巨人背后的专家

2020
DDoS攻击态势报告

中国电信 CHINA TELECOM 云堤 SECURITY NSFOCUS

关于中国电信集团云网安全科技有限公司（云堤公司）

中国电信集团云网安全科技有限公司（云堤公司）是中国电信集团旗下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，整合中国电信云网、安全、数据等优势资源和能力，为客户提供云网安全、数据安全、信息安全等各类安全产品和服务。云堤公司前身是中国电信股份有限公司网络安全产品运营中心，成立于 2015 年 1 月，负责研发并运营 “云堤” 系列网络安全产品，主要包括：分布式近源防护架构的 DDoS 攻击防护平台、网站安全专家服务系统（云监控 + 云防护）、域名安全服务系统，反欺诈服务系统等。云堤平台通过国家等保三级测评，已为 8000+ 客户提供网络安全防护服务，并成为历次重大国事活动网络安全保障的首选网络安全防护平台，受到了客户及有关部门的高度认可。

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 日起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 40 多个分支机构 , 为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户 , 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、新加坡设立海外子公司 , 深入开展全球业务 , 打造全球网络安全行业的中国品牌。

版权声明

目录 CONTENTS

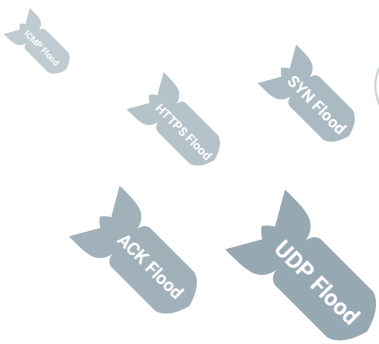
目录 CONTENTS

插图索引

目录 CONTENTS

1

執行摘要



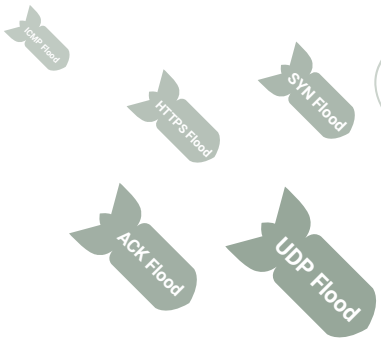
执行摘要

2020 年，得益于主管部门治理成效显著以及设备防护能力增强，我们监控到 DDoS 攻击次数相比 2019 年总量有所下降。但是在疫情期间的 DDoS 攻击有增无减，特别是医疗、政府、教育行业。1 到 4 月份是中国疫情最严重的时候，同时也是遭受 DDoS 攻击最频繁的时候，期间大部分的 DDoS 攻击都来自境外，美国是最大境外攻击来源国。5G 环境下的 DDoS 攻击带宽增加，中小型攻击替代小型攻击占主导地位，半数攻击峰值在 5-50Gpbs 区间。随着 HTTP2.0 的逐步应用， HTTP2.0 协议漏洞接二连三爆出，新协议带来了新的攻击威胁。DDoS 反射型攻击数量和反射源数量占比增加，新型反射攻击层出不穷。从攻击源 IP 看，中国是 DDoS 受控攻击源最多的国家。某国产品牌手机逾两千万部沦为”肉鸡”，移动终端不断沦陷，成为黑客的”帮手”。参与 DDoS 攻击的物联网设备占比相较去年有所提升，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。

本报告的第二章的是 2020 年的 DDoS 攻击态势概览。在第三章，本文从攻击次数、流量、攻击类型、时间、地域、行业等多个维度，以及从攻击资源、团伙性行为、物联网和僵尸网络四个视角，力求全面剖析 2020 年的 DDoS 的变化和演进，以便抛砖引玉，帮助各组织 / 机构持续改善自身网络安全防御体系及技术。

2

2020年DDoS攻击态势概览



2.1 2020 vs 2019

下降：攻击次数减少了 16.16%，攻击总流量下降了 19.67%

平均: 相比 2019 年攻击峰值向 1-5G 单侧分化，2020 年的攻击峰值在 5-50G 的各区间分布趋于平均，占全部攻击的 53.06%

持平：平均峰值为 38.64Gbps，和 2019 年同期的 40.05Gbps 基本持平

增长：反射攻击增长明显，占所有攻击类型的 34%

2.2 重要观点

观点一：2020 年 DDoS 攻击次数和总流量下降，国家主管部门 4 月 11 日开展的“净网 2020”专项治理效果明显。

观点二：受新冠疫情爆发的影响，二月份的 DDoS 数量激增，攻击势力主要来自境外，美国是最大境外攻击来源国。

观点三：5G 环境下的 DDoS 攻击带宽增加，中小型攻击替代小型攻击占主导地位。

观点四：DDoS 反射型攻击数量和反射源数量占比增加，新型反射攻击层出不穷，反射攻击防护需要及时更新。

观点五：新型 HTTP2.0 DDoS 攻击预警，CC2.0 时代即将到来。

观点六：攻击平均时长缩短，攻击成本不断下降。

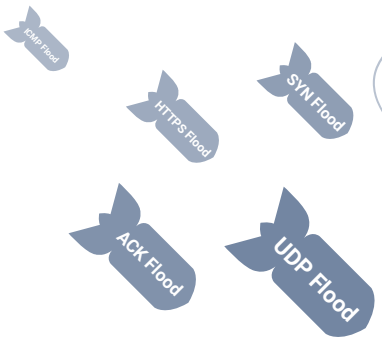
观点七：医疗、教育、政府行业疫情期间遭受 DDoS 攻击次数增长显著。

观点八：单一团伙的攻击总流量最高达到 3624TB，这个最大攻击总流量是去年的两倍以上。

观点九：我们监测到的 Mirai 和 Gafgyt 仍旧是当今世界范围内影响最大的两个 Linux/IoT DDoS 家族。

3

2020 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

2020 年 （截止 2020 年 12 月），我们监控到 DDoS 攻击次数为 15.25 万次，攻击总流量为 38.65 万 TB，与 2019 年同期相比，攻击次数减少了 16.16%，攻击总流量下降了 19.67%。 当然这未必是好消息，因为攻击次数和攻击流量减少最主要的原因是抗 D 设备检测和防护能力越来越强，防护及时有效，使得攻击者连续打击没有效果，所以提前结束攻击。另一部分得益于主管部门治理的结果，众所周知，黑灰产一直是 DDoS 中占比较高的攻击对象，而今年的“净网 2020”专项治理行动重点打击黑灰产业链。

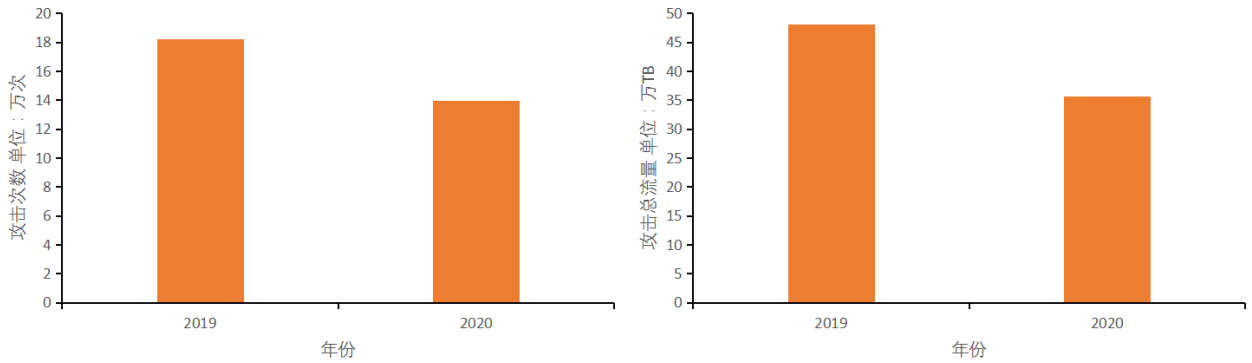


图 3.1 2020 年 DDoS 攻击态势

数据来源：中国电信云堤

我们统计了 2016 年至 2020 年的 DDoS 攻击次数和攻击流量，从历史趋势变化来看，在经历了 2017 年和 2018 年 DDoS 攻击大年后，2019 年和 2020 年似乎相对平静。但是平静不意味着祥和，在 5G 酝酿之际， IoT 设备和移动终端不断沦陷，新的流量源泉在暗自涌动，同时，伴随着 HTTP2.0 等新技术的发展，新型攻击手段也在暗自研制当中，从 DDoS 往年的攻击经验来看，当前的下降绝不是悄无声息的消失，未来可能会面临更大的高峰。

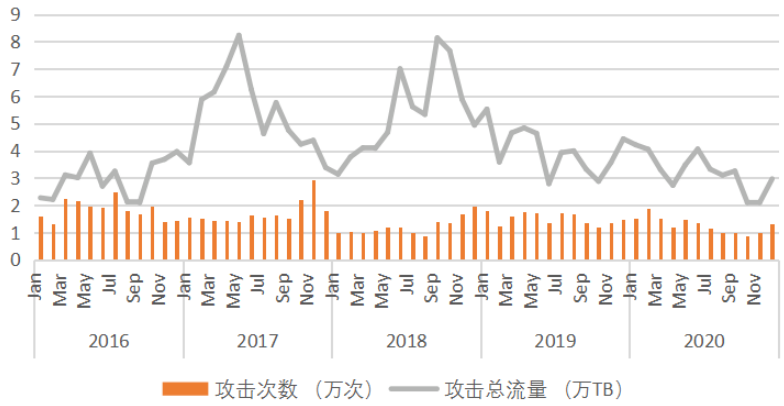
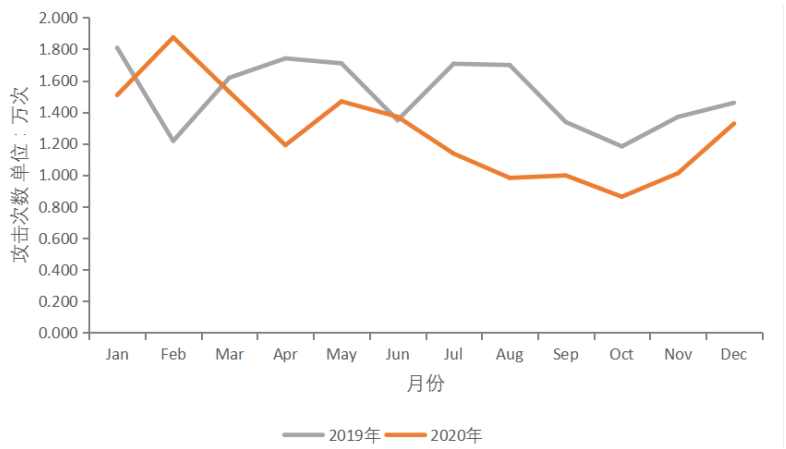


图 3.2　DDoS 多年攻击态势

数据来源：中国电信云堤

正如外交部发言人汪文斌 29 日说的一样，中国仍是网络攻击的主要受害者之一，在疫情期间遭受的网络攻击有增无减。

对于国内的 DDoS 攻击，从各月攻击次数来看，今年的 DDoS 主要集中在上半年，其中 2 月份为 14.5%，占比最高。要知道，往年的 2 月份都是 DDoS 最“消停”的时候，今年不降反增，并且成为全年攻击最高峰。这和新冠疫情的爆发脱不开干系。中国作为率先爆发新冠疫情的国家，很快在全球成为了众矢之的，使得国内 DDoS 数量激增。同时，人们当时的生产活动、娱乐消遣主要集中在线上，互联网娱乐行业之间的恶意竞争也容易导致 DDoS 增加。



2020 年 DDoS 攻击分析

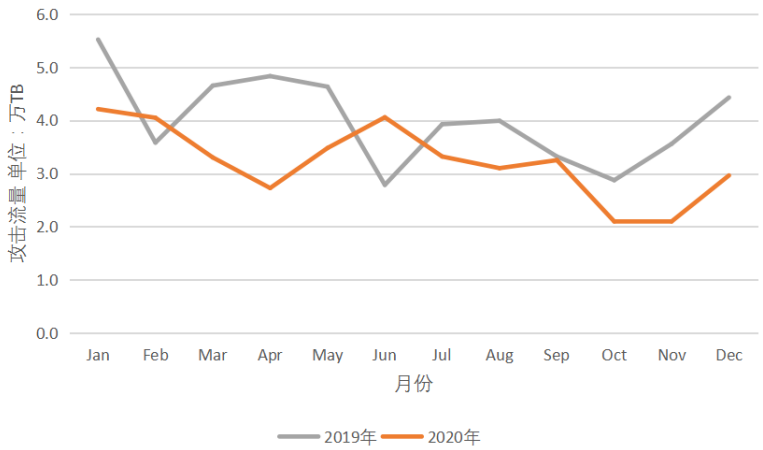


图 3.3　攻击次数与攻击流量

数据来源：中国电信云堤

上面的统计是从攻击事件的角度来看攻击态势，一次攻击事件通常由多个攻击源同时发起，规模有大有小。如果我们从攻击源的视角来看，把攻击来源区分为国内和国外分开统计，我们发现， 1-4 月份的攻击中，74.21% 的攻击都来自国外。美国是最大境外攻击来源国，攻击占比 24%。

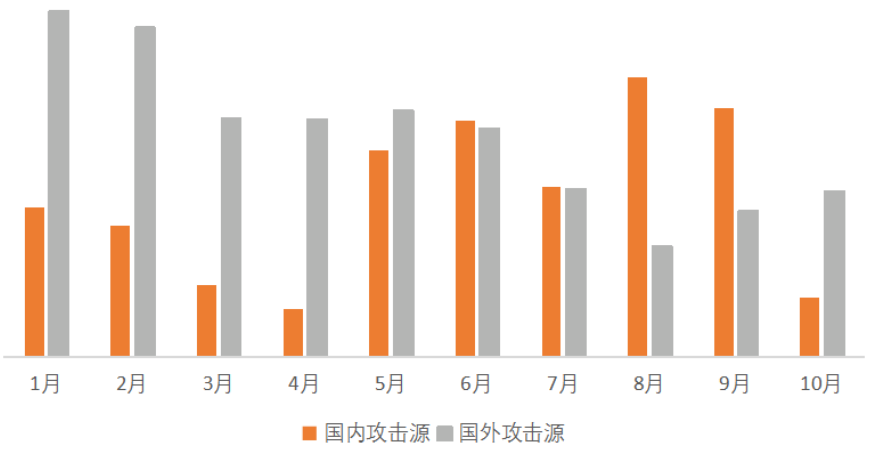


图 3.4　国内外攻击次数与占比

数据来源：中国电信云堤

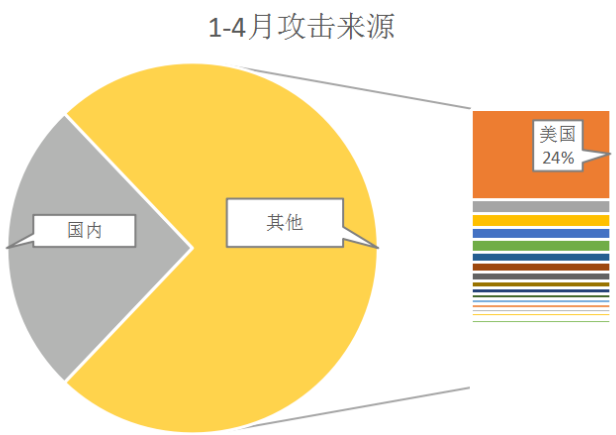


图 3.5　1-4 月攻击来源分布

数据来源：中国电信云堤

3.1.2　攻击峰值分布

在全部 DDoS 攻击中，18.16% 的攻击峰值在 5-10Gbps 之间，在所有区间中占比最高。不过，相比 2019 年攻击峰值向 1-5Gbps 单侧分化，2020 年的攻击峰值在 5-50Gbps 的各区间分布趋于平均，占全部攻击的 53.07%，5Gbps 以下的小规模攻击比例有所减少。专家分析，主要是因为 5G 网络的引入，设备可用带宽增加，同时这些也能被物联网僵尸网络所利用，使其执行 DDoS 的可用带宽大大增加。所以在 5G 环境下的 DDoS 整体攻击能力提高，对 DDoS 的清洗和防护都提出了更大的挑战。

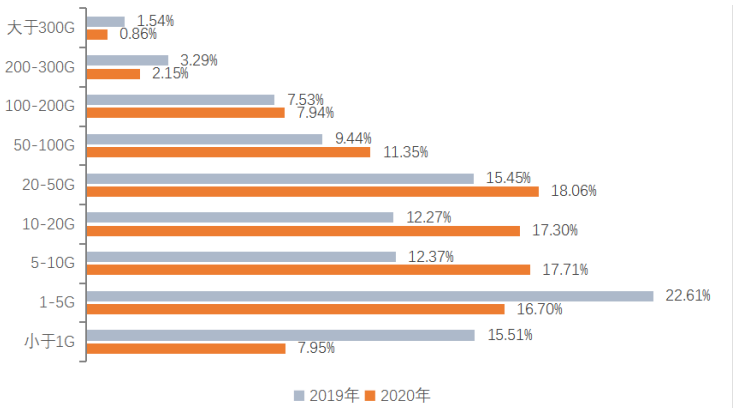


图 3.6　攻击峰值分布

数据来源：中国电信云堤

2020 年 DDoS 攻击分析

从各季度来看，DDoS 攻击峰值小于 5G 的小型攻击普遍减少，在 5-50Gbps 之间的中小型攻击持续增加，进入 Q4 后，中小型攻击在全部攻击中占比 58.4%，300Gbps 以上的超大规模攻击整体占比和绝对数量同时减少，截止 2020 年 12 月全年共发生了 1194 次，同比 2019 年的 2910 次减少 58.97%，整体占比从 2019 年的 1.54% 下降到 0.86%。由此也可以看出普遍黑客所掌控的攻击能力范围，小流量攻击打不死，打了没效果，而大流量攻击大多黑客掌控不了。

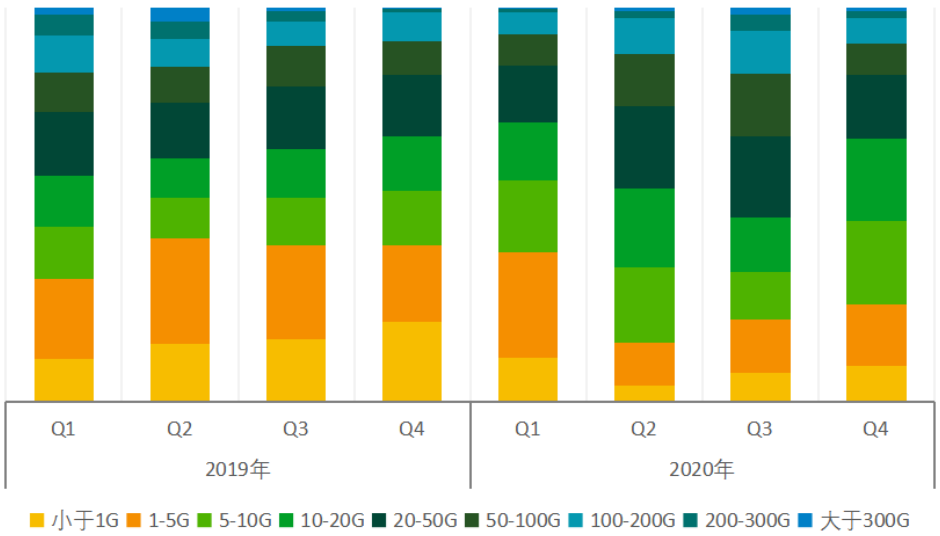


图 3.7　2019 年 vs 2020 年各季度各类规模攻击次数占比

数据来源：中国电信云堤

从最近三年各月数据来看，攻击峰值在 100Gbps 以上的大型攻击的次数在 2018 年和 2019 年连续两年在高位波动后，在 2020 年有明显下降。2020 年，100Gbps 以上的大型攻击发生了 1.59 万次（截止至 2020 年 12 月），与 2019 年同期的 2.28 万次（截止至 2019 年 12 月）和 2018 年同期的 2.2 万次相比，减少了 30.26%。攻击峰值在 300Gbps 以上的超大型攻击的次数从 2018 年平均每月 247 次小幅增长到 2019 年平均每月 262 次后，2020 年大幅减少到平均每月 93 次，减少了 64.5%。

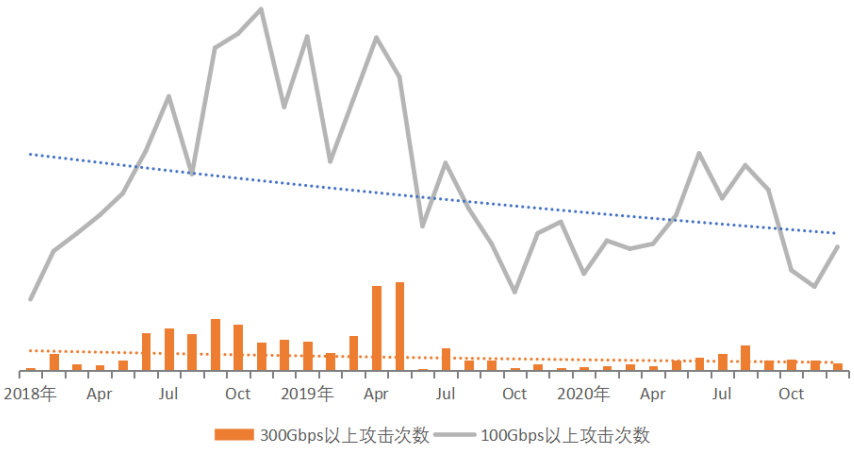


图 3.8　大流量攻击的次数变化

数据来源：中国电信云堤

单看 2020 年， 6、7、8、9 月份为大流量攻击高峰。6 月最高，占比 12.66%。

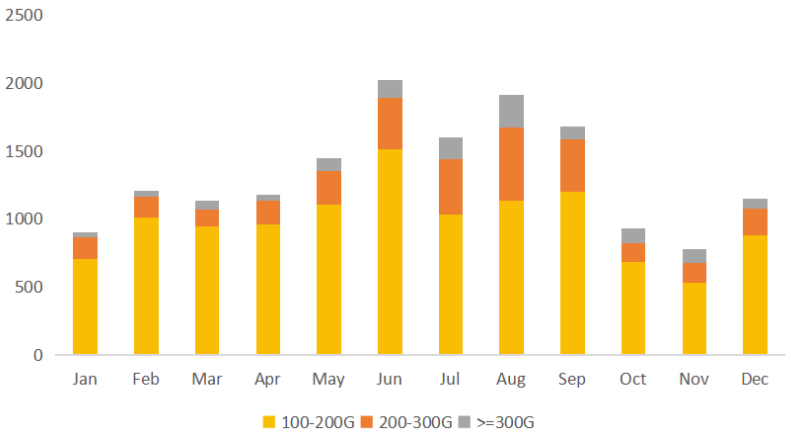


图 3.9　2020 年大流量攻击的次数变化

数据来源：中国电信云堤

3.1.3　单次攻击最高和平均峰值

截止 2020 年 12 月，DDoS 攻击的平均峰值为 38.64Gbps，和 2019 年同期的 40.05Gbps 差别不大，2020 年前半年 DDoS 攻击的平均峰值普遍低于 2019 年，在 6 月份之后 2020 年的 DDoS 攻击的平均峰

值普遍高于 2019 年。

从最大峰值来看，2020 年的最大峰值在 6 月份之前普遍低于 2019 年，6 月份之后和 2019 年同期相比出现交错的情况。2019 年的最高峰值 885Gbps 出现在 2019 年 5 月份，2020 年的最高峰值 878Gbps 出现在 2020 年 12 月份。

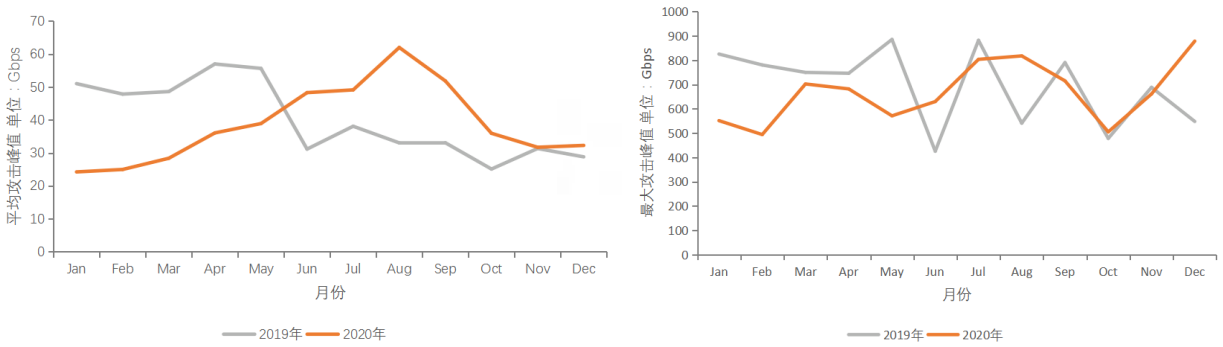


图 3.10　攻击平均峰值和最高峰值

数据来源：中国电信云堤

我们统计了从 2016 年至 2020 年的 DDoS 平均攻击峰值，从历史趋势变化来看，平均攻击峰值自 2018 下半年起已经进入了新的梯度。虽有波动，但依然维持在了较高的水平。

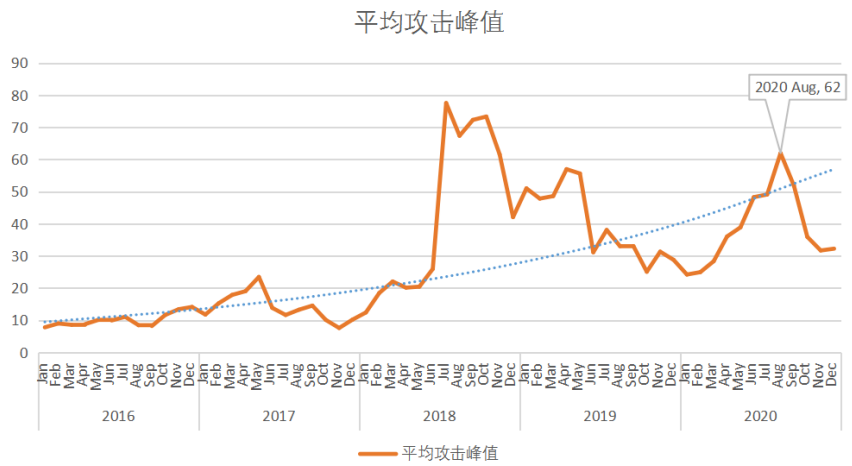


图 3.11　DDoS 多年攻击平均峰值变化趋势

数据来源：中国电信云堤

3.2 DDoS 攻击类型分析

3.2.1 攻击类型占比

2020 年，主要的攻击类型为 UDP Flood，SYN Flood，NTP Reflection Flood，这三大类攻击占了总攻击次数的 56%。UDP Flood 和 SYN Flood 依然是 DDoS 的主要攻击手法。值得关注的是，ACK Flood 由去年的攻击次数占比 14.9% 减少至 2%，NTP Reflection Flood 取代了去年 ACK Flood 排名第三的位置。

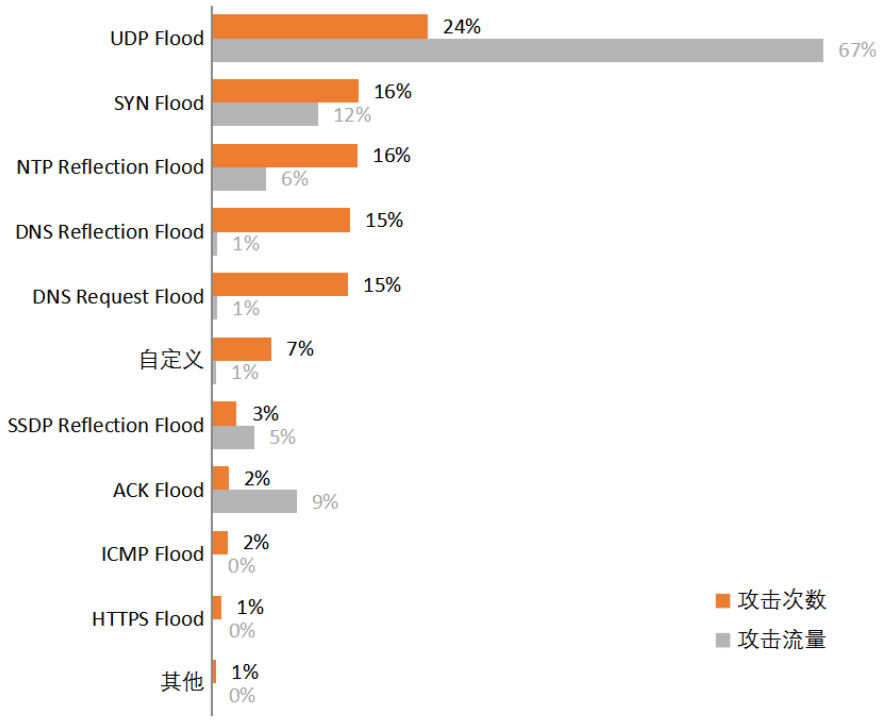


图 3.12 攻击类型的攻击次数分布

数据来源：绿盟科威胁情报中心（NTI）

从混合型攻击事件来看，相比 2019 年，2020 年混合多种类型的 DDoS 攻击事件数量有所增加。在实际攻击过程中，攻击者混合使用多种方式组合探测以求最佳攻击方式，利用协议，系统的缺陷，尽其所能展开攻击，达到最完美的攻击效果。

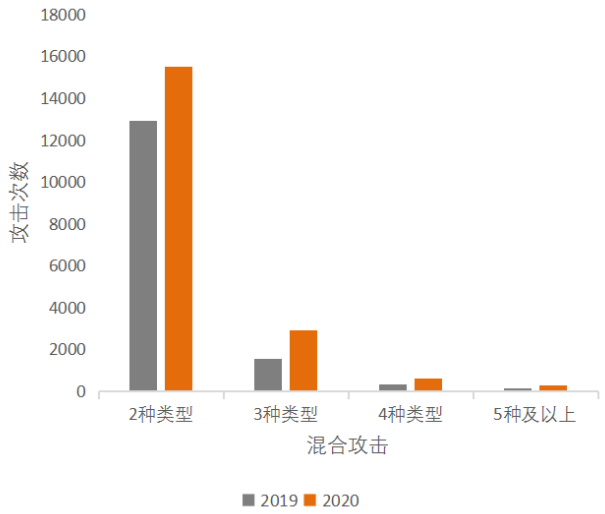


图 3.13　混合攻击分布

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

从攻击类型各流量区间占比来看，大流量攻击主要是 SYN Flood 和 UDP Flood。

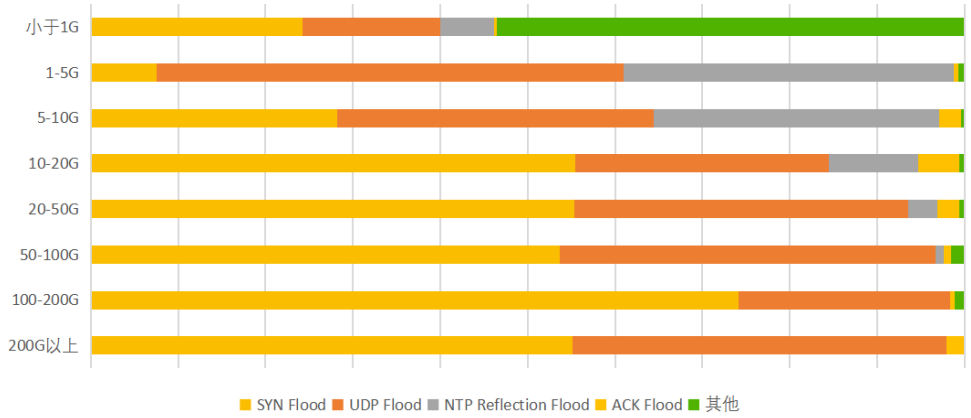


图 3.14　DDoS 攻击类型各流量区间

数据来源：绿盟科技威胁情报中心（NTI）

3.2.3 反射攻击

2020 年，反射类型的攻击次数占全部攻击的 34%。和 2019 年相比，反射类型的攻击次数增长较大，同时占比也比较大。2020 年主要的反射攻击类型为 NTP 反射攻击、DNS 反射攻击和 SSDP 反射攻击，其中，NTP 反射攻击在所有反射攻击中占主导地位，攻击次数占比 80%，攻击流量占比 53%。

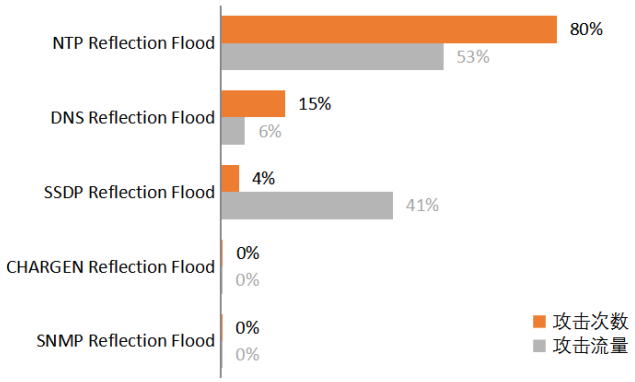


图 3.15 各类反射攻击次数与流量占比

数据来源：绿盟科技威胁情报中心（NTI）

从攻击源类型来看，反射源占比增加，2020 年中反射源数量占所有攻击源的 14%。众所周知，大部分反射源为 IoT 设备，随着 5G 和物联网的快速发展，IoT 设备增长迅速，与传统的单 IP 大流量攻击不一样，黑客利用控制的海量的 IoT 设备发起慢速攻击，每 IP 的攻击的频率和正常用户的范围频率保持一致，这使得传统的基于地理位置和限速的策略失效，因此需要多维度的检测算法区分攻击源和正常源。

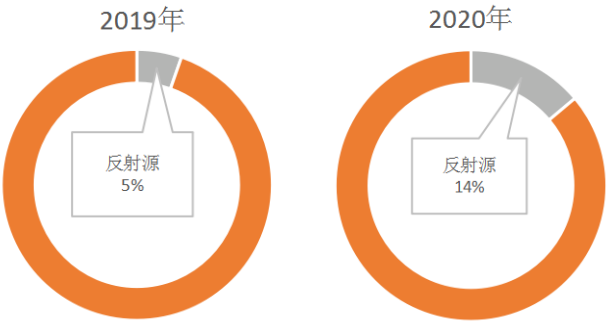


图 3.16 反射源数量占比

数据来源：绿盟科技威胁情报中心（NTI）

2020 年 2 月，AWS（亚马逊）声称遭遇了 2.3 Tbps 的大规模 DDoS 攻击，而此前记录的最大攻击是 2018 年的 1.7 Tbps，而针对 AWS 的攻击是基于 CLDAP 反射的攻击，一共持续了三天。

2020 年 10 月，Google（谷歌）披露，早在三年前（2017 年），Google 遭受到了攻击流量峰值高达 2.54 Tbps 的 DDoS 攻击，刷新了攻击记录。这次攻击同样是利用了互联网上的 CLDAP，DNS，SMTP 等服务器形成的反射攻击。反射攻击仍然是目前带宽消耗型 DDoS 攻击的主力军。众多知名大流量 DDoS 攻击事件中，都有反射攻击身影。

反射攻击仍在不断更新，从过去的 NTP 反射、SSDP 反射，近两年还出现了 TCP 反射、Memcached 反射等等。反射攻击不难防护，但这些新的反射攻击方法，需要 DDoS 技术相关的研发人员和运维人员，不断更新防护技术与策略以应对。绿盟抗 D 设备支持检测并防护各类已知、未知反射攻击。

3.2.4 新型攻击

新型攻击方法不断发现，DDoS 防御技术需要及时更新。

DNS 协议安全漏洞“NXNSAttack”可导致大型 DDoS 攻击

2020 年 5 月，以色列研究人员报告了一个新的 DNS 服务器漏洞，被称为”NXNSAttack”。这个漏洞是在 DNS 递归解析在实施过程中存在的，不同于直接以主机或服务为目标造成影响的 DDoS 攻击，NXNSAttack 的攻击目标是受害者的域名解析能力，它利用 DNS 递归解析器发起指向恶意 nameserver 服务器的 DNS 查询请求，恶意 nameserver 服务器返回特制响应包，导致 DNS 递归服务器向受害 DNS 服务器发送大量请求包从而拒绝服务，最大能导致流量增加 1620 倍。受害 DNS 服务器遭到攻击后，新的客户端无法找到连接到服务的 IP 地址，因此无法解析服务的主机名。相比于常见的随机域名攻击，这种新型攻击能够利用较少的资源达到同样的效果，同时攻击更加隐蔽，无法从域名的组成上分析出攻击特征。

RangeAmp 攻击

2020 年 5 月，中国研究人员发布了另外一种新型的 DDoS 攻击放大方法 (RangeAmp)，利用 HTTP 头部的 Range 字段发起恶意请求，可使 CDN（内容分发网络）和 CDN，或者 CDN 和目标服务器的流量最高放大几千甚至上万倍，从而导致带宽耗尽。这种利用漏洞型的攻击，传统的防护算法不再生效（302 跳转等），利用关键字匹配策略需要不断抓包分析，往往攻击已经发生很久了。绿盟抗 D 的智能防护可以自动学习正常流量特征，并提取攻击指纹，对异常未知的流量生成策略，自动拦截。

新型 HTTP2 DDoS 攻击预警，CC2.0 时代即将到来

DDoS 是依赖于网络协议存在的，网络协议的普及率越高就越容易受到攻击，每增加一层网络协议，都会为 DDoS 攻击者提供一个新的攻击维度，网络协议越复杂，潜在的 DDoS 攻击方式就越多。随着 HTTP2.0 的逐步应用，新协议带来了新的 HTTP 攻击威胁。HTTP2.0 协议漏洞接二连三爆出，越来越多研究指出，不同于过去的 CC 攻击，基于 HTTP2.0 的新型 CC 攻击、慢速攻击有更大的危害，对业务服务器性能消耗有更明显作用。并且除了传统的 CC 和慢速攻击，HTTP2.0 协议还引入了新型攻击，例如基于控制帧的洪水攻击和基于控制帧的慢速攻击，以及 HTTP2.0 的头部压缩攻击，此类攻击已有多个 CVE 记录。根据 MY SSL 数据显示，国内已有 65.8% 的网站支持 HTTP2.0 协议，预计 2021 年国内将出现更多基于 HTTP2.0 的 DDoS 攻击。HTTP2.0 的攻击方式多样，靠单一防护方案往往不能达到很好的防护效果，所以需要一个多层次的防护方案，绿盟 ADS 将于 2021 年新版本支持基于 HTTP2.0 协议的 DDoS 攻击防护。

这些新型的攻击方法，需要 DDoS 技术相关的研发人员和运维人员，不断更新已有技术和策略，来应对这些新型攻击。

3.3 DDoS 攻击时间刻画

3.3.1 DDoS 攻击持续时间占比

2020 年，DDoS 攻击的平均时长为 42 分钟，和 2019 年相比，下降了 21%。我们检测到，2020 年，持续时间最长的 DDoS 攻击在 13 天左右，远远大于前期的攻击时长。

2020 年，攻击时长在 30 分钟以内的 DDoS 攻击占了全部攻击的 80%，与 2019 年的 75% 相比提升了 6%，这种短时攻击的高占比说明攻击者越来越重视攻击成本和效率，倾向于在短时间内，以极大的流量导致目标服务的用户掉线、延时和抖动。同时，僵尸网络即服务（Botnet-as-a-Service）和 DDoS 即服务（DDoS-as-a-Service）的流行也是重要原因之一，平台用户只要付款就可以即时获得一批佣兵式的攻击资源，可以在短时间内发起大规模攻击。[1] 在长周期内，多次瞬时攻击能够严重影响目标服务质量，同时攻击成本得到有效控制。

1 http://blog.nsfocus.net/gafgy-botnet-baas/

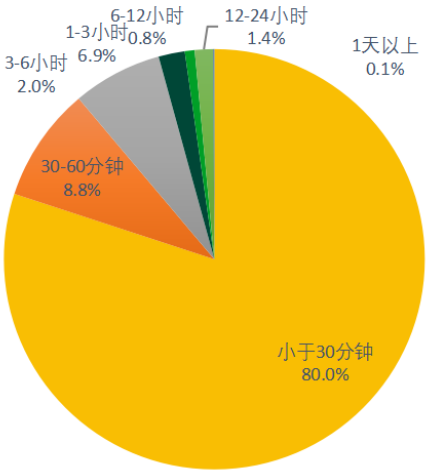


图 3.17　攻击持续时间占比

数据来源：中国电信云堤

3.3.2　一天中 DDoS 攻击活动分布

从一天 24 小时攻击占比可知，业务高峰时段（10 点 -22 点），为攻击者发起 DDoS 攻击的高峰期，占全天攻击的 73.4%。这段时间也是在线业务的访问最高峰区间，攻击者在访问高峰期发起 DDoS 攻击，以此来提升攻击的效果和影响。

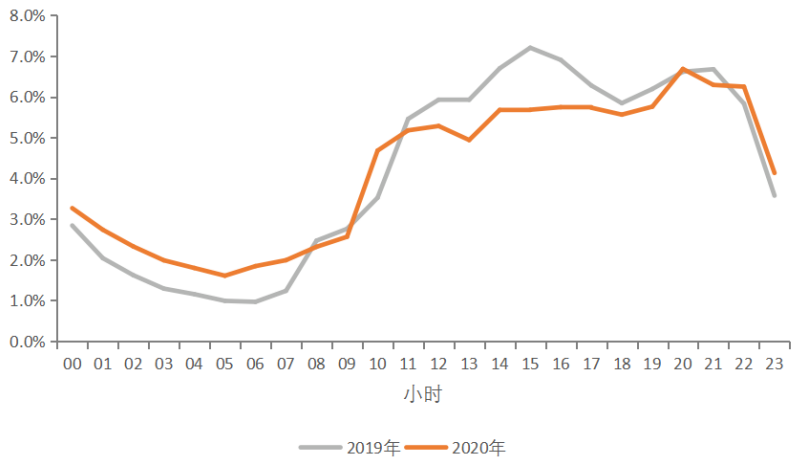


图 3.18　一天 24 小时 DDoS 攻击占比

数据来源：中国电信云堤

3.3.3 一周中 DDoS 攻击活动分布

从每周中 DDoS 攻击活动的分布来看，一周中各天所发生的 DDoS 攻击事件比例并无明显差别。背后的一个重要原因是现有网络服务往往提供 7 X 24 服务，因而一周中每一天都可能被攻击。周日依然是相对平静的一天。

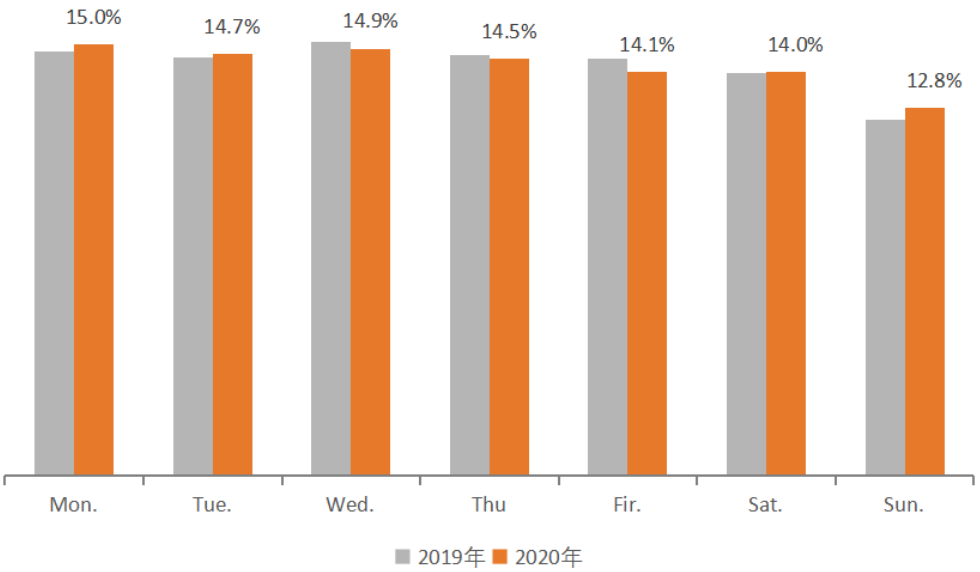


图 3.19 一周七天 DDoS 攻击占比

数据来源：中国电信云堤

3.4 DDoS 攻击地域分布

3.4.1 DDoS 受控攻击源地域分布

经统计，2020 年中国是 DDoS 受控攻击源最多的国家，占比为 59.7%，其次是美国和俄罗斯，占比分别为 7.8% 和 3.4%。

2020 年 DDoS 攻击分析

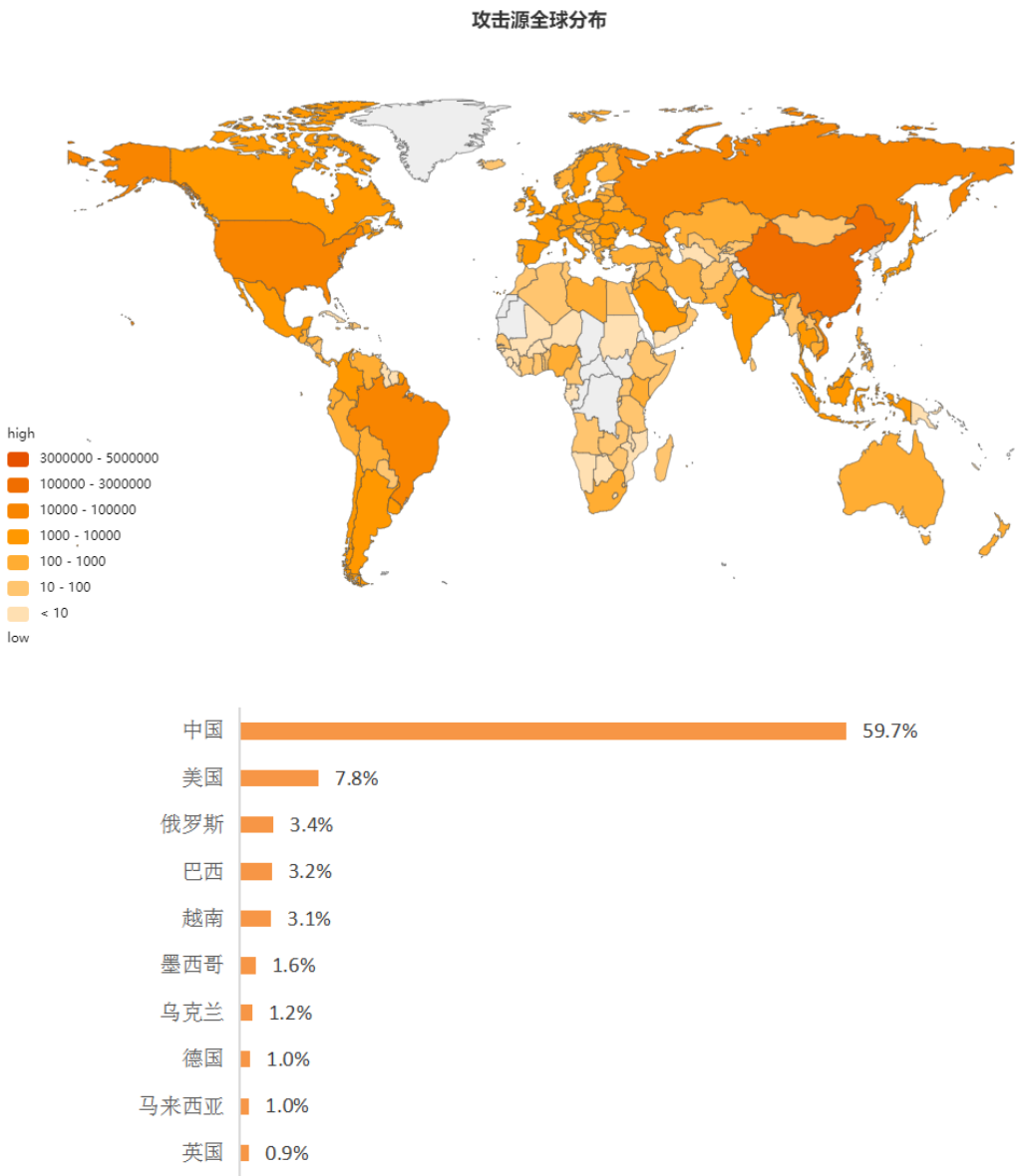


图 3.20　全球攻击源 IP 分布比例

数据来源：中国电信云堤

2020 年，国内 DDoS 受控攻击源数目前三的省份是浙江、江苏、广东，占全国 DDoS 受控攻击源总量的 59.7%。

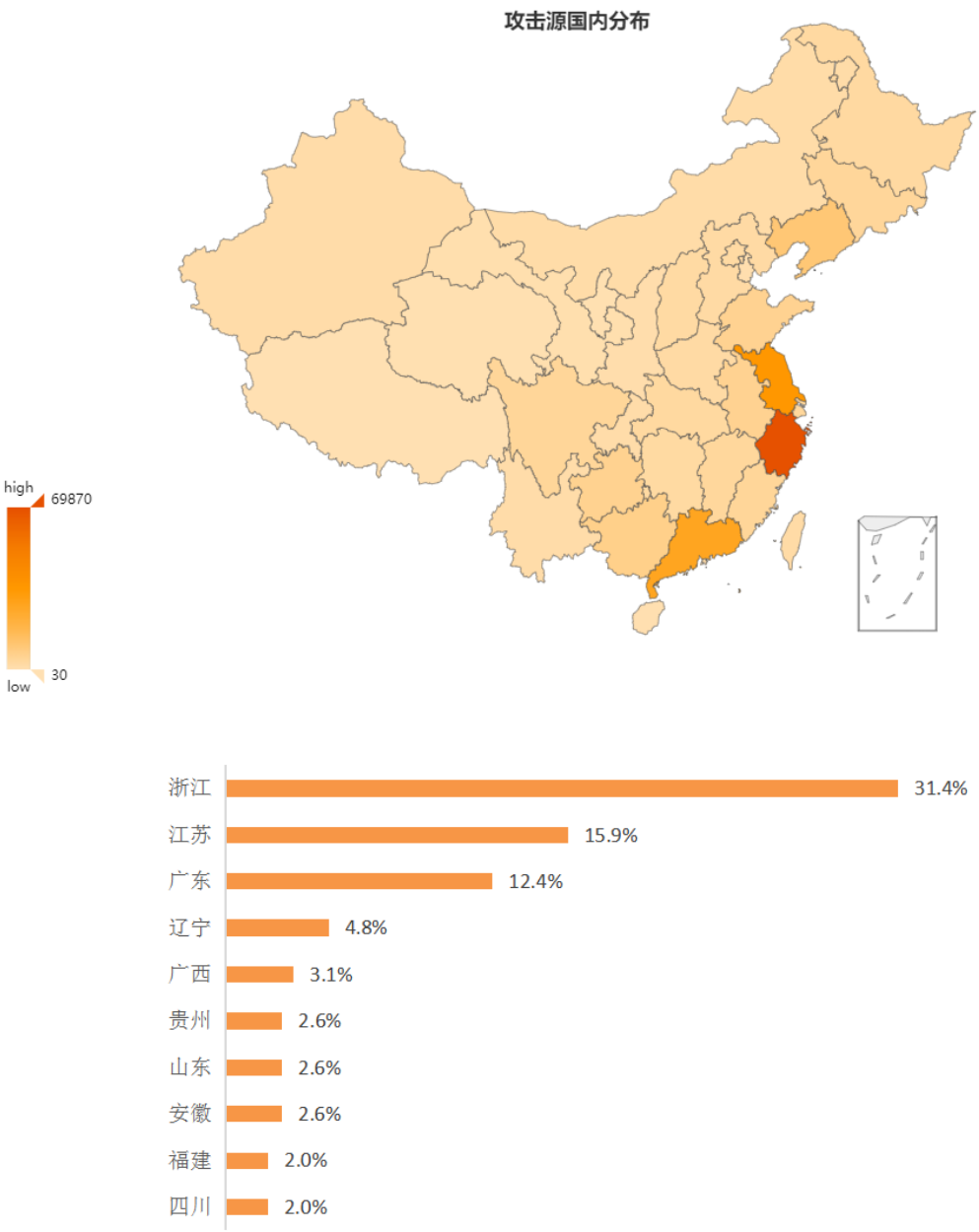


图 3.21　全国攻击源 IP 分布比例

数据来源：中国电信云堤

3.4.2 DDoS 攻击目标地域分布

2020 年，受攻击最严重的国家是中国，约占全部攻击国家的 70.7%；其次是美国，占全部攻击的 12.7%。

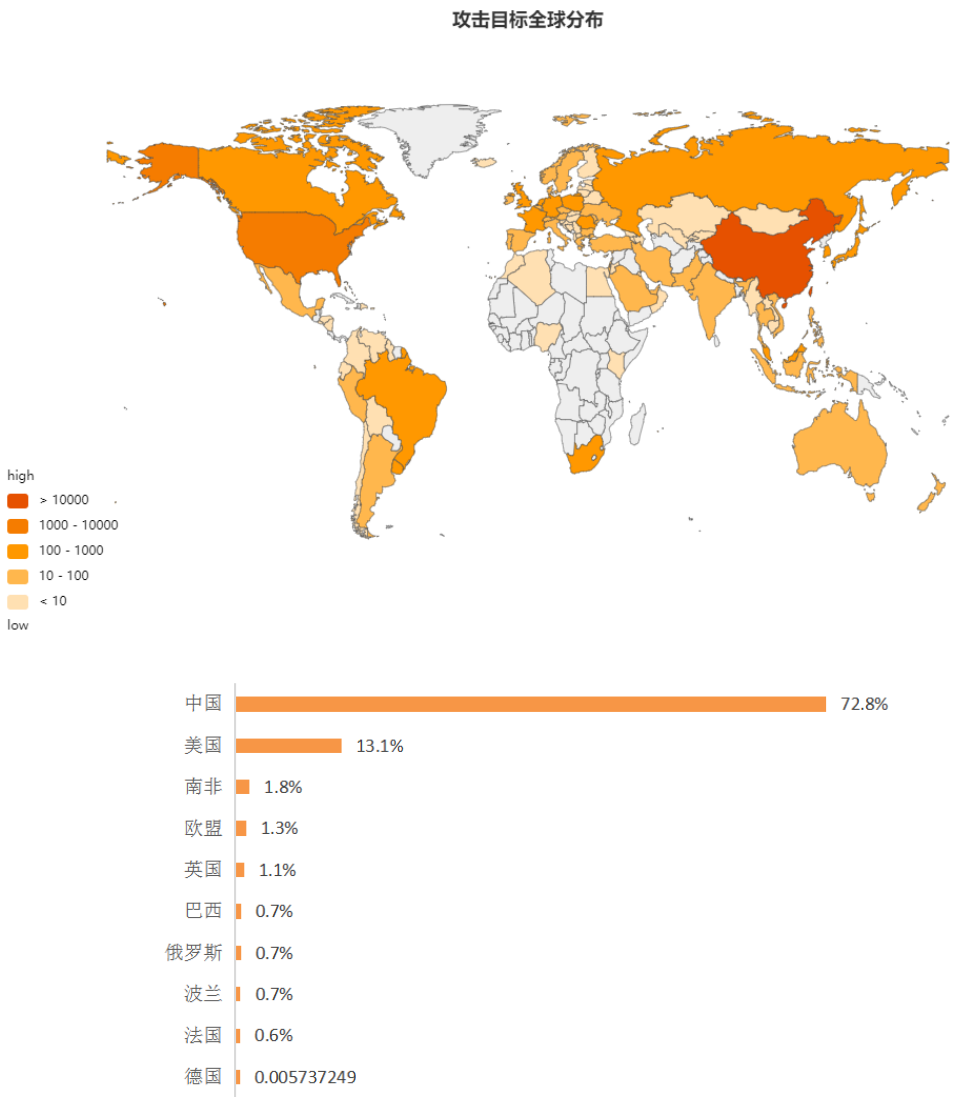


图 3.22 全球攻击目标 IP 分布比例

数据来源：中国电信云堤

在国内，江苏成为受 DDoS 攻击最多的省份，其它依次是广东、浙江和香港。东部沿海依然是被 DDoS 攻击的高危地区。

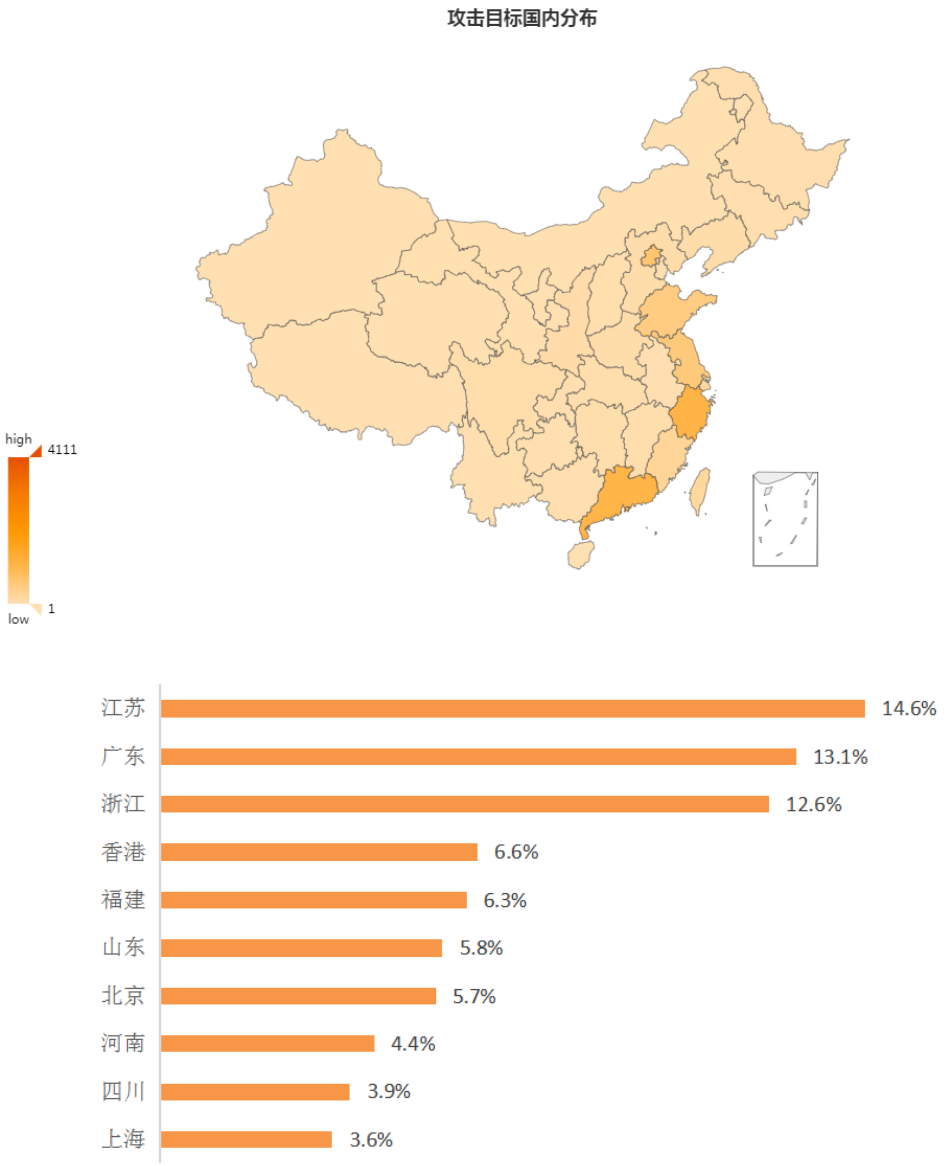


图 3.23　全国被攻击目标 IP 分布比例

数据来源：中国电信云堤

3.5 DDoS 攻击行业分析

医疗行业在疫情期间遭受的 DDoS 攻击有增无减。数据显示，2020 上半年被攻击次数普遍高于 2019 年同期，三月和四月为攻击最高峰，之后逐月递减。7 月之后的 DDoS 趋势和去年基本保持一致，且稍稍减少。

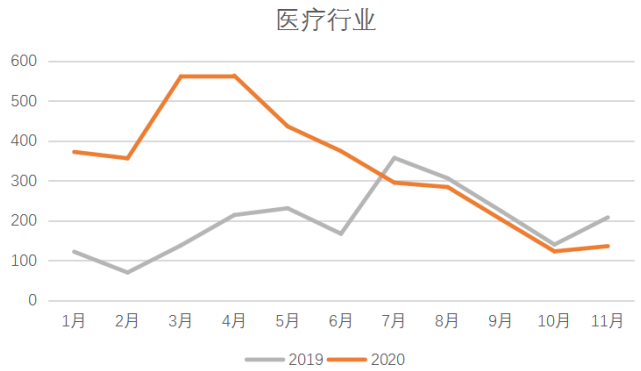


图 3.24 医疗行业被攻击次数态势

数据来源：中国电信云堤

除了医疗行业，政府和教育行业的 DDoS 态势也有相同趋势。稍有不同的是，在下半年，DDoS 下降的趋势更加明显，政府机关相对去年明显下降主要得益于净网治理。而教育行业主要是因为下半年学生开学，不再依赖于线上教学。

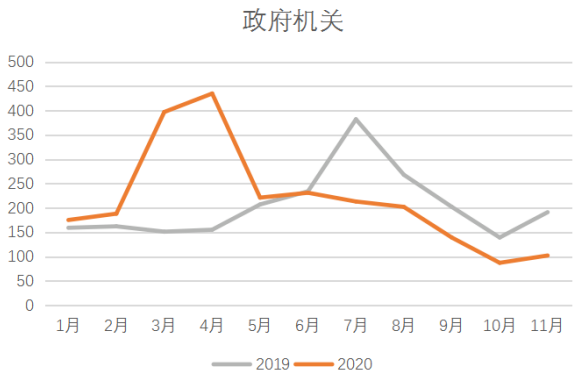


图 3.25 政府机关被攻击次数态势

数据来源：中国电信云堤

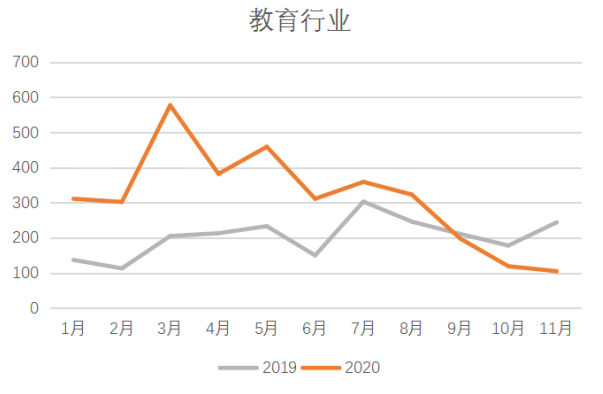


图 3.26　教育行业被攻击次数态势

数据来源：中国电信云堤

3.6　攻击资源行为分析

3.6.1　攻击资源活跃度分析

在攻击源活跃时间的监测中发现，和 2019 年趋势一致，存活时间大于 10 天的攻击资源占比 11%。像这种能够长期被控制的肉鸡大部分都是物联网设备，物联网设备大都存在设备系统老，人员维护少，更新慢等问题。一旦被感染，就会成为僵尸网络中的一员，并且长期被控制。

图 3.27　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）

高活跃度资源类型

高活跃度资源物联网设备占比 22%，相比去年占比提高了 10 个百分点。

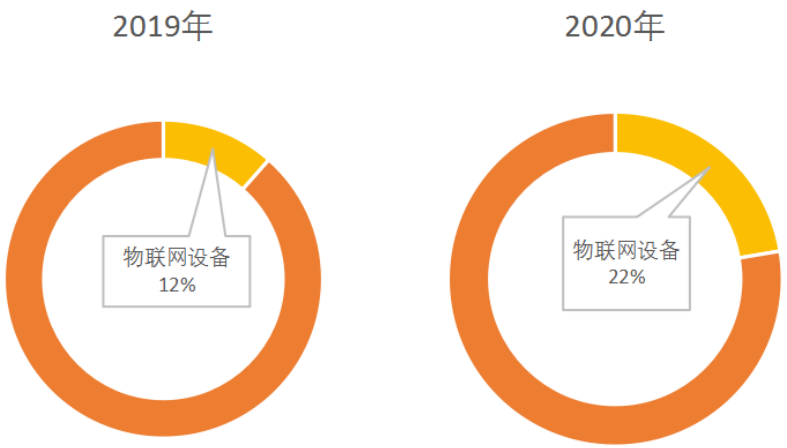


图 3.28　长期活跃攻击源中的物联网占比

数据来源：绿盟科技威胁情报中心（NTI）

3.6.2　活跃攻击资源地域分布

根据攻击源 IP 的活跃持续时间分布，活跃时间达十天以上的攻击源，我们视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，威胁程度较高。

从全球分布来看，高活跃度攻击源主要分布在美国、中国，其次是俄罗斯。从国内来看，高活跃度攻击源在沿海和经济发达地区分布密集，其中中国台湾、浙江、中国香港和安徽的高活跃度攻击源最多。这些地区往往网络基础设施数量基数更大，同等安全防护水平下存在安全隐患的设备资源也更多。

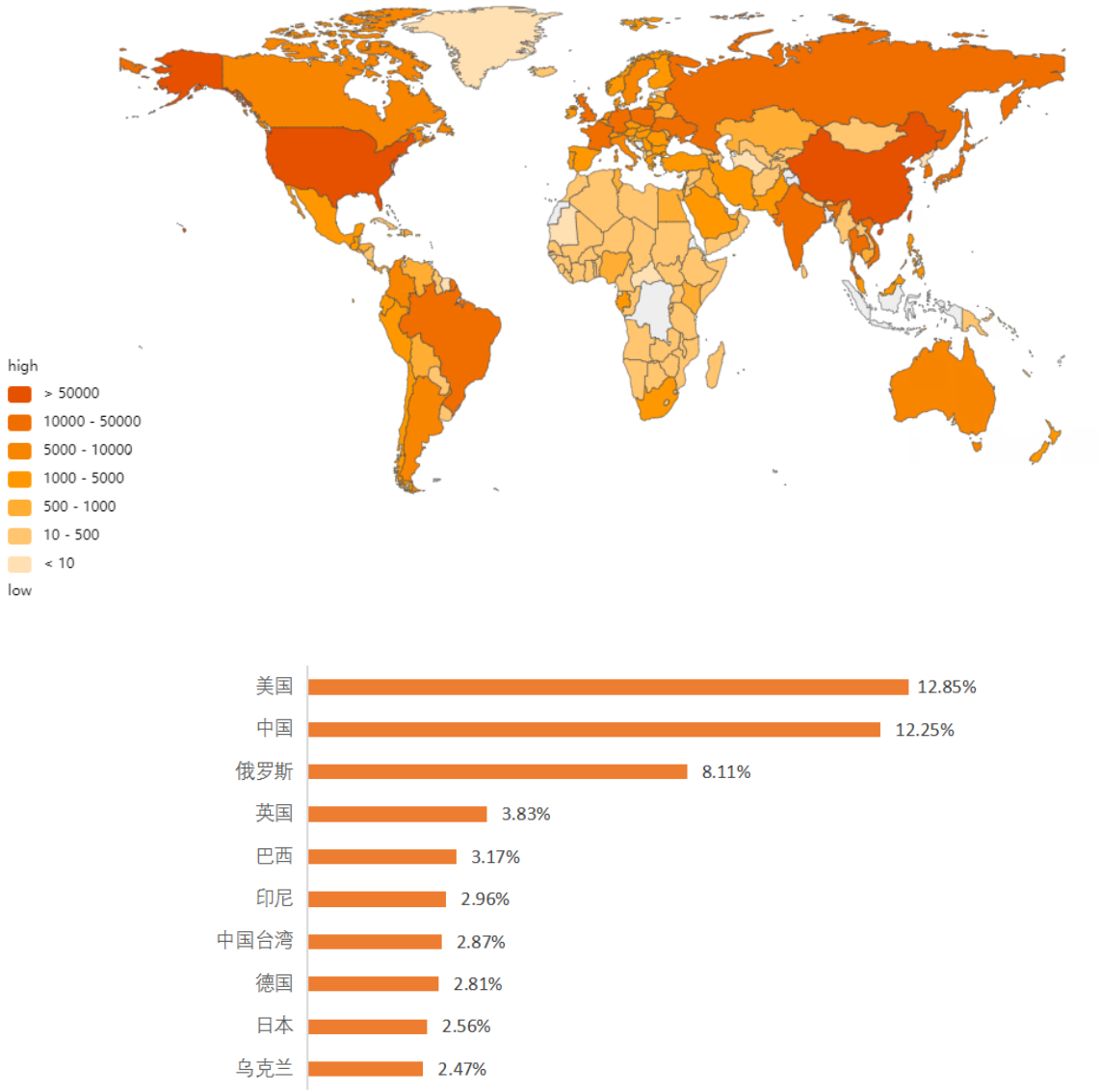


图 3.29　活跃程度较高的攻击资源全球分布

数据来源：绿盟科技威胁情报中心（NTI）

2020 年 DDoS 攻击分析

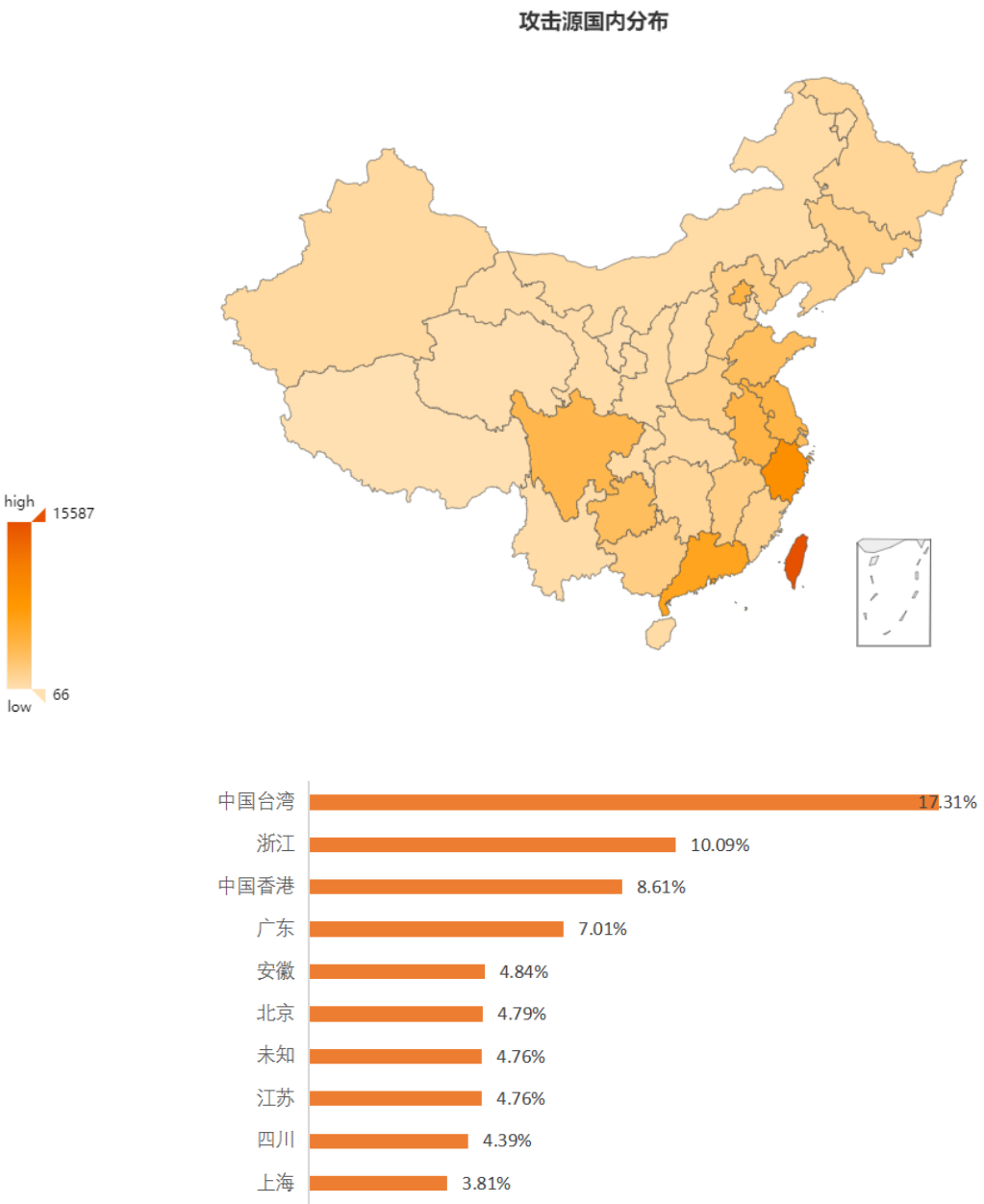


图 3.30　活跃程度较高的攻击资源全国分布

数据来源：绿盟科技威胁情报中心（NTI）

3.6.3 攻击资源惯犯分析

在 2020 年的 DDoS 攻击中， 4% 的惯犯[1] 承担了 78% 的攻击事件。可以看出，惯犯的威胁程度大，不容忽视。

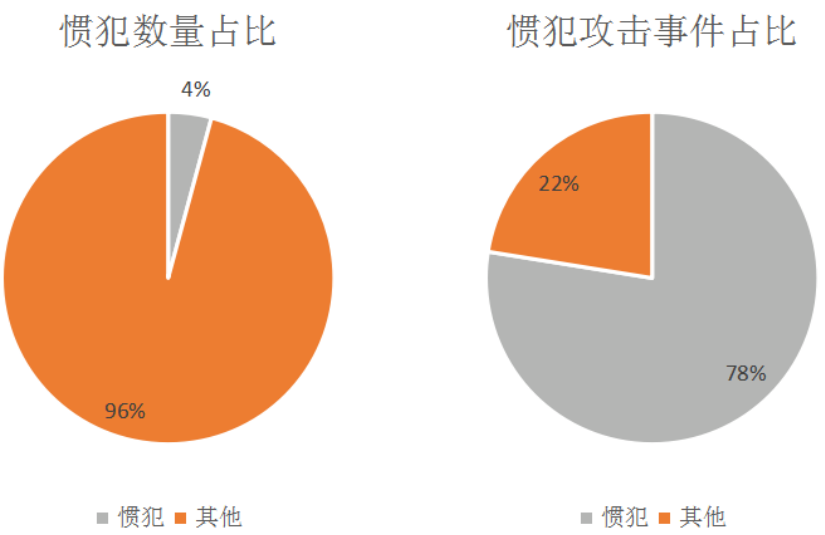


图 3.31 惯犯的数量占比和攻击事件占比

数据来源：绿盟科技威胁情报中心（NTI）

3.6.4 攻击资源异常行为类型分析

参与 DDoS 攻击的攻击资源异常行为类型相比去年更为丰富。2020 年参与过 DDoS 的攻击源中，41% 攻击源发起过多种异常行为，相比 2019 年，最高异常行为由 8 种增加到 12 种。

1 *此处，“DDoS 惯犯”意指长期出现且发起 DDoS 攻击 20 次以上的 IP*

2020 年 DDoS 攻击分析

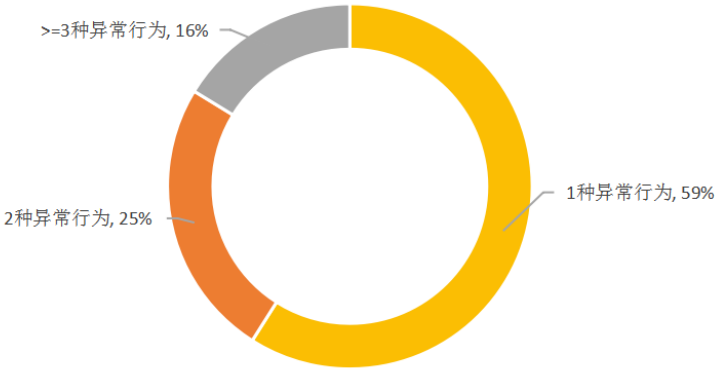


图 3.32　DDoS 惯犯参与的攻击类型数量分布

数据来源：绿盟科技威胁情报中心（NTI）

从下图中的异常行为类型分布可知，8.7% 的攻击源曾被僵尸网络所控制；8% 的攻击源有过发送垃圾邮件行为；58. 1% 的攻击源被威胁情报标记曾经多次进行 DDoS 攻击，这些攻击源往往包含能够被远程控制且长期未得到修复的漏洞，或具备反射能力。

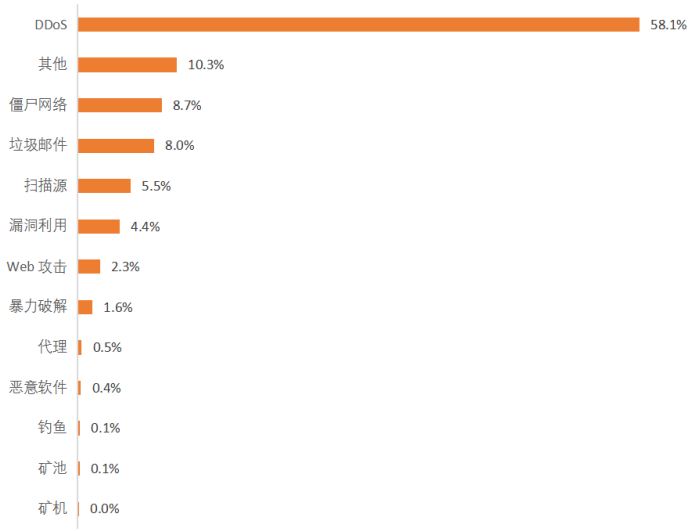


图 3.33　DDoS 惯犯异常行为类型占比

数据来源：绿盟科技威胁情报中心（NTI）

3.6.5 攻击资源团伙行为分析

DDoS 攻击通常以协作方式从多个来源发起，DDoS 惯犯们常常共同组合发起攻击，我们将这样的群体称为“IP 团伙”。在本报告中，我们基于绿盟科技 2020 年全年 DDoS 攻击数据，识别了多个 IP 团伙并系统研究了他们的团伙行为。

采用这种研究方法背后的逻辑是：如果两个 IP 的历史攻击行为相似，那么他们则被划分为一个团伙。团伙行为的相似性主要体现在两方面：

（1）短时间内行为相似：反复在同一时刻用相同攻击手段对同一目标发起攻击。

（2）长周期行为相似：在不同时期反复对相同目标发起相同手段攻击。

在本节中，我们对 IP 团伙行为进行了统计分析，并且对重点团伙进行了刻画。通过分析，我们发现：

观点一：能够长期稳定被控制的攻击团伙，组成成员大部分是物联网设备，IDC 数据中心等基础设施。

观点二：单一团伙的攻击总流量最高达到 3624TB，这个最大攻击总流量是去年的两倍以上。

3.6.5.1 团伙规模

2020 年共发现 45 个活跃团伙，团伙规模分布如下，大部分团伙规模都在 200 到 1 万之间。成员数量大于 1 万的大团伙有 4 个，其中规模最大的团伙成员高达 4.9 万个。

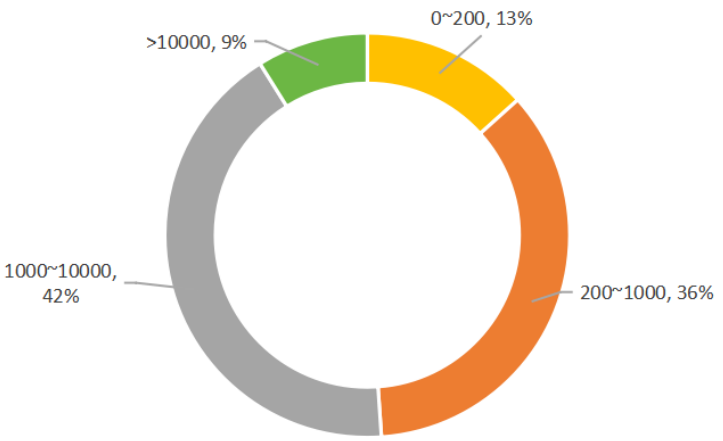


图 3.34 IP 团伙攻击源规模分布（每个区间代表团伙规模范围）

数据来源：绿盟科技威胁情报中心（NTI）

3.6.5.2 团伙攻击总流量

各团伙的流量分布如下，涵盖了来自同一团伙所有成员的全部攻击。单一团伙的攻击总流量最高达到 3624TB，这个最大攻击总流量是去年的两倍以上。

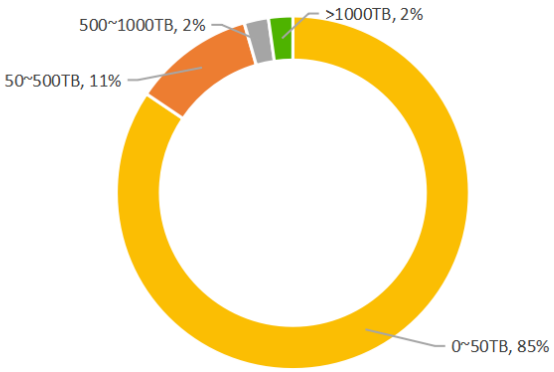


图 3.35 攻击总流量各区间团伙数量分布

数据来源：绿盟科技威胁情报中心（NTI）

3.6.5.3. 团伙攻击资源类型

能够长期被操控的团伙攻击资源主要就是 IDC 和物联网设备，统计团伙所有攻击资源类型，占比最高的就是物联网设备，占比 31%。其中，占比最高的为 15% 的摄像头、12% 的路由器设备和 3% 的网络电话。

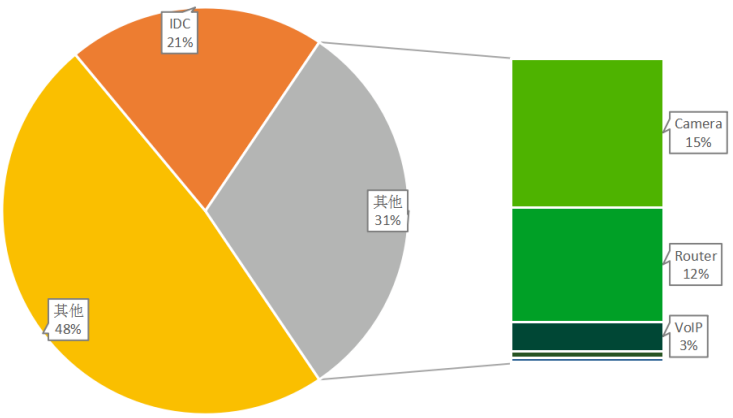


图 3.36 团伙攻击资源类型分布

数据来源：绿盟科技威胁情报中心（NTI）

3.7 物联网攻击资源分析

3.7.1 国内物联网资产暴露情况

根据不同端口及扫描时长的扫描结果数据，对各类型的物联网资产的变化情况进行统计分析发现，国内的物联网资产中，VoIP 电话的网络地址变更最频繁，发生过变化的资产占总资产的 80%，其次是路由器和摄像头，变化资产分别占 60% 和 40%[1]。

为保证资产的时效性与准确性，我们选择 2020 年 11 月的单轮国内物联网测绘结果，共发现 186 万个存活的 IP 地址，具体国内物联网资产类型分布情况物联网设备类型分布如下图所示。其中，摄像头、路由器、VoIP 电话数量分别位列前三，这和往年的分布是一样的，但是新增了安全设备和网络存储器；网络安全设备主要是指防火墙、WAF 等安全产品；网络存储器（NAS）是一种专用数据存储服务器，将存储设备与服务器彻底分离，集中管理数据，从而释放带宽，降低成本。近年来，国内的 NAS 服务器遭勒索病毒攻击事件频发，暴露互联网上的存储设备，更应该保障其安全。

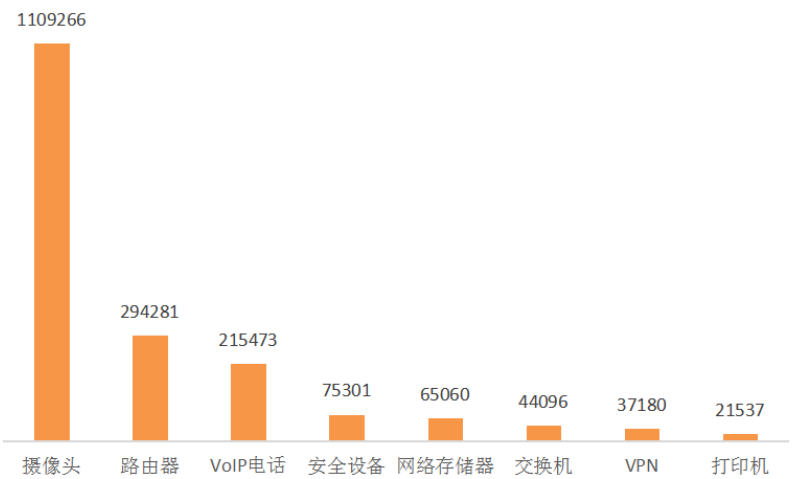


图 3.37 国内物联网资产类型分布情况

数据来源：绿盟科技威胁情报中心（NTI）

1 2018 物联网安全年报 https://ti.nsfocus.com/api/v1/search/getReportPDF/?file=2018_IoT_Security_Report_20190308.pdf

3.7.2 异常物联网设备的 DDoS 参与度

考虑到上文中提到的网络地址变化因素，我们仍然使用 2020 年 11 月的单轮国内物联网测绘结果。与情报数据关联后发现在 186 万的物联网 IP 中异常物联网设备的数量约 28 万个，占比 15.4%。各异常行为类型占比如下图 [1] 所示，其中参与 DDoS 的物联网设备，所使用的 IP 数量约 8.2 万，占全部异常物联网设备的 IP 总量的 28.7%。

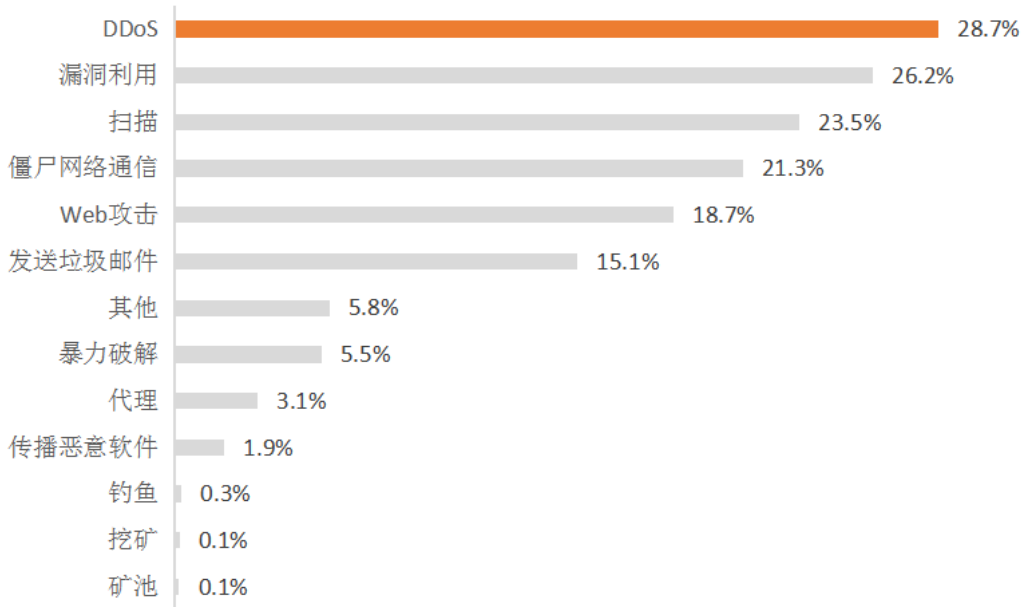


图 3.38 异常物联网设备异常行为占比

数据来源：绿盟科技威胁情报中心（NTI）

3.7.3 参与 DDoS 攻击的物联网设备类型分布

从设备类型来看，全部参与 DDoS 攻击的物联网设备中，占比前五名的分别是摄像头、VoIP 电话、路由器、网络存储器以及安全设备，占比总量约 94%，其中仅摄像头的数量就占总量的一半以上，约 61%。结合图 3.39 中物联网资产类型的分布可知，摄像头和路由器由于其在互联网中暴露的基数大以及各类设备所具有的一定共性决定了这两类物联网设备一直备受攻击者青睐。此外， VoIP 电话被攻击

1 *由于某些设备有多种异常行为，从而导致中累计百分比大于 100%。*

者利用发起恶意行为的比例占自身数量的 4.3%，仅次于摄像头 4.4%，高于路由器 1.9%。由此可见，VoIP 电话在 DDoS 攻击中也是容易被利用的物联网设备之一。

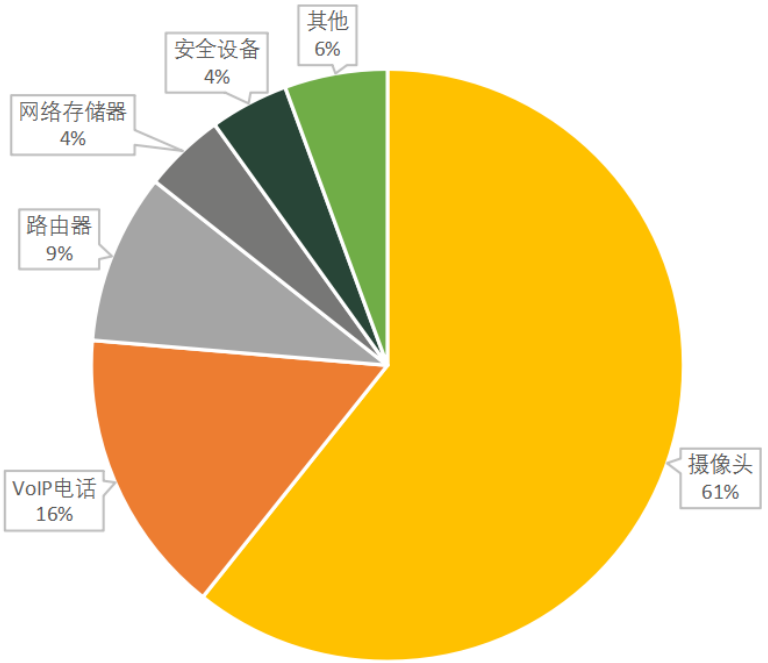


图 3.39　参与 DDoS 攻击的物联网设备类型分布

数据来源：绿盟科技威胁情报中心（NTI）

3.8　DDoS 僵尸网络

3.8.1　僵尸网络概览

2020 年度，绿盟科技伏影实验室监控到来自 DDoS 僵尸网络的指令数逾 104 万条（截止 10 月底），较 2019 年增幅近一倍。其中 DDoS 攻击指令条目约 103 万。

根据家族信息（含变种）、攻击目标和攻击时间三个维度，并规定指令下发超时时限，得出了逾 16 万起攻击事件，并在 8 月达到峰值。月度攻击事件数变化如下图：

2020 年 DDoS 攻击分析

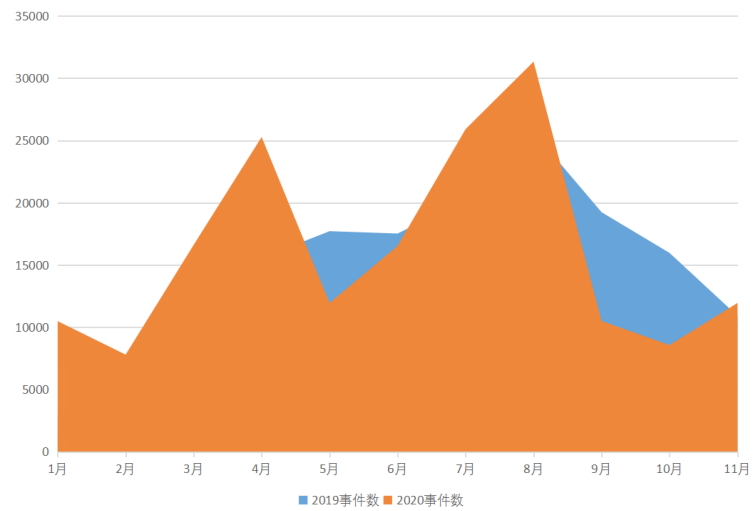


图 3.40　DDoS 月度攻击事件变化

DDoS 类型方面，相比于 2019 年，TCP flood、UDP flood 和 CC 占据主导地位，其中 TCP flood 与 CC 比重明显上升，如下图所示：

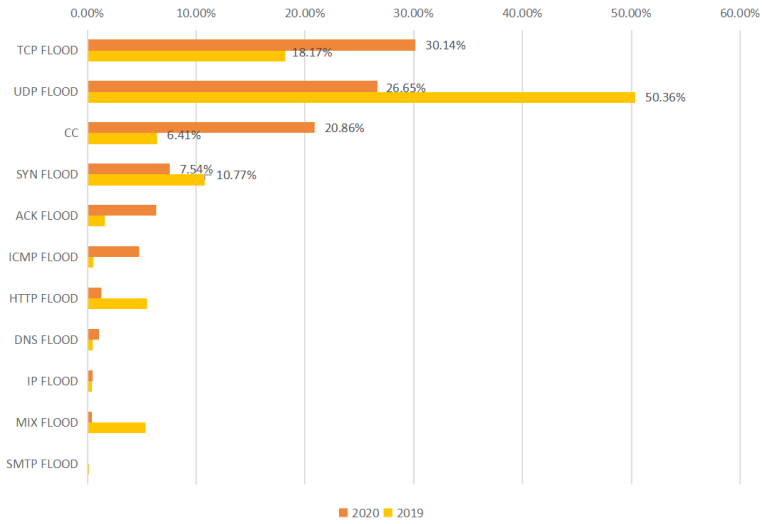


图 3.41　DDoS 类型对比

上述 DDoS 攻击总共来自 10 个家族。伏影实验室监控的家族活跃情况如下，易知 Mirai 处于支配地位，制造了近 3/4 的攻击事件。

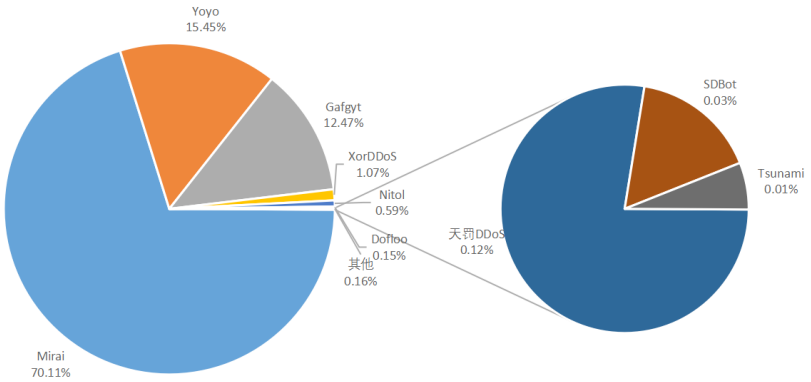


图 3.42　家族攻击事件数占比

在攻击指令下发方面，情况则有所差异。Dofloo（AESDDoS）占据了近 60%，而 Mirai 只占不到 20%。同样，攻击事件数偏少的 SDBot 在指令数方面也排名靠前。这种差异主要源于 DDoS 家族自身的攻击特征以及其在国际化与非国际化的黑产平台上的不同推广程度。

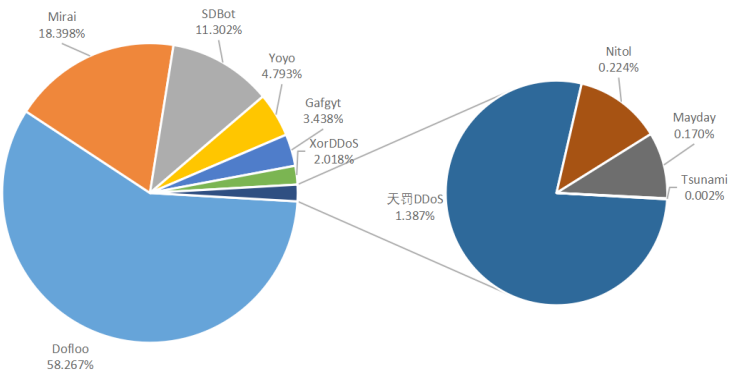


图 3.43　家族 DDoS 指令数占比

传播方面，2020 年度 IoT 平台 DDoS 家族的漏洞利用数超过 130 个。利用载荷组成与往年类似，位居前二的依然是 CVE-2017-17215 和 CVE-2014-8361，其余类型主要为各类设备的远程命令执行与注入。而 Windows 平台家族的传播方式同样无显著变化，SQL 注入、远程漏洞、弱口令爆破和破解软件都是其入侵的常见手段。下图为本年度 DDoS 家族使用 IoT 平台流行漏洞：

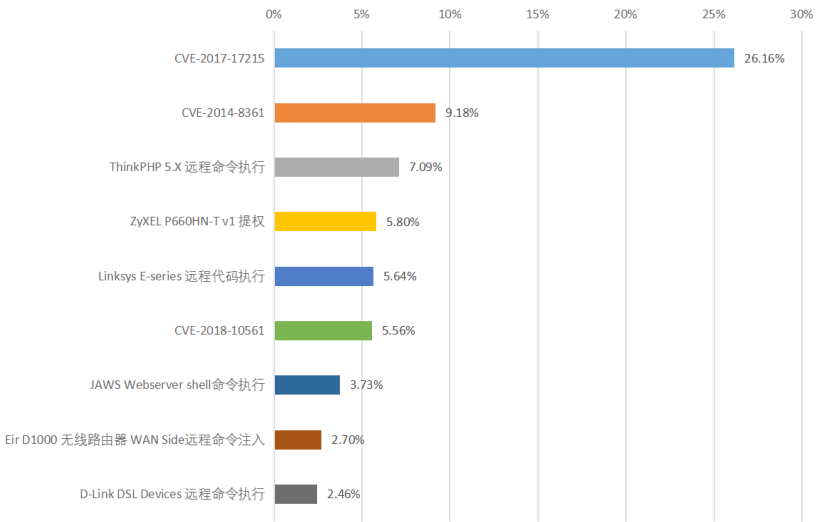


图 3.44　IoT 漏洞利用情况

3.8.2　热点家族

3.8.2.1　Mirai 与 Gafgyt

Mirai 和 Gafgyt 仍旧是当今世界范围内影响最大的两个 Linux/IoT DDoS 家族。这两大家族因其代码开源属性而利用广泛，故其变种如同雨后春笋般不断涌现，甚至改良并进化出新型家族，成为 IoT 安全的严重威胁之一。

Mirai 和 Gafgyt 的 C&C 数量和攻击范围在当今可谓首屈一指。2020 年，伏影实验室追踪到这两个家族的 C&C 地址就超过了 1500 个（更新到 11 月底），活跃 C&C 占到 94%，平均每日就会新部署约 4~5 个 C&C。这些 C&C 攻击了超过 22 万个 IP 和域名，平均每月 700 多个目标。下图为两个家族合并后的月度攻击目标数变化：

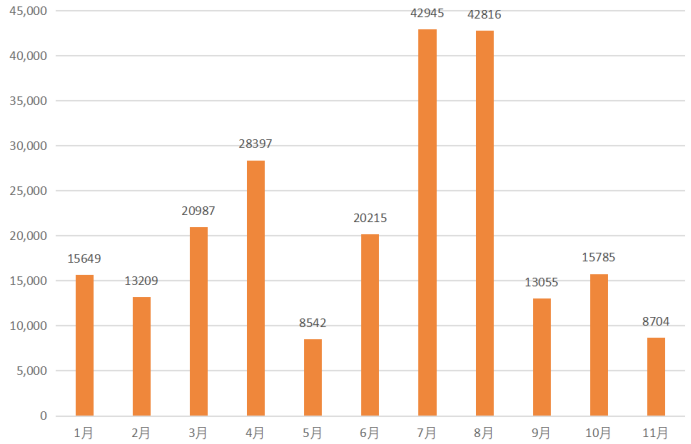


图 3.45　Mirai+Gafgyt 攻击目标的月度数量

在进行 DDoS 攻击时，Mirai 和 Gafgyt 类型多样，包括 SYN/ACK flood、IP flood 、UDP/TCP flood、DNS flood、Greth flood 和 HTTP flood 等手段，涵盖面从网络层到传输层。

传播方面，Mirai 和 Gafgyt 利用的最多的便是华为 HG532 路由器漏洞和 Realtek rtl81xx SDK 远程代码执行漏洞，以上也是目前统计到的 IoT 家族使用最多的两个漏洞。此外，少数木马中出现的疑似 0day 载荷，表明其控制者在紧跟“时代步伐”的同时，依然在寻求更多更快的传播渠道。

此外，Mirai 和 Gafgyt 的开源属性为新型 DDoS 家族的衍生提供了灵感和便利。2019 年底，由 Mirai 运营者控制的 DDoS 家族 DarkNexus 开始活动。与 Mirai 和 Gafgyt 相比，DarkNexus 总体行为更为复杂，DDoS 手段更为新颖，感染链条更加隐秘。 DarkNexus 还拥有 Mirai 和 Gafgyt 所不具备的定制化扫描功能，使得定向传播成为可能。诸此特性为 IoT 安全增加了很多不确定性的威胁。

3.8.2.2　Dofloo、SDBot 和 Yoyo

Dofloo（AESDDoS）长期被认为与 XorDDoS 和天罚 DDoS 等家族属于同一个 DDoS 攻击组织。该家族主要服务于灰黑互吃领域，攻击游戏私服与博彩等行业，其 C&C 和 Victim 90% 均位于中国，本年度攻击方式以 CC flood、TCP flood 和 UDP flood 为主。

相比 Mirai 和 Gafgyt 这样的国际化的家族，Dofloo 暴露出的 C&C 和攻击目标非常有限，制造的攻击事件较少，可见其一直运营在小规模的黑产平台上。但这并不意味着 Dofloo 活跃度偏低。2020 年伏影实验室监控发现，Dofloo 在下发攻击指令的间隔大约在 5 秒钟 ~1 分钟左右，频度较高。若以 10 分

钟间隔为超时上限，则相同 C&C 针对相同目标下发的指令的连续时段最高可达 31 小时左右，这样的时长加上每条指令自带的攻击次数或时间，足以令受害者业务崩溃。

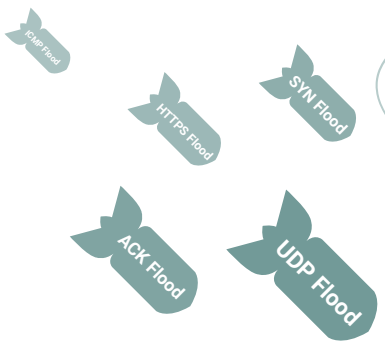
SDBot 家族与 Dofloo 情况类似，C&C 数量与攻击目标有限，但在本年度上半年特定时段内活跃度高，下发攻击指令频率高，且指令连续下发时段最高可达 34 小时左右，攻击方式以 TCP flood 为主。

Yoyo 家族在 DDoS 界已活跃 10 余年。本年度追踪数据显示，该家族背靠极少量的 C&C，运营范围小于 Dofloo，然而同样在特定时段表现出高活跃度，且能够连续数月保持稳定的活跃度。本年度 Yoyo 以 ICMP flood 为支配攻击手段，其目标数量比起 Dofloo 也相对更多，范围更广，涉及跑分平台、加速器、下载站、在线视频接口、博彩和私服等行业。

从目前情况看，尽管这类家族整体规模有限，不过一旦接到任务就会非常活跃，不可小视。此外，在当今 Mirai 和 Gafgyt 变种引领的 DDoS 木马同质化的趋势下，它们的存在也反映了不同国家区域之间的生态差异，并为解读这些差异提供了观察入口。

4

总结



总结

回顾 2020，每天都在见证历史，我们同样深刻感受到在疫情爆发中、国际关系变化中、5G 的发展中的各方势力关于网络空间安全的一次次凶险博弈。国际大事件往往会给黑客创造网络攻击的时机，新的攻击手法也是层出不穷，随着 5G 和物联网设备的快速发展，黑客利用海量物联网设备发起的慢速攻击需要新的应对思路。移动终端不断沦陷，对传统的 DDoS 防护技术和架构带来巨大的挑战。反射攻击仍是 DDoS 攻击主力，新型反射攻击层出不穷，防护需要及时更新。针对 HTTP2.0 等新型攻击方法的不断被发现，迫使 DDoS 防御技术的升级。DDoS 的防护要充分利用大数据和人工智能技术，才能在瞬息变幻的环境变化中跟踪他们的脚步甚至预测到他们的攻击，推出新的防御算法，在这没有硝烟的网络战争中使自己既能料敌于先，也能后发先至，才有把握使胜利的天平始终倾斜在我们这边。

中国电信集团云网安全科技有限公司（云堤公司）

中国电信集团云网安全科技有限公司（云堤公司）是中国电信集团旗下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，整合中国电信云网、安全、数据等优势资源和能力，为客户提供云网安全、数据安全、信息安全等各类安全产品和服务。云堤公司前身是中国电信股份有限公司网络安全产品运营中心，成立于 2015 年 1 月，负责研发并运营“云堤”系列网络安全产品，主要包括：分布式近源防护架构的 DDoS 攻击防护平台、网站安全专家服务系统（云监控 + 云防护）、域名安全服务系统，反欺诈服务系统等。云堤平台通过国家等保三级测评，已为 8000+ 客户提供网络安全防护服务，并成为历次重大国事活动网络安全保障的首选网络安全防护平台，受到了客户及有关部门的高度认可。

绿盟威胁情报中心

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 2.0 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。

网址：https://nti.nsfocus.com/

伏影实验室

伏影实验室专注于安全威胁与监测技术研究。 研究目标包括僵尸网络威胁，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。

2020 DDoS攻击态势报告

中国电信 CHINA TELECOM 云堤 SECURITY NSFOCUS

欢迎关注
中国电信云堤官方微信

欢迎关注
绿盟科技官方微信