示范项目”4 个，中国通信学会科学技术奖一等奖，多次入围权威机构评选的网络安全百强企业，并跻身领军者行列。已为政务、金融、企业等全行业超过 6000 家客户提供了运营商级网络安全服务。

版权声明

NSFOCUS

CONTENTS

01

执行摘要

疫情之下，全球数字化正在加速发展，各行业向数字化、智能化转型的步伐加快。与此同时，网络安全作为数字化发展的重要保障，在网络威胁日益加剧的情况下，面临诸多挑战。DDoS 攻击作为网络安全的严重威胁之一，至今已活跃超过 20 年。DDoS 攻击事件频繁发生，新型攻击不断涌现，给网络安全带来了巨大挑战。及时掌握 DDoS 的攻击目标、攻击资源、攻击手段、攻击能力等，是建立动态高效的 DDoS 安全防御体系的基础。

绿盟科技联合中国电信安全公司推出《2021DDoS 攻击态势报告》，旨在从 DDoS 攻击整体态势、攻击类型、攻击资源、僵尸网络等方面剖析 2021 年 DDoS 的演化情况，力求让用户全面了解 2021 年 DDoS 攻击态势，以便帮助各组织 / 机构持续改善自身网络安全防御体系及技术，提升应对日益复杂的 DDoS 攻击能力，助力云计算、大数据、物联网、工业互联网等新兴数字产业的快速发展。2021 年 DDoS 攻击整体态势如下：

经过主管机构近两年持续推进的“净网 2020”、“净网 2021”专项行动，黑灰产业链遭到了严重打击，DDoS 攻击次数和攻击流量整体呈现出下降的趋势。然而，这并不代表攻击者就此放弃与防守方的博弈，在利益的驱使下，他们从未放弃过这种对抗博弈。也正是在攻防两端能力长期的较量下，DDoS 攻击复杂化、规模化不断提升。2021 年混合攻击次数大幅增长，单次攻击事件包含大容量泛洪、应用层攻击、连接耗尽型攻击等，而新型攻击也在不断涌现。在数字化发展的浪潮下，攻击者抓住机遇，利用高网络带宽提升自身的攻击能力，单次平均攻击峰值和最高攻击峰值不断增长，大于 300Gbps 以上的超大型攻击次数较 2020 年更是大幅增长，对 DDoS 的清洗和防护都提出了更大的挑战。大流量攻击的贡献者主要来自反射攻击，NTP 反射放大 400~500 倍，攻击效果显著，一直备受攻击者的青睐。参与 DDoS 攻击的物联网设备数量也在持续增长，投入小、收益高、更新快、基数庞大等一系列优越条件使得物联网设备逐渐发展成发起大规模 DDoS 攻击的利器。僵尸网络 Dofloo、XorDDoS 和 Mirai 三大家族各有特色，2021 年攻击活动活跃度位列前三，且利用漏洞和弱口令扩张控制范围的势头愈演愈烈。

02

重要观点

★ 观点一：打击网络黑灰产“毒瘤”，国内网络空间日趋清朗

经过主管机构近两年持续推进的“净网 2020”、“净网 2021”专项行动，黑灰产业链遭到了严重打击。DDoS 攻击次数和攻击总流量连续三年持续下降，2021 年 DDoS 攻击次数较 2020 年减少了 19.14%，攻击总流量减少了 6.05%，治理效果显著。

★ 观点二：DDoS 攻击方式复杂多变，令人防不胜防

在攻防两端能力长期的较量下，DDoS 攻击手法更为“巧妙”。攻击者根据目标系统具体情况，灵活变换攻击方式，利用协议、系统的缺陷，尽其所能展开攻击，危害极大。2021 年 DDoS 混合攻击大幅增长，较 2020 年增长了 80.8%。

★ 观点三：攻击者持续“进阶”，防护遭遇挑战

随着全球数字化蓬勃发展，网络设备可用带宽增加，一旦被僵尸网络所利用，其执行 DDoS 攻击的可用带宽也随之增加。近三年 DDoS 单次平均攻击峰值和最高攻击峰值呈增长趋势，大于 300Gbps 以上的超大型攻击次数较 2020 年更是大幅增长，DDoS 攻击者能力不断提升。

★ 观点四：物联网设备“备受青睐”，威胁不容小觑

2021 年参与 DDoS 攻击的物联网设备较 2020 年增加约 2 万个，近三年连续增长。其中，由于摄像头和路由器基数庞大、投入小、收益高等，一直备受 DDoS 攻击者的青睐，安全问题尤为严重，参与 DDoS 攻击的数量占总量的七成以上。

★ 观点五：僵尸网络利用漏洞和弱口令扩张控制范围的势头愈演愈烈

2021 年 Mirai 僵尸网络已经发展到 27 个分支版本，从利用弱口令发展到利用漏洞感染扩展，如今发现最高携带了 36 个 Nday 漏洞，寻找一切机会感染其他设备扩张控制范围。另外 Meris 新家族集成 HTTP Pipeline 攻击技术并利用漏洞和弱口令感染，在 2021 年的 DDoS 应用层攻击方面表现极为活跃。

03

2021 年 DDoS 攻击分析

3.1 DDoS 攻击次数和流量峰值情况

3.1.1 DDoS 攻击次数和攻击流量

2021 年共监测到 DDoS 攻击次数为 12.33 万次，攻击总流量为 36.31 万 TB，如图 3.1 所示。与 2020 年相比，攻击次数减少了 19.14%，攻击总流量减少了 6.05%。分析其主要原因，一方面是由于抗 D 设备检测和防护能力越来越强，使得攻击难度和成本增加，攻击者就很有可能转向那些低风险、高回报的目标。另一方面得益于主管部门近两年持续推进的“净网 2020”、“净网 2021”专项行动，黑灰产业链遭到了严重打击。

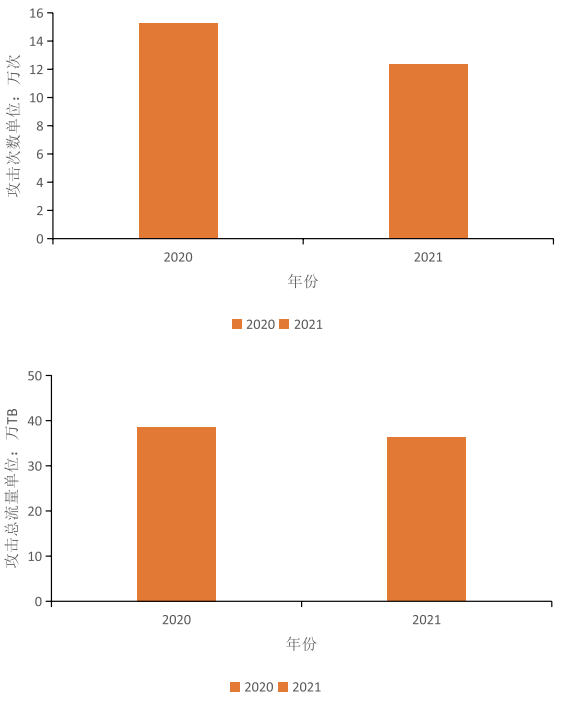

图 3.1 2021 年 DDoS 攻击态势

数据来源：中国电信安全公司

从 2019 年至 2021 年的 DDoS 攻击次数和攻击流量来看，每月平均攻击次数分别为 1.52 万次、1.27 万次和 1.03 万次，平均攻击总流量分别为 4.0 万 TB、3.22 万 TB 和 3.03 万 TB，整体呈现出下降的趋势，如图 3.2 所示。另一方面，与前两年一样，2021 年的 DDoS 攻击表现较为平稳，无大幅度的波动。但是这并不能代表 DDoS 攻击的长远发展态势，5G 时代的海量带宽，物联网的规模化应用，未来很可能会再出现大规模的 DDoS 攻击。

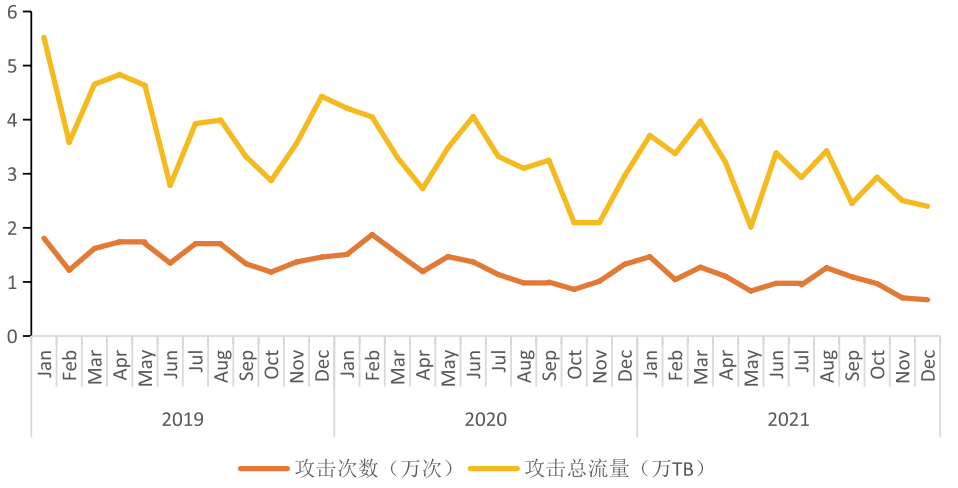

图 3.2　近三年 DDoS 攻击态势

数据来源：中国电信安全公司

从 2021 年各月攻击次数来看，如图 3.3 所示，DDoS 攻击次数整体平稳，在 1 月份达到峰值，较 2020 年 1 月份，同比下降 2.9%，基本持平。2 月份 DDoS 的攻击次数，较去年 2 月份，同比下降 44.4%，呈现出新冠疫情前“消停”的状态。值得注意的是在 2020 和 2021 年的 10 月份，DDoS 攻击都呈现出一个小低谷，攻击次数较 9 月份环比分别下降了 13.6% 和 11.5%，这主要是由于国庆节前夕，全国范围内都加强了网络安全保障，网络安全防护能力提升。

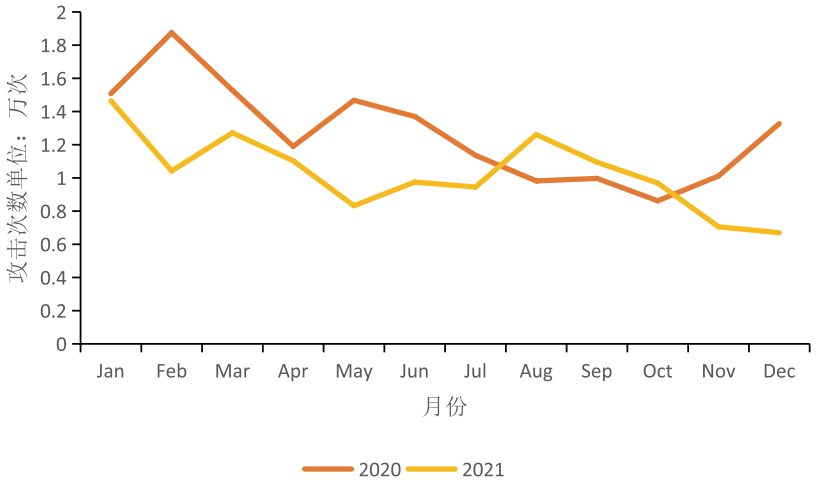

图 3.3　攻击次数

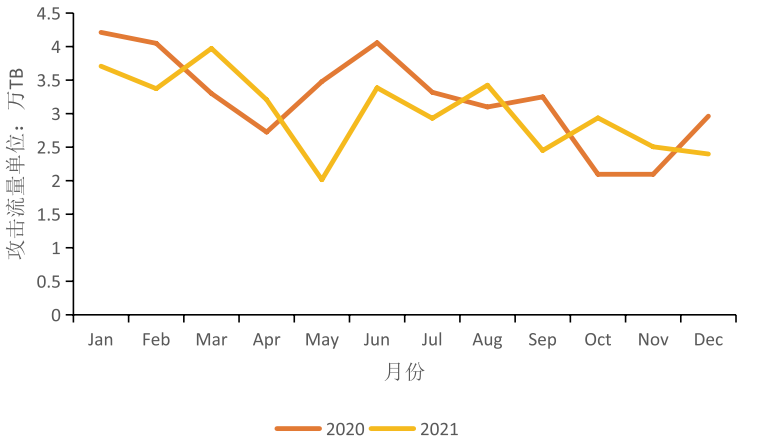

图 3.4　攻击流量

数据来源：中国电信安全公司

3.1.2　攻击峰值分布

2021 年，如图 3.5 所示，在全部 DDoS 攻击中，21.47% 的攻击峰值在 20-50Gbps 之间，占比最高，较 2020 年增加了 3.41%。攻击峰值在 1G-20Gbps 的各区间分布趋于平均，较 2020 年占比有所减少。5-50Gbps 的中小型攻击占比约为 52.13%，与 2020 年的分布基本一致。大于 200Gbps 的 DDoS 攻击较 2020 年增加了 2.02%，这种大型攻击的增长无疑会给 DDoS 的清洗和防护带来更大的挑战。

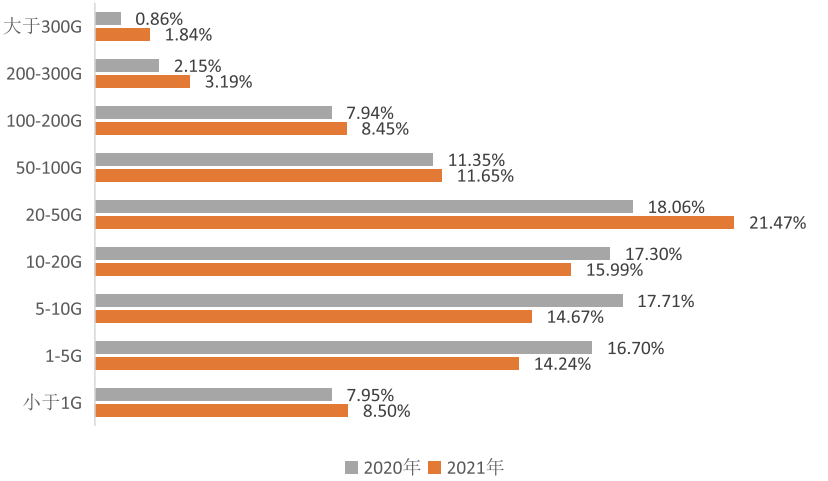

图 3.5　攻击峰值分布

数据来源：中国电信安全公司

从 2021 年各季度来看，如图 3.6 所示，DDoS 攻击峰值小于 5Gbps 的小型攻击呈增长趋势，峰值在 5-50Gbps 之间的中小型攻击在前两个季度的占比基本持平，进入 Q3 后，环比下降了 7.74%，Q4 环比下降了 11.8%。峰值在 50-300Gbps 的大规模攻击在各季度的占比基本持平，300Gbps 以上的超大规模攻击在 Q4 占比最高。从图中也可以看出来，与 2020 年分布一致，5-50Gbps 的中小型攻击仍是各季度的主流攻击流量，且每个季度表现的比较规律，反映出 DDoS 攻击者的能力仍然集中在中小型的攻击流量上，且对目标的了解能力和控制能力更精确。

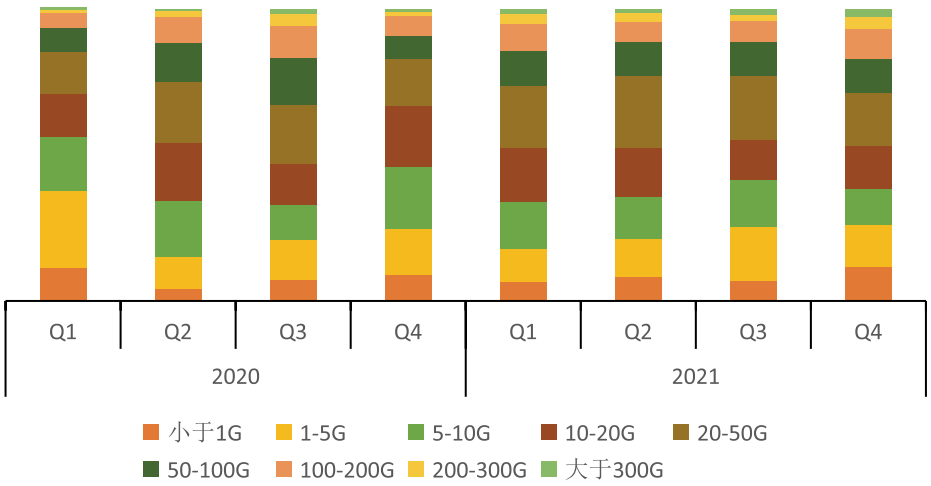

图 3.6　2020 年 vs 2021 年各季度各类规模攻击次数占比

数据来源：中国电信安全公司

3.1.3　大流量攻击分布

从近三年的 DDoS 大流量攻击数据来看，攻击峰值在 100Gbps 以上的大型攻击近两年趋于平稳，如图 3.7 所示。2021 年 100Gbps 以上的大型攻击发生了 1.64 万次，较 2020 年的 1.59 万次增加了 3.1%。攻击峰值在 300Gbps 以上的超大型攻击在经历 2020 年的大幅减少之后，2021 年又呈现出了大幅度的上升，较 2020 年增长了 84.8%，增加到每月平均 184 次。超大规模的 DDoS 攻击将会带来严重的破坏效果，甚至是毁灭性打击，这就要求抗 D 设备的防护性能要不断加强，以抵抗超大规模的 DDoS 的攻击。

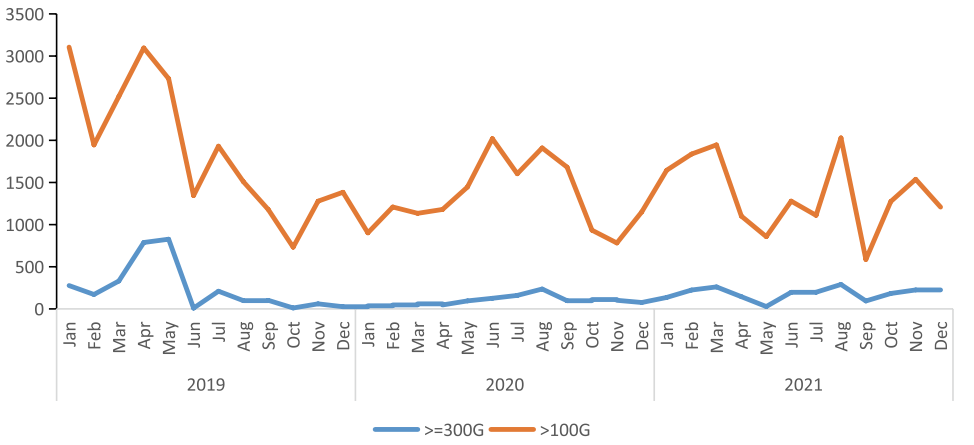

图 3.7　近三年大流量攻击的次数变化

数据来源：中国电信安全公司

单看 2021 年，1、2、3、8 月份为大流量攻击高峰，如图 3.8 所示。8 月最多，占比 12.36%。

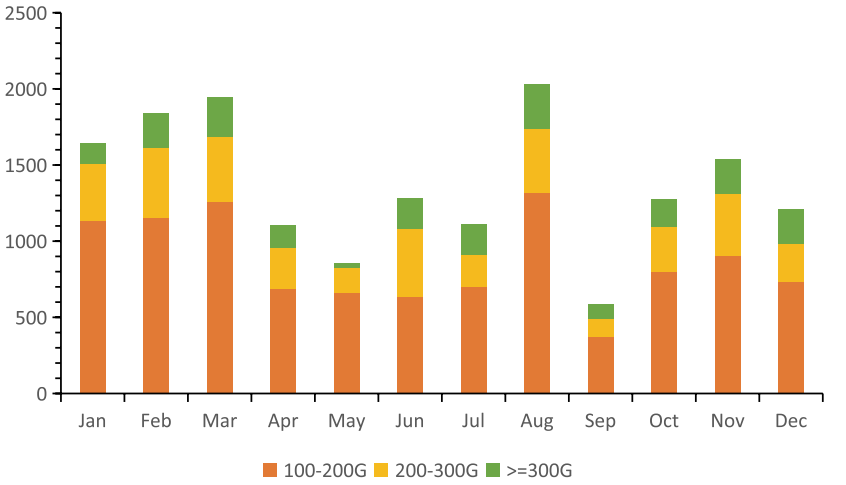

图 3.8　2021 年大流量攻击的次数变化

数据来源：中国电信安全公司

3.1.4　单次攻击最高和平均峰值

如图 3.9 所示，2021 年 1-3 月份，DDoS 攻击的平均峰值较 2020 年有明显的增长，同比增长了 59.07%、133.49% 和 89.87%。4-7 月份，与 2020 年同期基本持平，到了 8 月份，出

现下降，9 月份达到最低值，同比下降了 50.9%。从 10 月开始，又出现了回弹，在 11 月达到了全年最大值 64.21Gbps，同比增长 102.5%。

从最大攻击峰值来看，2021 年 DDoS 的最大攻击峰值较 2020 年有明显的增长，并且在 7 月份达到了全年的高峰值 1853Gbps，这也表明 DDoS 攻击者的攻击能力正在提高。

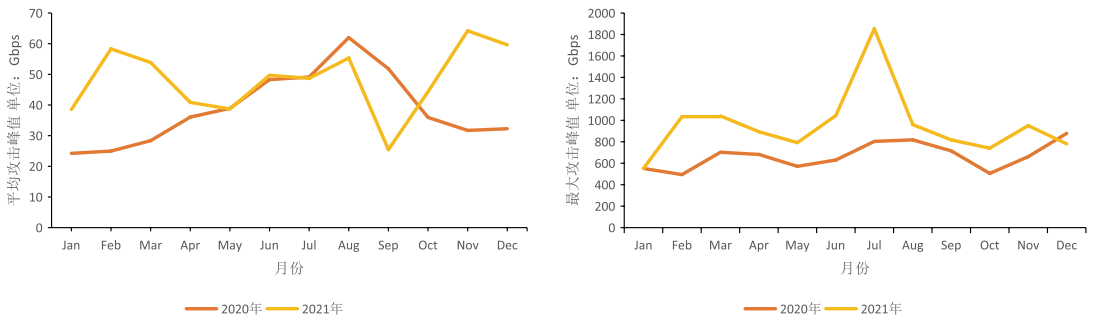

图 3.9　攻击平均峰值和最高峰值

数据来源：中国电信安全公司

从 2019 年至 2021 年，DDoS 平均攻击峰值虽然有波动，但是整体呈现出了增长趋势，在今年 11 月份，更是达到了三年中的最大值 64.21Gbps，如图 3.10 所示。从最高攻击峰值的变化趋势来看，整体也呈现出增长趋势，这也再次反映出 DDoS 攻击者的能力不断提高。

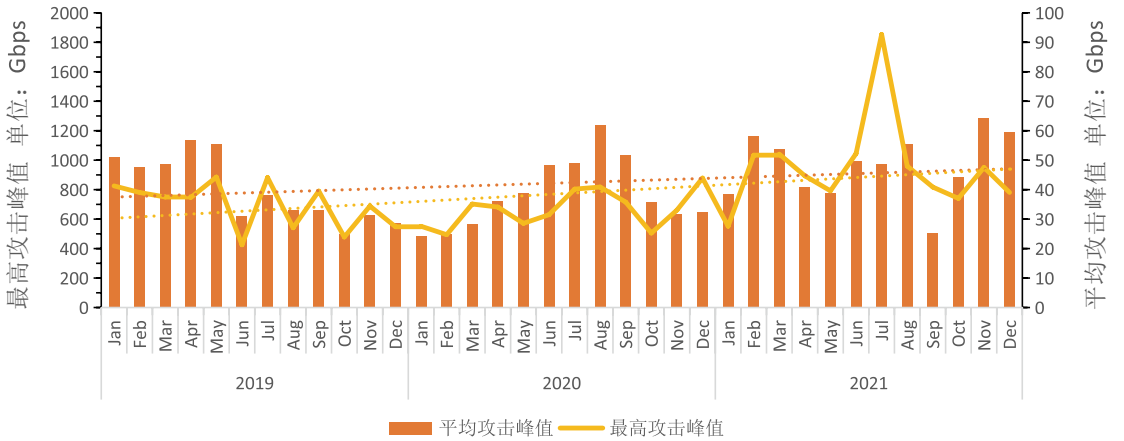

图 3.10　近三年 DDoS 攻击平均峰值和最高攻击峰值变化趋势

数据来源：中国电信安全公司

3.1.5 小结

近三年，在 DDoS 攻击次数和攻击流量持续下降的情况下，DDoS 单次平均攻击峰值和最高攻击峰值持续增长，2021 年大于 300Gbps 以上的超大型攻击次数更是大幅增长。这反映出 DDoS 攻击者能力不断提升，紧跟数字化发展的脚步，利用高网络带宽提升自身的攻击规模。

3.2 DDoS 攻击类型分析

3.2.1 攻击类型占比

2021 年，DDoS 攻击的主要类型仍然是 SYN Flood、NTP Reflection Flood 和 UDP Flood，攻击次数远远超过其他攻击类型，占总攻击数量的 83.8%，如图 3.11 所示。与 2020 年相比，SYN Flood 攻击显著增加，攻击次数和流量分别增加了 31.7% 和 63.58%；UDP Flood 攻击流量大幅减少，减少了 55.1%。

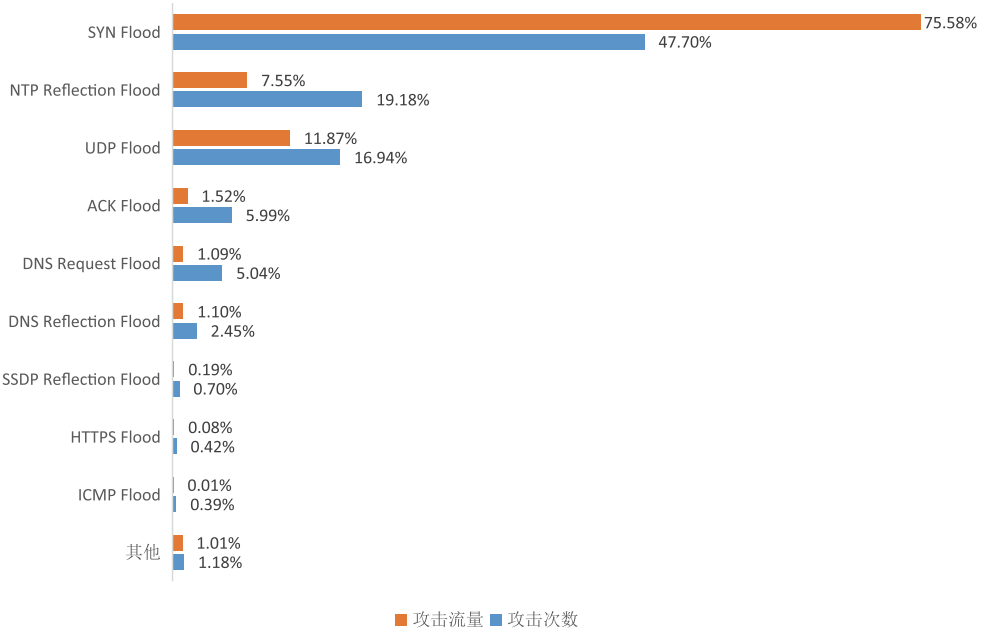

图 3.11 DDoS 攻击类型分布

数据来源：绿盟科技威胁情报中心（NTI）

2021 年混合多种类型的 DDoS 攻击次数大幅增加，较 2020 年增长了 80.8%。其中，采用 2 种类型的 DDoS 攻击增长了 104.6%，其他混合攻击的数量较 2020 年有所减少，如图 3.12 所示。一方面，攻击者会根据目标系统的具体情况灵活组合，发起多种攻击方式，利用协议、

系统的缺陷，尽其所能展开攻击。另一方面，在能够达到攻击目的的前提下，攻击者更倾向于采用较低的成本来发起攻击，以获得最大的收益。

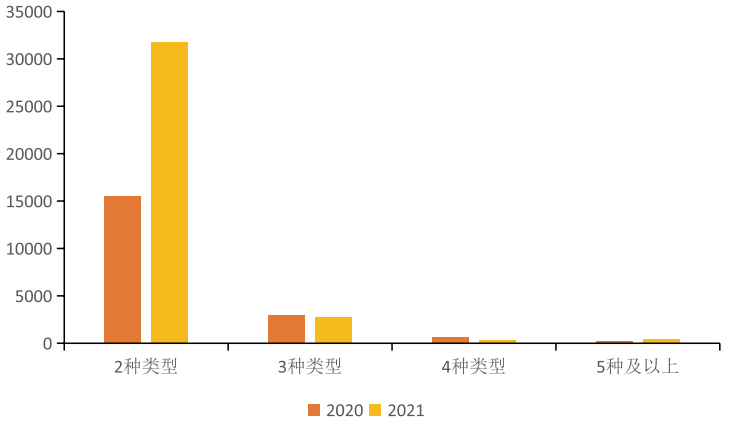

图 3.12　混合攻击分布

数据来源：绿盟科技威胁情报中心（NTI）

3.2.2　攻击类型各流量区间分布

从图 3.13 中看出，大部分的 DDoS 攻击流量小于 5G，在 5-50G 之间的中小型攻击主要包括 ACK Flood、UDP Flood、NTP Reflection Flood 和 SYN Flood，大于 50G 的大型攻击主要包括 ACK Flood、UDP Flood 和 SYN Flood。

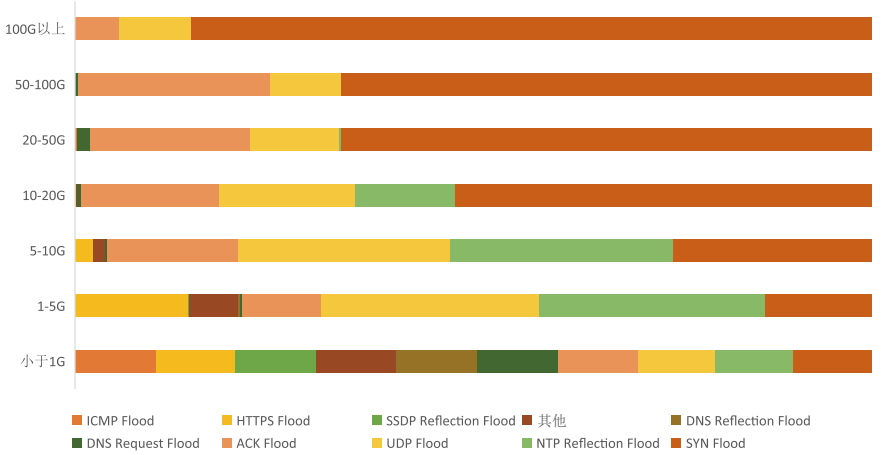

图 3.13　DDoS 攻击类型各流量区间

数据来源：绿盟科技威胁情报中心（NTI）

3.2.3 反射攻击

反射型 DDoS 攻击由于实现简单、效果显著，已成为 DDoS 攻击的主要手段之一。攻击类型仍然以 NTP、DNS 和 SSDP 反射攻击为主，总占比高达 90%，如图 3.14 所示。其中，NTP 反射攻击次数占比约 43%，远远超过其他反射攻击，这主要是由于 UDP 反射放大类型分布与协议的反射放大比直接相关，NTP 反射放大 400~500 倍，攻击效果显著。

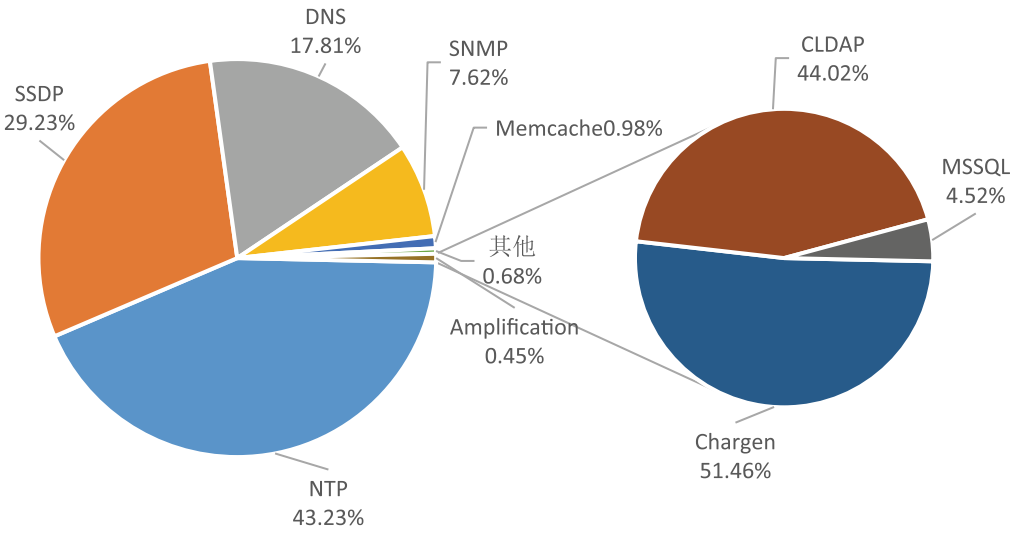

图 3.14 各类反射攻击类型分布

数据来源：绿盟科技威胁情报中心（NTI）

3.2.4 小结

2021 年攻击者仍然采用 SYN Flood、NTP Reflection Flood 和 UDP Flood 等主要方式发起 DDoS 攻击。其中，SYN Flood 攻击显著增加，成为攻击次数和攻击流量最多的 DDoS 攻击类型。其次是 NTP 反射攻击，由于能够放大 400~500 倍，攻击效果显著，攻击次数也较多。混合 DDoS 攻击大幅增长，较 2020 年增长了 80.8%，反映出 DDoS 攻击的复杂度不断提升。

3.3 DDoS 攻击时间刻画

3.3.1 DDoS 攻击持续时间占比

在 2021 年，攻击时长在 30 分钟以内的 DDoS 攻击占了全部攻击的 77.0%，如图 3.15 所示，较 2020 年减少了 3%。这种短时攻击仍是攻击者采用的主要攻击方式，主要是因为攻击

者越来越重视攻击成本和效率，倾向于在短时间内发起大规模攻击，耗尽服务器的资源，导致服务器瘫痪。

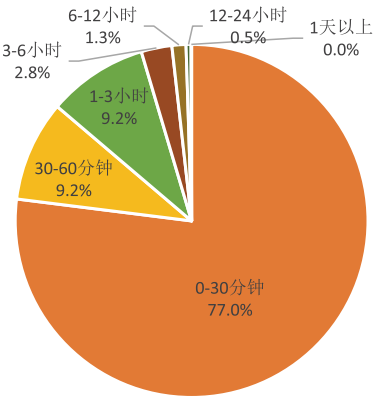

图 3.15　2021 年 DDoS 攻击持续时间占比

数据来源：中国电信安全公司

从各季度攻击持续时间来看，如图 3.16 所示。四个季度的 DDoS 攻击持续时间分布较稳定，无大的波动，90% 以上的攻击集中在 3 小时之内。

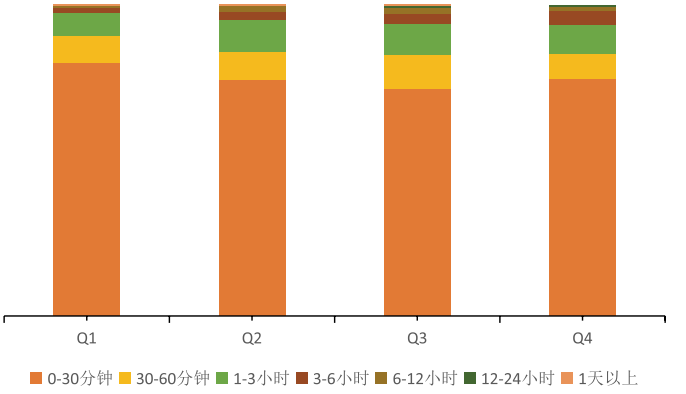

图 3.16　2021 年各季度 DDoS 攻击持续时间占比

数据来源：中国电信安全公司

3.3.2　一天中 DDoS 攻击活动分布

按天统计分析，DDoS 攻击呈现出了明显的时间特性，攻击活动的高峰时段主要集中在（10 点 -22 点），占全天攻击数量的 71.9%，与 2020 年的分布也是一致的，如图 3.17 所示。这

与一天当中的网络服务访问量有直接关系，10 点 -22 点是在线业务的访问高峰期，攻击者在这个时间段内发起 DDoS 攻击，更容易达到攻击效果。

图 3.17　一天 24 小时 DDoS 攻击占比

数据来源：中国电信安全公司

3.3.3　一周中 DDoS 攻击活动分布

按周统计分析，如图 3.18 所示， 2021 年 DDoS 攻击活动在周一到周六分布较平稳，并无明显的差异，周日的攻击数量依然相对少一些，与往年基本一致。

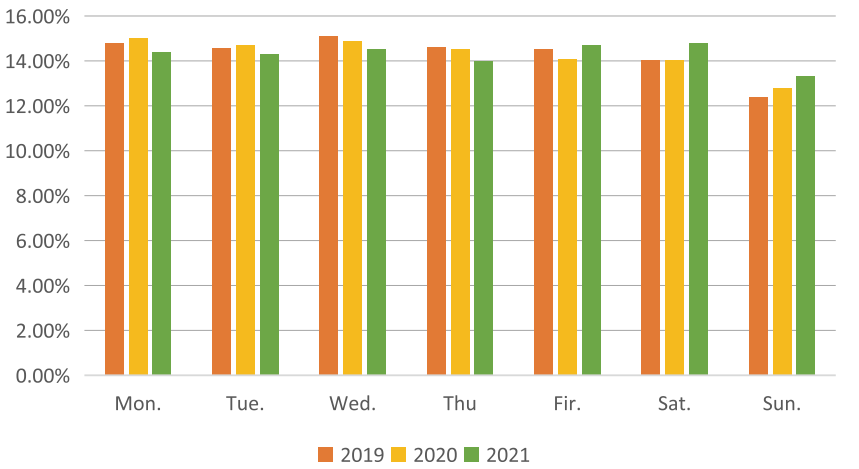

图 3.18　一周七天 DDoS 攻击占比

数据来源：中国电信安全公司

3.3.4 小结

2021 年在 30 分钟以内的 DDoS 短时攻击仍是攻击者采用的主要攻击方式，并且主要集中在每天的 10 点 -22 点，在线业务的访问高峰期。从每个季度来看，DDoS 攻击持续时间分布较稳定，无明显波动，70% 以上的攻击集中在 30 分钟之内。从每周来看，周一到周六的 DDoS 攻击数量分布较平稳，周日的攻击数量相对少一些。

3.4 DDoS 攻击地域分布

3.4.1 DDoS 受控攻击源地域分布

2021 年，参与 DDoS 攻击的境外 DDoS 受控攻击源数量排名前五的国家分别是美国、日本、德国、韩国和英国，如图 3.19 所示。

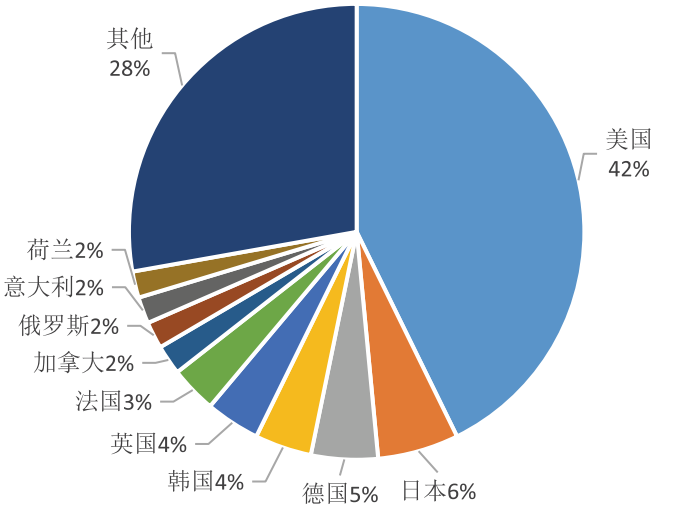

图 3.19 境外的 DDoS 受控攻击源数量占比分布

数据来源：绿盟科技威胁情报中心（NTI）& 中国电信安全公司

2021 年，参与 DDoS 攻击的位于我国境内的 DDoS 受控攻击源数目前三的省份分别是浙江、广东和江苏，占全国 DDoS 受控攻击源总量的 35.04%，这三个省份在近三年一直盘踞全国受控攻击源数量的前三名，如图 3.20 所示。

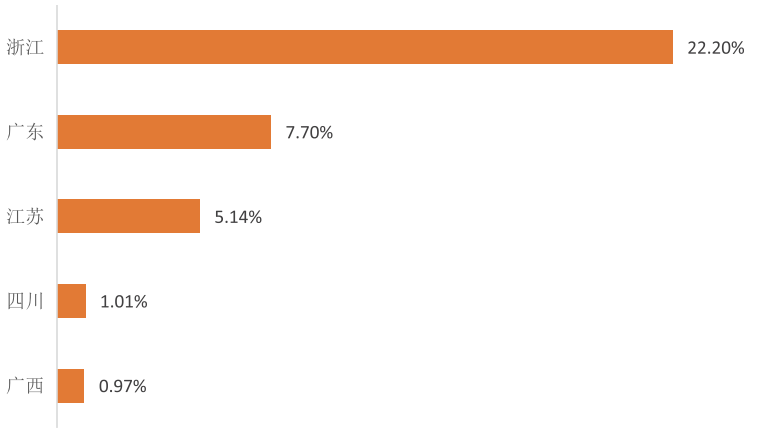

图 3.20　我国境内的 DDoS 受控攻击源数量占比分布

数据来源：中国电信安全公司

3.4.2　DDoS 攻击目标地域分布

全球遭受DDoS攻击较严重的前三名分别是中国、美国和欧盟，与2020年的分布基本一致。其中，受攻击最严重的国家仍是中国，占比高达72.3%，远远超过其他国家受攻击次数的总和，其次是美国，占全部攻击的14.0%，如图3.21所示。

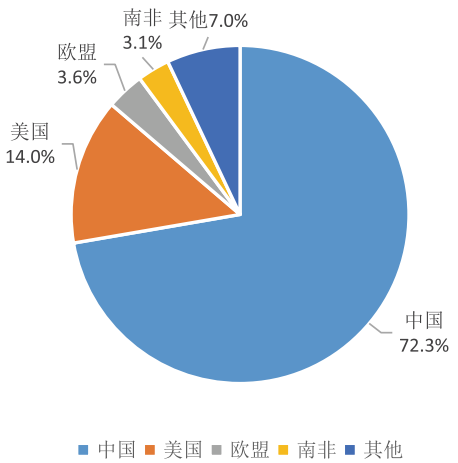

图 3.21　全球攻击目标 IP 分布比例

数据来源：中国电信安全公司

如图3.22所示，国内遭受DDoS攻击最多的省份是浙江，其他依次是福建、江苏和广东。东部沿海互联网发达地区仍然是被DDoS攻击的高危地区。

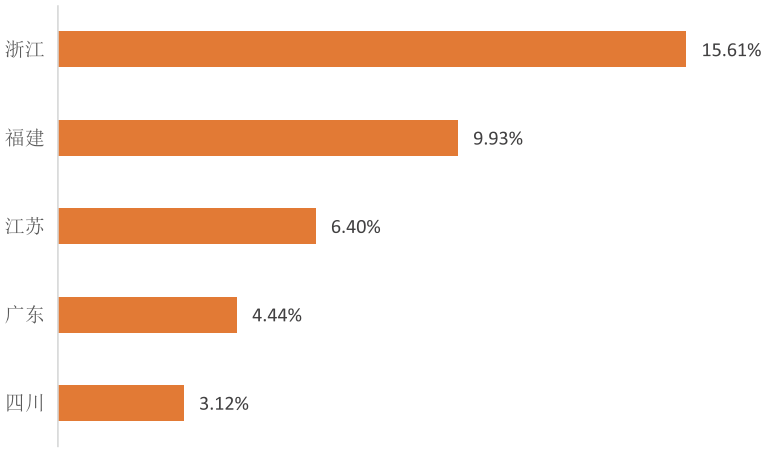

图 3.22　全国攻击目标 IP 分布比例

数据来源：中国电信安全公司

3.4.3　小结

参与 DDoS 攻击的境外受控攻击源数量最多的国家是美国，占比高达 42%。另外，同 2020 年，我国仍是遭受 DDoS 攻击最多的国家，占比为 72.3%，远远超过其他国家受攻击数量的总和，给我国的网络安全带来严重威胁。从国内看，受控攻击源主要分布在浙江、广东、江苏等互联网发达地区，同时这些地区也是被 DDoS 攻击的高危地区。

3.5　高活跃攻击资源分析

DDoS 攻击资源指发起 DDoS 攻击的网络资源 [1]，主要分为控制端资源、肉鸡资源、反射服务器资源等。然而，由于网络资源变化较快，大部分攻击资源的存活时间在 10 天以内，少量的攻击资源存活时间超过 10 天，存活时间较长的资源更容易被攻击者利用，威胁程度更高。因此，本报告进一步从资源活跃时间方面对高活跃资源进行研究分析，旨在为互联网环境威胁治理提供参考。

3.5.1　攻击资源活跃度分析

我们认为活跃时间达十天以上的攻击资源为高活跃度攻击资源，这些资源一般存在明显的安全隐患，极易被利用。如图 3.23 所示，2021 年攻击资源存活时间超过 10 天的占比为 7.0%，较去年下降了 4.0%。这主要是由于各种加密货币不断涌现，并且价格急剧上涨，攻击者也注意到了挖矿的丰厚收益，所以原来被长期控制的一部分设备纷纷加入“挖矿”，从中牟利。

[1]　CNCERT.《我国 DDoS 攻击资源分析报告（2021 年第 1 季度）》

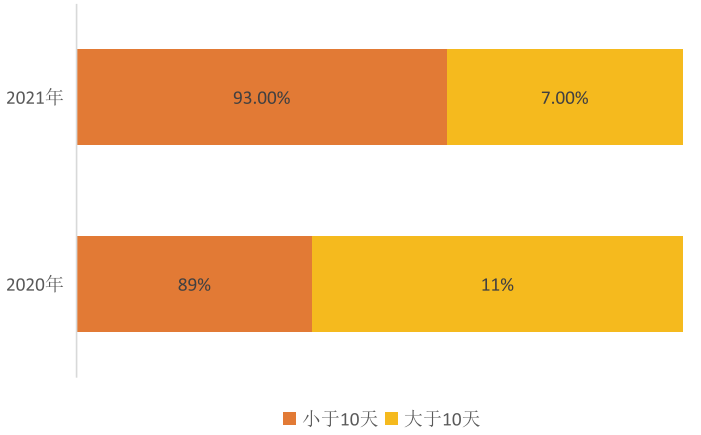

图 3.23　攻击资源活跃时间分布

数据来源：绿盟科技威胁情报中心（NTI）

3.5.2　高活跃攻击资源地域分布

2021 年，境外的高活跃度攻击源数量排名前五的国家分别是美国、英国、俄罗斯、日本和德国，如图 3.24 所示。

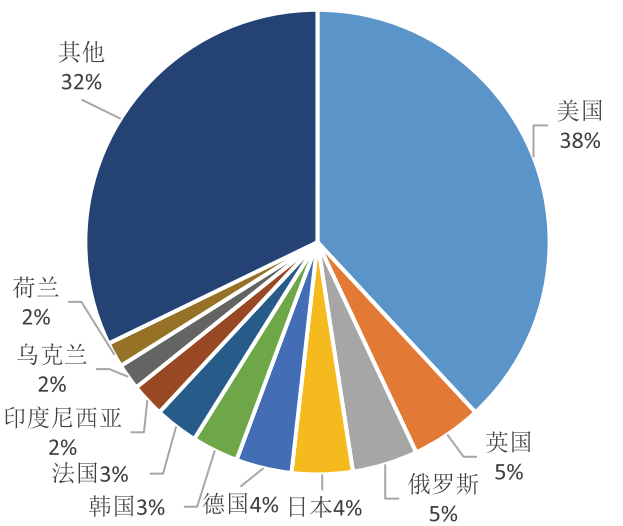

图 3.24　境外的高活跃度攻击资源数量占比分布

数据来源：绿盟科技威胁情报中心（NTI）

如图 3.25 所示，2021 年我国境内的高活跃度攻击资源数量最多的 10 个省市与 2020 年分布一致，主要集中在东南沿海或经济发达地区。浙江省超过台湾省，成为高活跃度攻击资源最多的省份，其次是广东省和山东省。

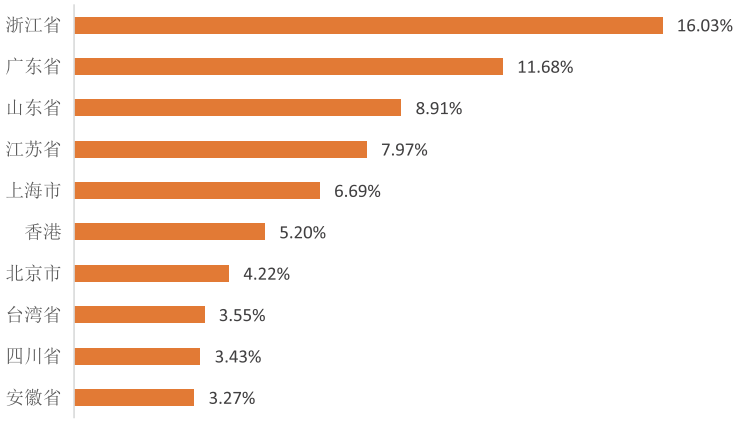

图 3.25　我国境内的高活跃度攻击资源数量占比分布

数据来源：绿盟科技威胁情报中心（NTI）

3.5.3　高活跃攻击资源恶意行为分析

为了统计高活跃资产被黑客利用参与恶意攻击的情况，将高活跃资产 IP 与绿盟威胁情报中心的情报数据进行关联。分析结果显示，大部分的高活跃攻击资源被用来发起 DDoS 攻击，6.5% 的高活跃攻击源被僵尸网络所控制，3.5% 的有过发送垃圾邮件行为，如图 3.26 所示。这些攻击资源活跃时间长，且长期存在安全风险，容易被攻击者利用。

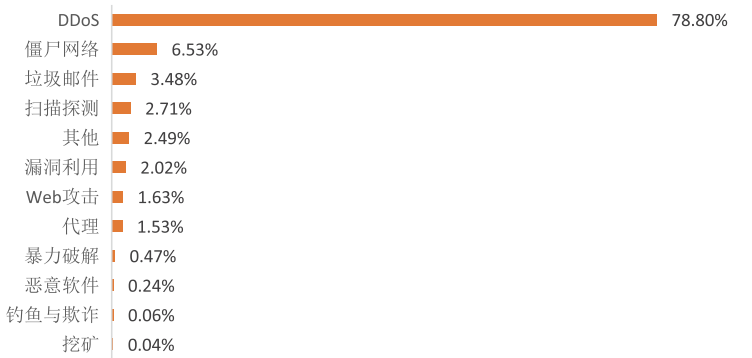

图 3.26　高活跃攻击源恶意行为类型占比

数据来源：绿盟科技威胁情报中心（NTI）

3.5.4 小结

2021 年高活跃资源数量较 2020 年下降了 4.0%，并且主要分布在互联网或经济发达地区。这些高活跃资源存活时间较长，更容易被攻击者利用。从参与的恶意行为来看，高达 75% 以上的高活跃资源被用来发起 DDoS 攻击，高活跃资源的安全隐患不容忽视。

3.6 物联网攻击资源分析

3.6.1 国内物联网资产暴露情况

为保证资产存活的准确性，采用 2021 年 11 月国内全网段的测绘数据进行统计分析。经过统计发现，国内有 201 万个物联网资产暴露在互联网上，相较于 2020 年共增加了 15 万，一方面是因为物联网资产暴露本身的增长，另一方面也与我们对设备指纹扩充有关。具体的暴露设备类型分布情况如图 3.27 所示，其中，摄像头、路由器、VoIP 电话数量分别位列前三。

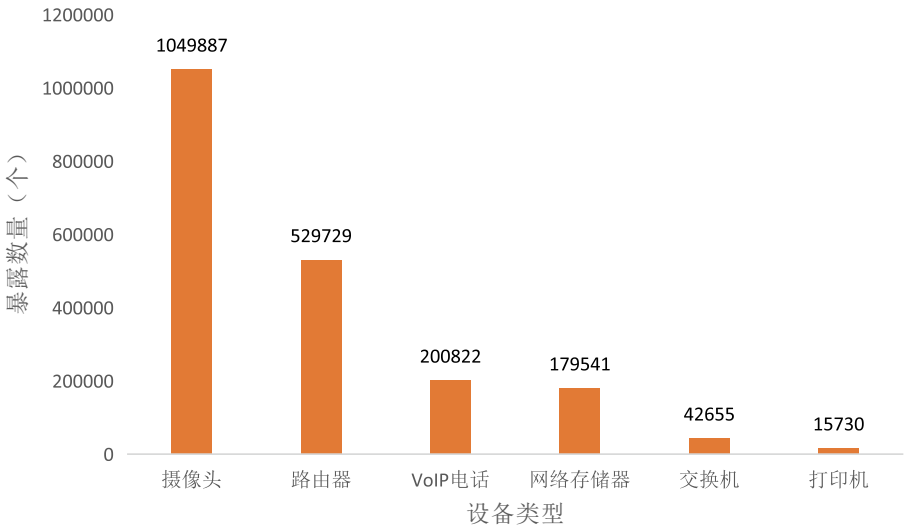

图 3.27 国内物联网资产暴露情况

数据来源：绿盟科技威胁情报中心（NTI）

3.6.2 异常物联网设备的 DDoS 参与度

为了统计暴露在公网的物联网设备被黑客利用参与恶意攻击的情况，将物联网设备 IP 与绿盟威胁情报中心的情报数据进行关联。分析结果显示，暴露在公网的物联网设备中，约有 37 万个设备参与了恶意攻击，占比约 18%。各种恶意攻击的分布如图 3.28 所示，其中参与 DDoS 攻击的设备数量最多，占比约 28.5%，与 2020 年持平。

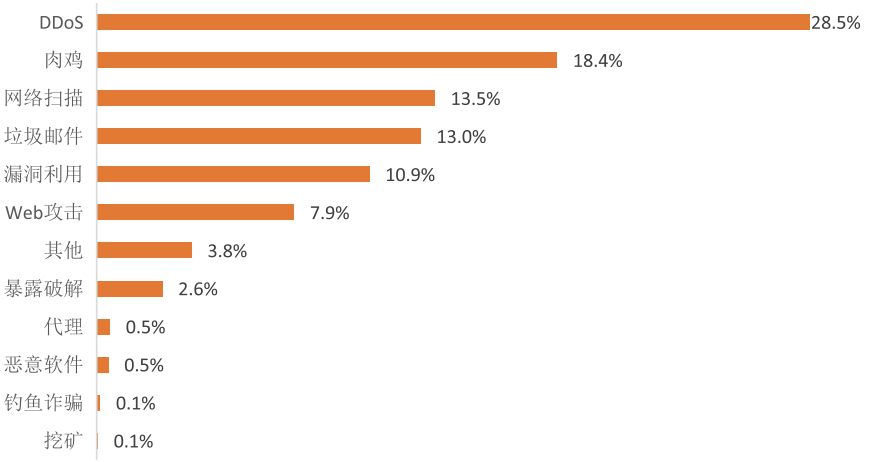

图 3.28　异常物联网设备攻击行为分布

数据来源：绿盟科技威胁情报中心（NTI）

3.6.3　参与 DDoS 攻击的物联网设备类型分布

从设备类型来看，参与 DDoS 攻击的物联网设备主要包括摄像头、VoIP 电话、路由器、网络存储器和打印机，如图 3.29 所示。其中，约 6 万台摄像头参与 DDoS 攻击，超过总攻击数量的一半，占比高达 54.8%。2021 年路由器参与 DDoS 攻击的数量较 2020 年增长了 13.6%，超过 VoIP 设备，成为参与 DDoS 攻击活动数量排名第二的设备。摄像头和路由器由于在互联网中暴露的基数大以及所具有的一些共性特征，决定了这两类物联网设备一直备受 DDoS 攻击者的青睐。VoIP 也是容易被利用的设备，2021 年参与 DDoS 活动的占比约为 13.2%。

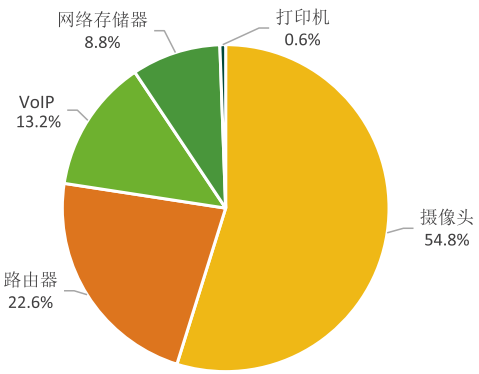

图 3.29　参与 DDoS 攻击的物联网设备类型分布

数据来源：绿盟科技威胁情报中心（NTI）

3.6.4 小结

2021 年暴露在互联网上的物联网资产较 2020 年共增加了 15 万，在这些设备中，约 18% 参与过恶意攻击。其中，参与 DDoS 攻击的设备数量最多，占比约为 28.5%，与 2020 年持平。物联网资产中的摄像头和路由器的安全问题尤为严重，参与 DDoS 攻击的数量占总量的七成以上。

3.7 DDoS 僵尸网络

3.7.1 僵尸网络家族攻击分布

绿盟科技 Bothunter 在 2021 年对僵尸网络家族中 15 个 DDoS 僵尸网络家族进行跟踪，从中发现 Dofloo、XorDDoS、Mirai、Gafgyt 家族攻击活动活跃度位列前四，攻击指令主要来自 8 个家族。到 11 月份共跟踪到 DDoS 攻击指令百万量级，其中攻击事件数量大约是攻击指令的六分之一，主要的 8 个家族攻击占比分布如图 3.30 所示。

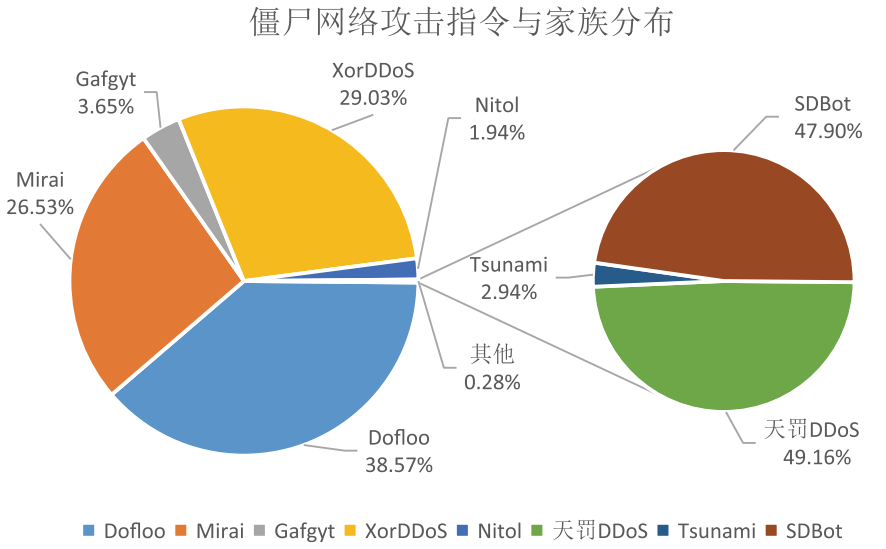

图 3.30 家族攻击事件数占比

3.7.2 僵尸网络家族活跃度分布

如图 3.31 所示，Mirai 家族在全年的整体活跃度较平稳，但其变种和感染速度最快。Dofloo 在 1 月份达到活跃高峰，在 9 月至 11 月活跃也较频繁。XorDDoS 在 5 月份达到活跃高峰，其余家族活跃度相对更低，尚且无法与 Mirai、Dofloo、XorDDoS 相提并论，但常一起参与攻击，可能是加入了 BaaS 组织。

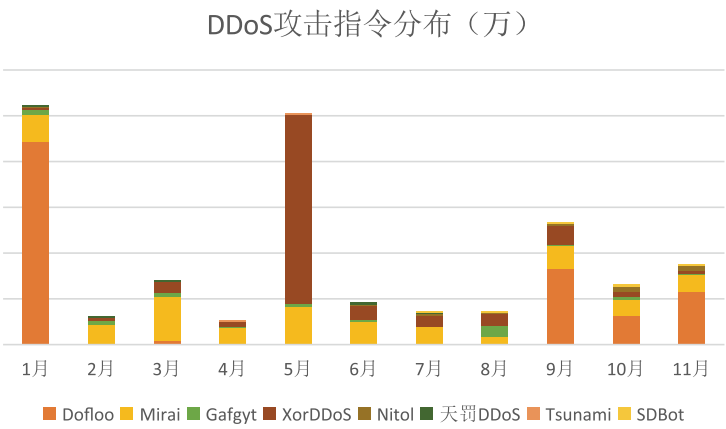

图 3.31　家族 DDoS 指令数占比

3.7.3　僵尸网络漏洞利用分布

DDoS 僵尸网络利用漏洞和弱口令扩张控制范围的势头愈演愈烈。分析发现，当前被僵尸网络利用的在野漏洞已达 72 种，最快在 1 天内集成最新漏洞，抢在设备漏洞修复前，感染并控制设备。路由器设备 WEB 管理端的命令执行漏洞是被利用最频繁的漏洞，漏洞被各家族利用的分布情况如表 3.1 所示。

表 3.1　DDoS 僵尸网络家族漏洞利用 TOP20

攻击事件使用 Linux/IoT 漏洞 TOP20 对应家族分布表	Gafgyt	hybridMQ	Mirai	Mozi	Persirai_shiina	tsunami	vbot	ZHtrap
CVE-2017-17215	1	1	1	1	1	0	1	0
CVE-2018-10561	1	1	1	1	1	1	0	0
CVE-2014-8361	1	1	1	1	1	1	0	1
Netgear_DGN1000_1_1_00_48_Setup_cgi_Remote_Code_Execution	1	1	1	1	0	0	0	1
Eir_D1000_Wireless_Router_WAN_Side_Remote_Command_Injection	1	1	1	1	0	0	0	0
JAWS_Webserver_unauthenticated_shell_command_execution	1	1	1	1	0	0	0	0
CVE-2015-2051	1	1	1	1	0	1	0	0
CCTV-DVR Remote Code Execution	1	1	1	1	0	0	0	1
ThinkPHP_5_X_Remote_Command_Execution	1	1	1	0	1	1	0	0

攻击事件使用 Linux/IoT 漏洞 TOP20 对应家族分布表	Gafgyt	hybridMQ	Mirai	Mozi	Persirai_shiina	tsunami	vbot	ZHtrap
ZyXEL_P660HN_T_v1_ViewLog_asp_privilege_escalation	1	1	1	0	1	0	0	0
D_Link_OS_Command_Injection_via_UPnP_Interface	1	1	1	1	0	0	0	0
CVE-2016-6277	1	1	1	1	0	0	0	0
Vacron_NVR_RCE	1	1	1	1	0	0	0	0
Seagate_BlackArmor_NAS_sg2000_2000_1331_Command_Injection	0	0	1	0	0	0	0	0
CVE_2021_20090	0	0	1	0	0	0	0	0
SAPIDO_RB_1732_Remote_Command_Execution	0	0	1	0	0	0	0	0
CVE_2021_35395	0	0	1	0	0	0	0	0
Linksys_E_series_Unauthenticated_Remote_Code_Execution	1	1	1	0	1	0	0	0
Common_Shell_Command_Abuse	1	1	1	1	1	0	0	1
D_Link_DSL_Devices_login_cgi_Remote_Command_Execution	1	1	1	1	1	1	0	0

3.7.4 小结

2021 年僵尸网络家族中 Dofloo、XorDDoS 和 Mirai 家族攻击活动活跃度位列前三，其余家族活跃度相对较低。同时，被僵尸网络利用的在野漏洞已达 72 种，最快在 1 天内集成最新漏洞，抢在设备漏洞修复前，感染并控制设备，DDoS 僵尸网络利用漏洞和弱口令扩张控制范围的势头愈演愈烈。

04

总结

全球数字化的快速发展给各行业带来机遇的同时，也对网络安全防护能力提出了更高的要求，网络安全是数字化发展的前提，更是数字化发展的重要保障。DDoS 攻击作为一种古老传统的网络攻击方式，经久不衰，对网络安全造成了严重威胁。攻击者更是利用数字化发展中的机遇来提升自身攻击能力，逐渐表现出攻击目标明确、攻击手段复杂、攻击规模扩大、攻击资源庞大等特征，给网络安全防护体系的建设带来了巨大挑战。然而，没有挑战就没有突破，在这场攻防两端博弈的大战里，唯有不断突破关键技术研发才能获得发展，才能提升对日益复杂化的 DDoS 攻击精准检测和高效防护的能力。

威胁情报实验室

聚焦威胁情报领域安全研究。研究方向包括：互联网空间测绘、全球恶意资产挖掘、黑客威胁动态跟踪等方向，为绿盟威胁情报解决方案及产品提供关键技术支撑。

伏影实验室

专注于安全威胁监测与对抗技术研究。研究目标包括 Botnet、APT 高级威胁，DDoS 对抗，WEB 对抗，流行服务系统脆弱利用威胁、身份认证威胁，数字资产威胁，黑色产业威胁及新兴威胁。通过掌控现网威胁来识别风险，缓解威胁伤害，为威胁对抗提供决策支撑。

绿盟威胁情报中心（NTI）

绿盟威胁情报中心（NSFOCUS Threat Intelligence center, NTI）是绿盟科技为落实智慧安全 3.0 战略，促进网络空间安全生态建设和威胁情报应用，增强客户攻防对抗能力而组建的专业性安全研究组织。其依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，推出了绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品，为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。

NSFOCUS绿盟科技

扫描绿盟科技官微二维码
可在手机端直接观看报告电子书