中国联通 China unicom | 联通数科 Unicom Digital Tech | 百度安全 有AI更安全 | OASES Open AI System Security Alliance

2020年
DDoS攻击态势报告

2021.03

关于联通云盾

联通云盾是联通数字科技有限公司安全板块的产品品牌，是中国联通在网络安全领域的专业化知名品牌，专注于DDoS防护、域名防护、网站安全防护等领域，秉承合作开放共赢的理念，与合作伙伴一起致力于网络空间安全事件的监测、防护、处置，为用户提供运营商级网络安全服务。DDoS攻击防护服务(抗D先锋)作为联通云盾主打产品之一，为用户提供攻击监测、攻击防护（流量清洗、封堵、智能过滤）、攻击溯源、个性防护方案定制等多项服务。

关于百度安全

百度安全是百度公司旗下，以AI为核心、大数据为基础打造的知名安全品牌，是百度在互联网安全20年安全实践的总结与提炼。百度智云盾以成熟的防御技术和灵活的合作模式，长期以来为合作伙伴提供了IDC环境下完备、便捷的安全基础设施解决方案，并支持本地快速检测、DDoS攻击防御、自动化拓展T级云防等服务。同时，智云盾平台还集成了包括资产弱点评估、黑客攻击检测、实时安全防御和威胁情报在内的百度安全一系列技术能力，在提高IDC安全水平的同时，也为最终客户提供更为全面的安全增值产品。为国内IDC发展保驾护航。

关于中国联通智网创新中心

中国联通智网创新中心负责承担中国联通网络产品研发、智能化运营、集中客户交付及生态合作等职能，紧密围绕网络产品、网络中台、5G创新、运营支撑等方面，提高网络创新能力，打造智能网络中台，提升网络产品研发和交付运营核心能力。

关于OASES智能终端安全生态联盟

是国内致力于提升智能时代产业生态安全的联合组织，OASES联盟秉承以资源共享、核心开源、标准驱动、产业共赢的理念为基础，致力于AI时代智能终端安全生态的建设，推动提升智能终端安全的快速响应及防护能力，共同应对智能终端产业所面临的各种安全挑战。

版权及声明：

致谢：

感谢中国联通智能网络创新中心能力基座提供强大的数据支持！

目录

2020年DDoS攻击态势分析报告

序言

本报告为联通数字科技有限公司和百度安全联合监测及研究成果，针对 2020年发生的DDoS攻击事件进行汇总分析。报告给出了2020年中国联通全网范围内监测到DDoS攻击事件的数量、攻击强度、持续时长、受害者地域分布、攻击源追溯和分布等多个维度的情况分析。同时百度安全针对2020年度所监测的攻击事件进行了进一步的深度研究，对反射攻击、黑客团体等专题进行相关分析。从而力争达到对DDoS攻击形成立体宏观的刻画，为治理DDoS攻击，净化网络空间提供数据支撑。

DDoS攻击整体态势摘要

2020年，各个行业都在数字化转型的道路上如火如荼地发展，云计算、大数据、物联网、人工智能等技术已越发成熟，网络空间面临的威胁也随之加剧。特别是DDoS攻击，随着智能化攻击平台的源代码不断外流，攻击者团体也异常活跃。2020年发生的一场全球范围的疫情，使得政务、医疗、教育等行业业务大幅度互联网化，也成为DDoS攻击的新目标。我们监测到2020年发生的DDoS攻击数量相比于2019年增加了近一倍，攻击强度也是逐年提升，10Gbps-100Gbps之间的中等强度攻击比例逐年增大。攻击者更倾向于采取瞬时骚扰性的攻击手法，攻击持续时间短，但攻击频次增多，这就使得被攻击目标需要性能更强大、更专业的攻击防护手段。UDP Flood仍然是攻击者最普遍使用的攻击手段，而各种反射攻击，诸如SSDP、DNS、Memcached、NTP等依然盛行。全球范围来看，美国和中国成为DDoS攻击超级活跃的大国；中国国内范围，则是北上广深和东部沿海的经济发达地区遭受了更多的DDoS攻击，同时也有着更多活跃的DDoS攻击资源。相对于其他行业而言，互联网、软件服务行业明显遭到了更多的DDoS攻击，此外，在2020年，游戏、金融、教育等行业也是重灾区。

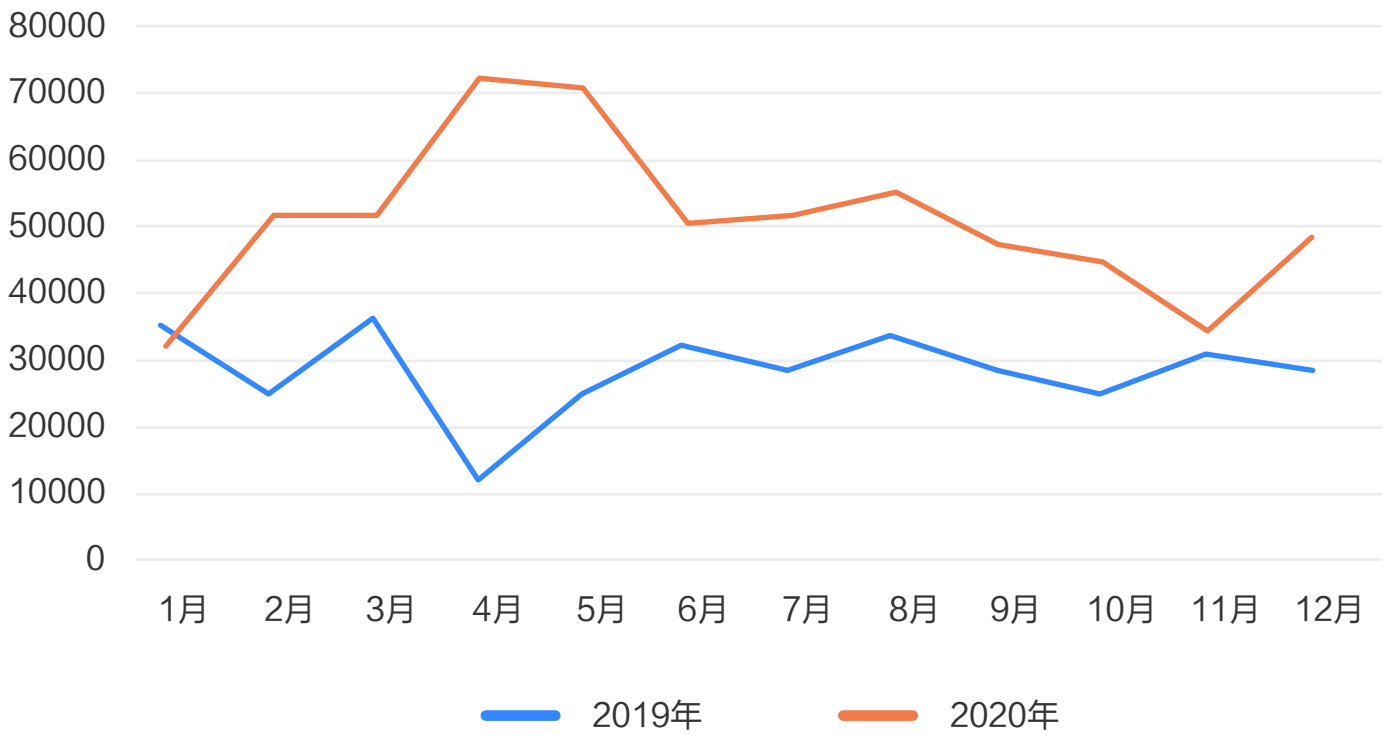
01

攻击态势

1.1攻击数量趋势

2020年全年，中国联通全网范围内共监测到DDoS攻击63万余次，是2019年的36万余次的近1.75倍。纵观全年，4、5两个月份为DDoS攻击高发期，其余各月攻击次数相对平均。监测到的DDoS攻击数量的提升，与监测手段逐步完善，监测精度日趋细化有着密不可分的关系。

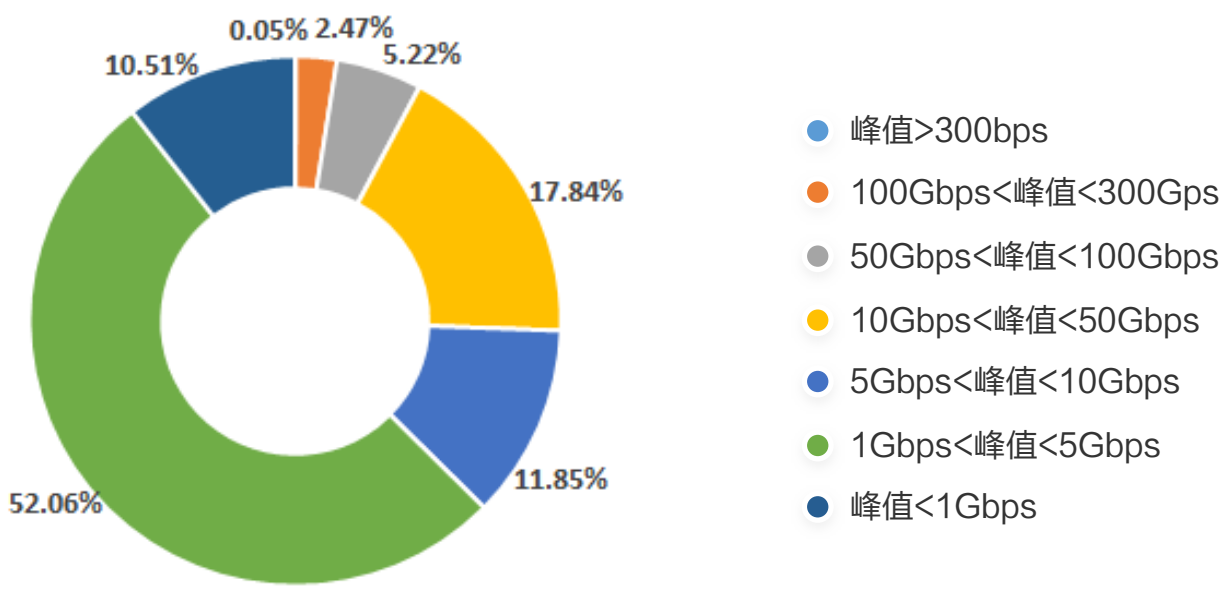
2020年VS2019年 各月攻击数量趋势图



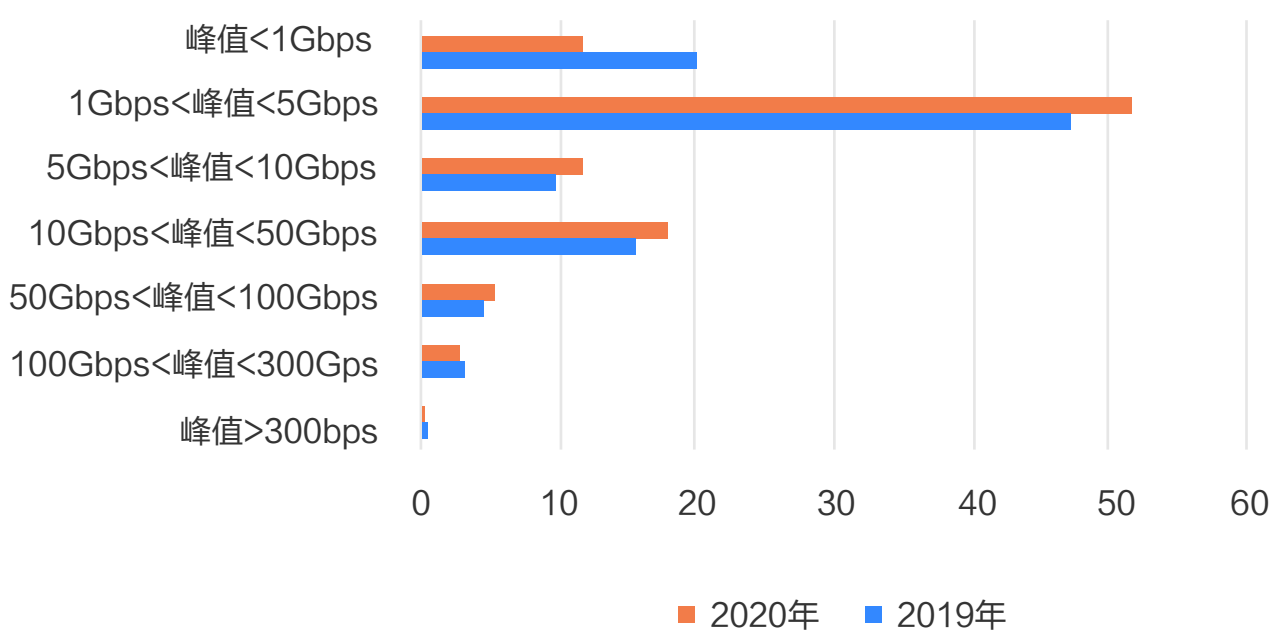
1.2攻击峰值趋势

2020年，DDoS攻击峰值主要集中在1Gbps-5Gbps区间内，占全部攻击总数量的52%，其次10Gbps-50Gbps区间，占总量的18%。全年共监测到100Gbps以上的大流量攻击事件16029件，其中300Gbps以上的超大流量攻击事件277件，年度最大攻击峰值达到1.49Tbps。从2020年与2019年DDoS攻击的攻击流量占比区间分析，2020年1Gbps以下攻击占比减少，1Gbps-100Gbps各流量区间内攻击占比，2020年均高于2019年，由此可见DDoS攻击的强度正在逐年提升。

2020年攻击峰值占比分布

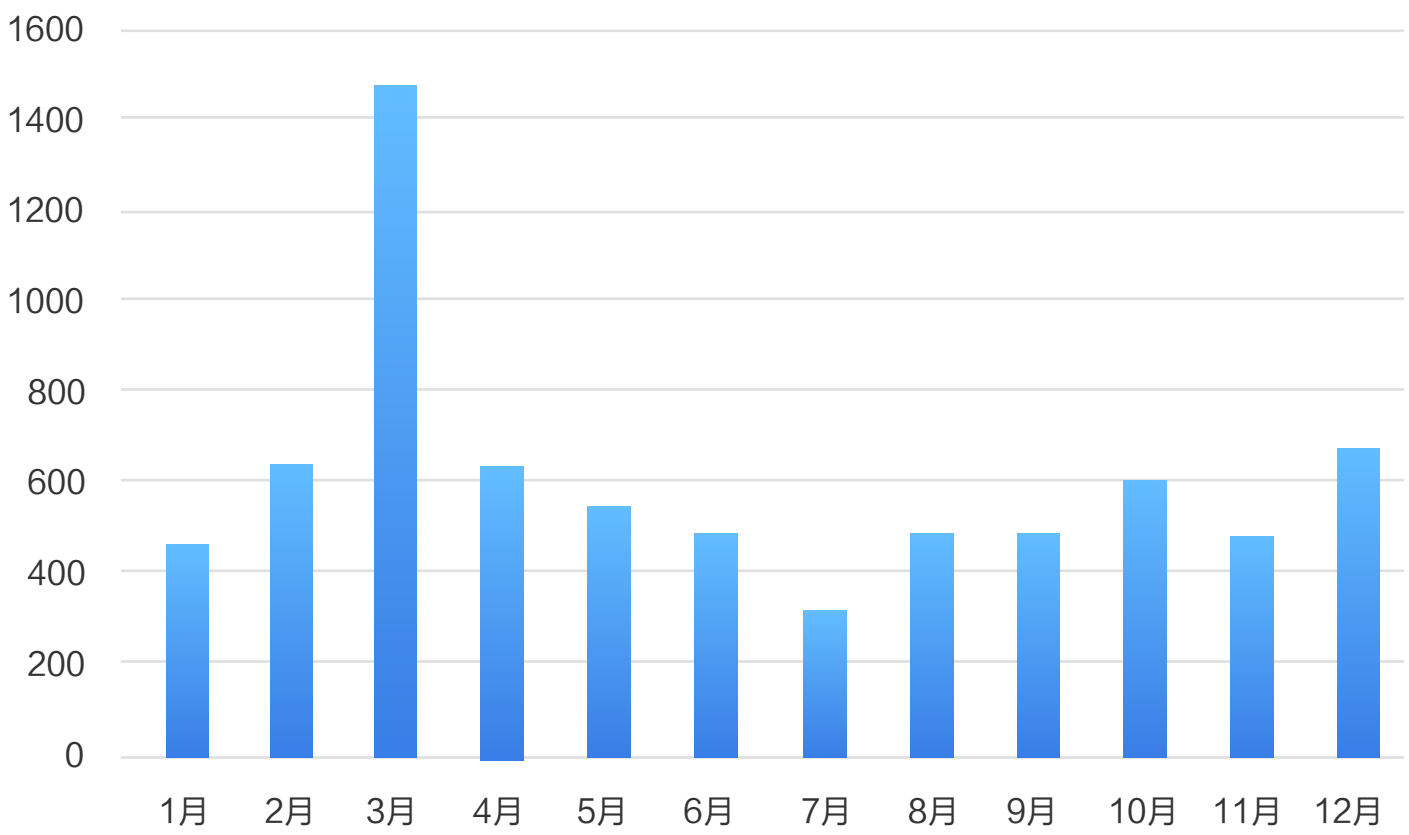


2020年VS 2019年 攻击流量区间占比



纵观2020年各月的攻击峰值，除了在3月达到全年峰值的最大1.49T外，其余11个月中，有10个月的峰值都达到了400Gbps以上，其中2、4、10、12四个月的峰值超过600Gbps，可见攻击强度之猛烈。

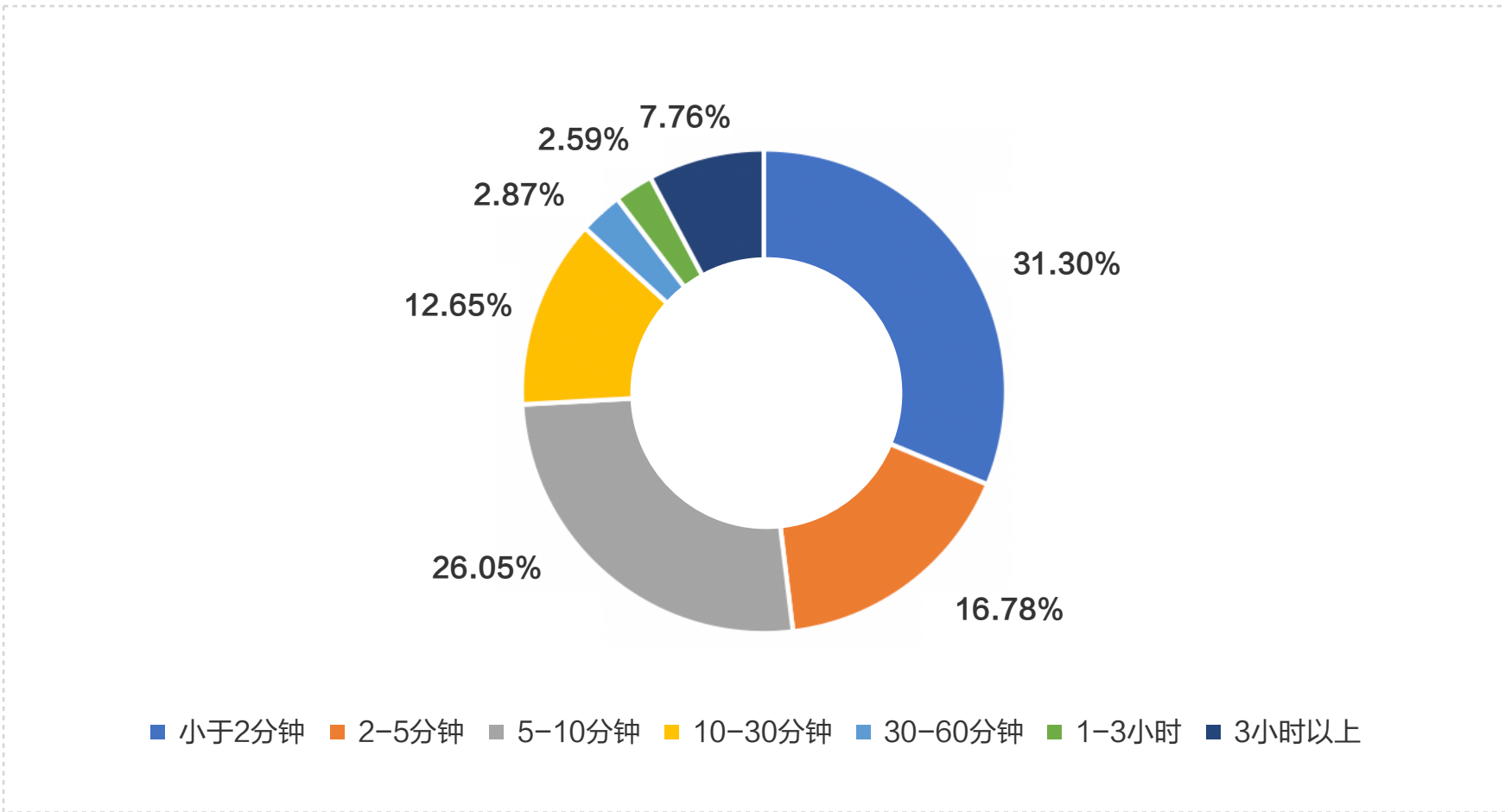
2020年各 月攻击峰值分布



1.3攻击时间趋势

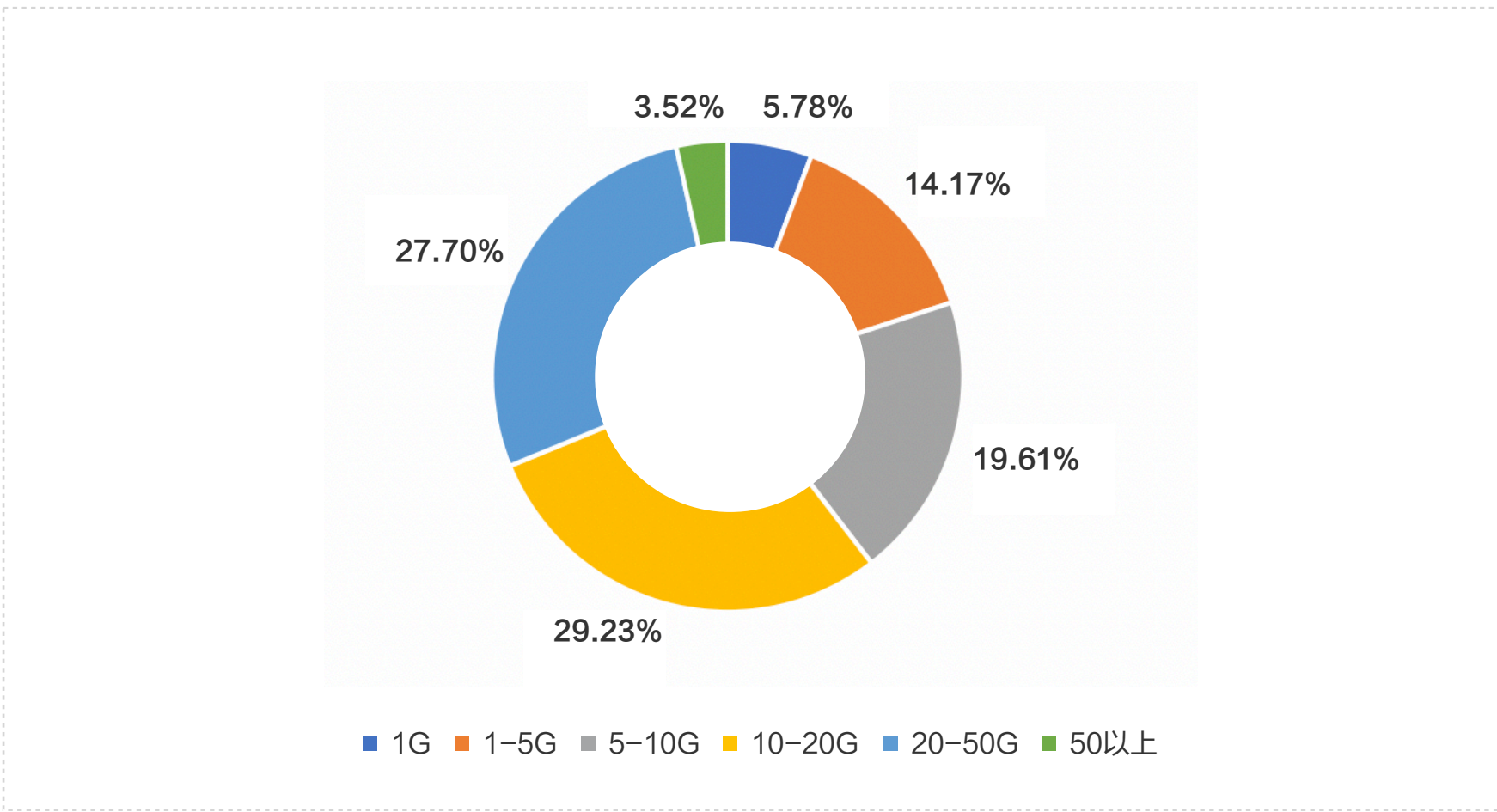
2020年DDoS攻击仍是以短时攻击为主，持续时长在10分钟之内的攻击占全部攻击的74%，其中更是以小于2分钟的攻击占比最大，达到31.3%。另一方面，攻击时长大于3小时的攻击占全部攻击的8%，其中持续时间最长攻击达到400小时之久。从2020年与2019年DDoS攻击的攻击时长占比区间分析，2020年10分钟之内的攻击占比更大，由此可见，攻击者更倾向于采取短时高频次的骚扰性攻击为主，但也不乏对攻击目标的长时间打击。

2020年 攻击时长占比

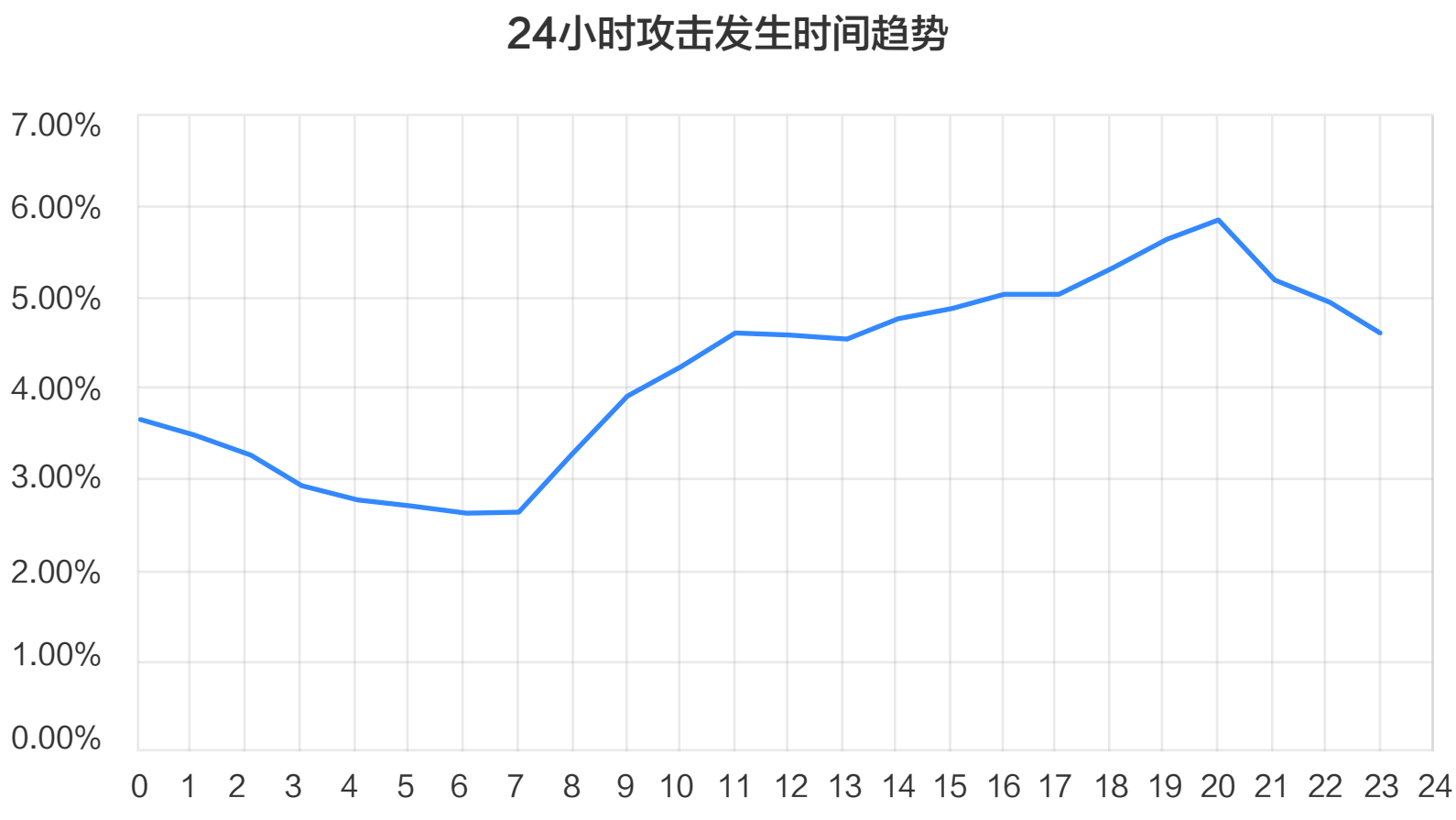


前面我们已经提到，小于2分钟的短时攻击占31%，接近三分之一。而这种短时的攻击，也是各类IDC和企业最难防范的一种攻击。接着我们对这一类2分钟以下的攻击做了进一步的分析。发现小于2分钟内的攻击中，攻击峰值主要集中在20Gbps以内。

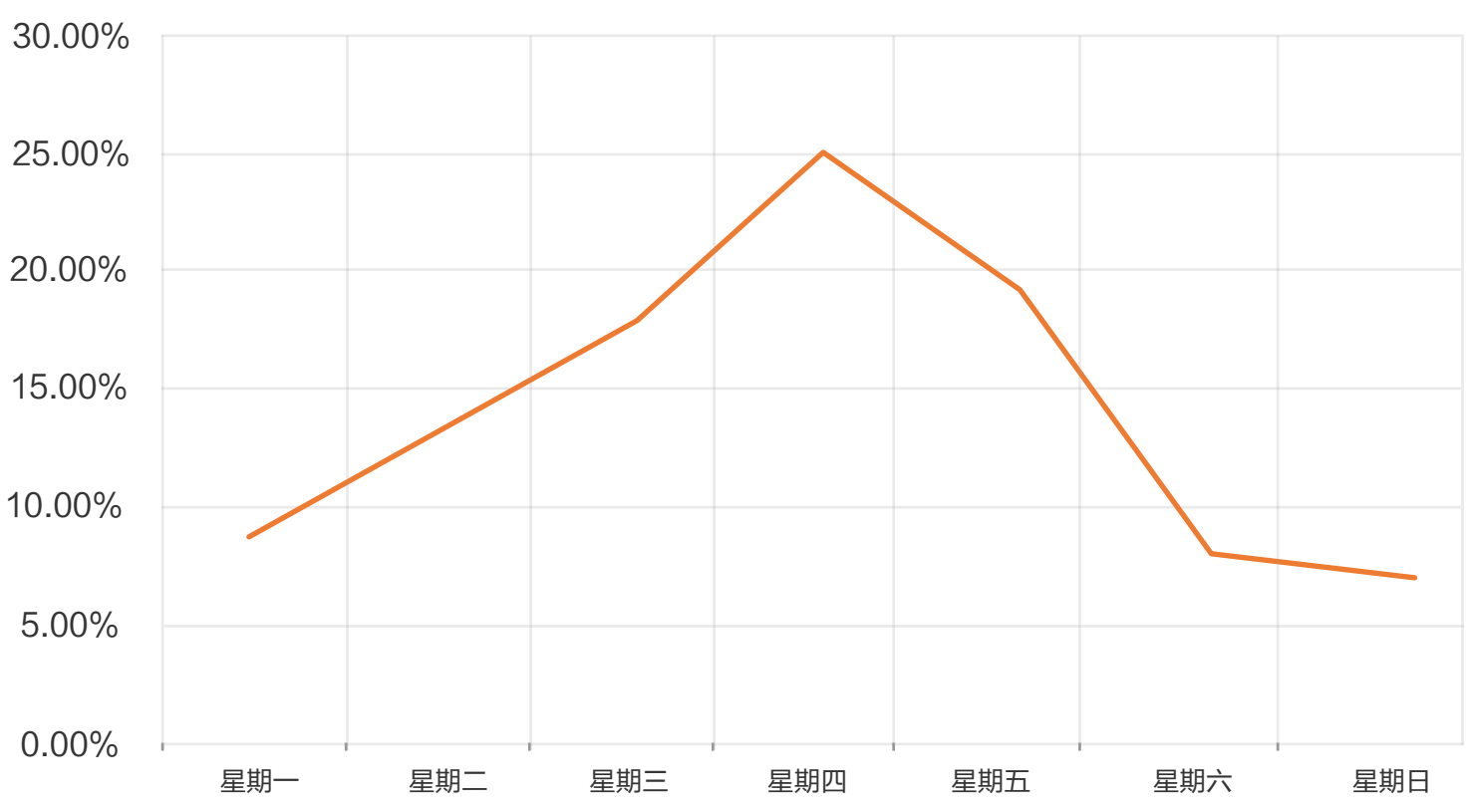
2分钟以下攻击峰值情况



从一天24小时发生DDoS攻击的占比分布分析，攻击数量从8点开始攀升，直至24点，均为DDoS高发期。其中又以11点至24点为攻击最频繁时段，在20点左右达到攻击发生频率最高峰。2020年，攻击在24小时内各时段发生的频度与2019年较为一致，可以看出DDoS攻击者均选择在业务高峰期发起针对目标的攻击。



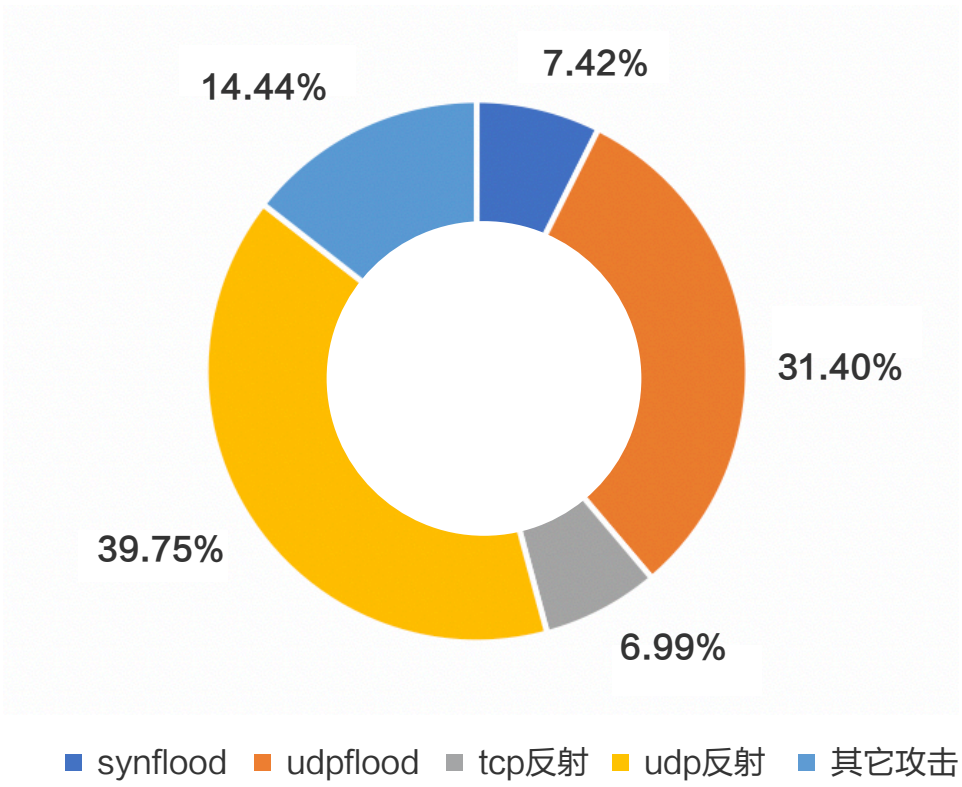
从一周攻击的趋势可以发现，从周一到周四，攻击次数由少到多，逐渐增强，而到了周末后则强度下降明显。攻击者看来也有明显的作息特征。



1.4 攻击手段趋势

2020年，DDoS攻击主要以UDP Flood、SYN Flood以及各类反射攻击为主要攻击手段，其中反射攻击逐渐崛起，手段也变的更为丰富。

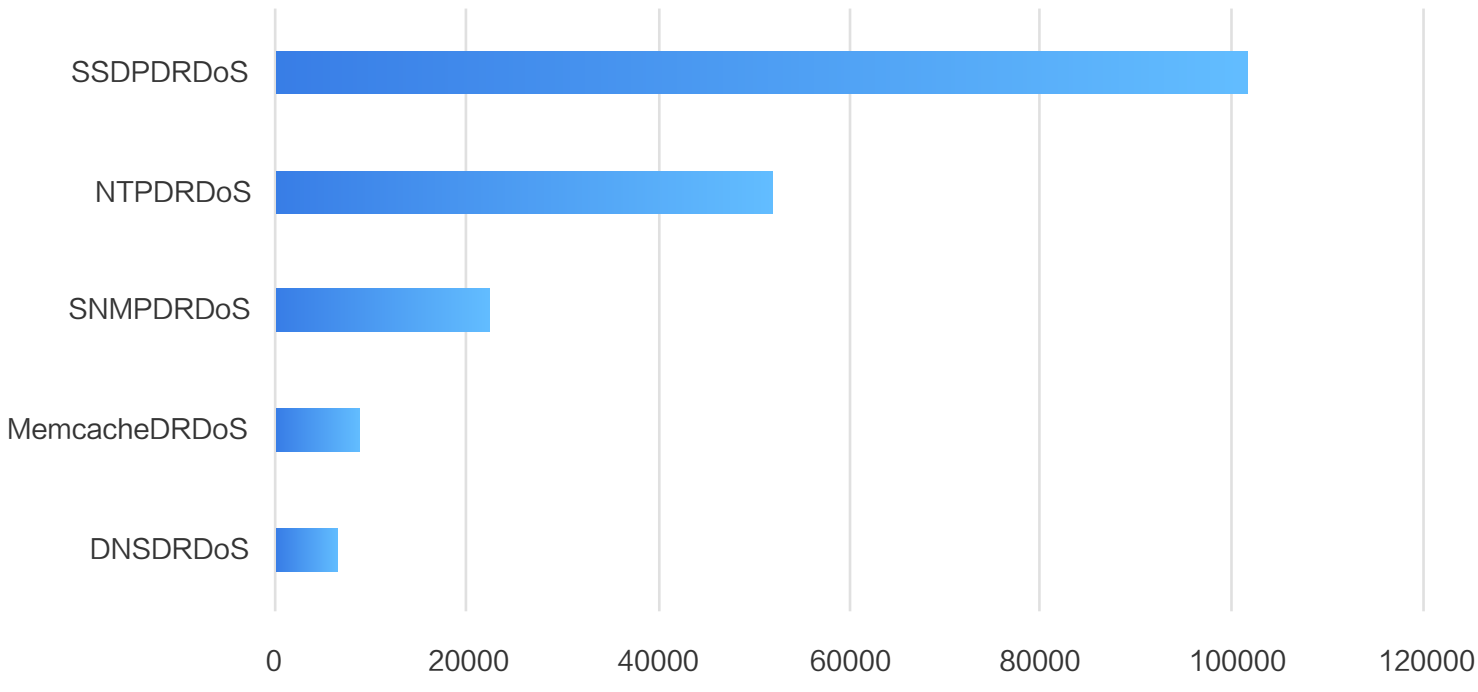
2020年攻击类型占比



从以上攻击类型的占比中我们可以发现，UDP反射攻击拥有高达39.75%的占比，由此可见反射攻击对当今网络造成的危险已经越来越大，并且各类新兴反射方式层出不穷。因此我们也认为很有必要对反射攻击进行进一步的分析研究，以更好的防范此类攻击。

在对反射攻击的攻击次数进行统计后，我们得出以下TOP5的反射型攻击，可以看到，SSDP、NTP两种反射攻击最为活跃，在后续的章节，我们也将对这两个类型的攻击手法，反射源等做详细的阐述分析。

反射型攻击TOP5



1.5国内攻击目标地域分析

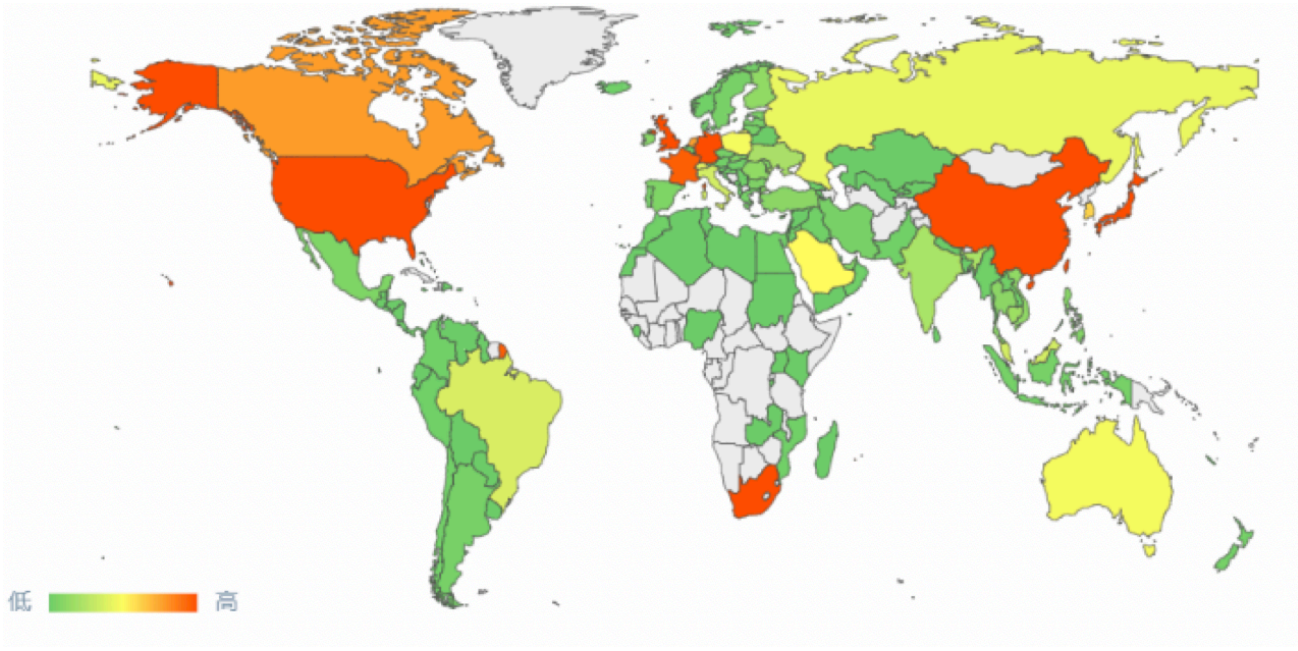
2020年，中国境内受攻击最多的省份为浙江，全年累计遭受攻击12万余次，约占全国受攻击总数的19.04%，随后排名依次从第二至第五位的省份和地区分别为北京、上海、山东、广东。通过攻击目标地域排名，可以看出超一线城市和经济发达地区一直为DDoS攻击的主要地区。

国内受攻击情况

1.6全球攻击目标地域分析

2020年，据监测数据显示，中国和美国仍为遭受DDoS攻击最严重的国家，其次为日本、新加坡、德国、南非等国家。

国际受攻击情况



1.7国内攻击活跃资源分析

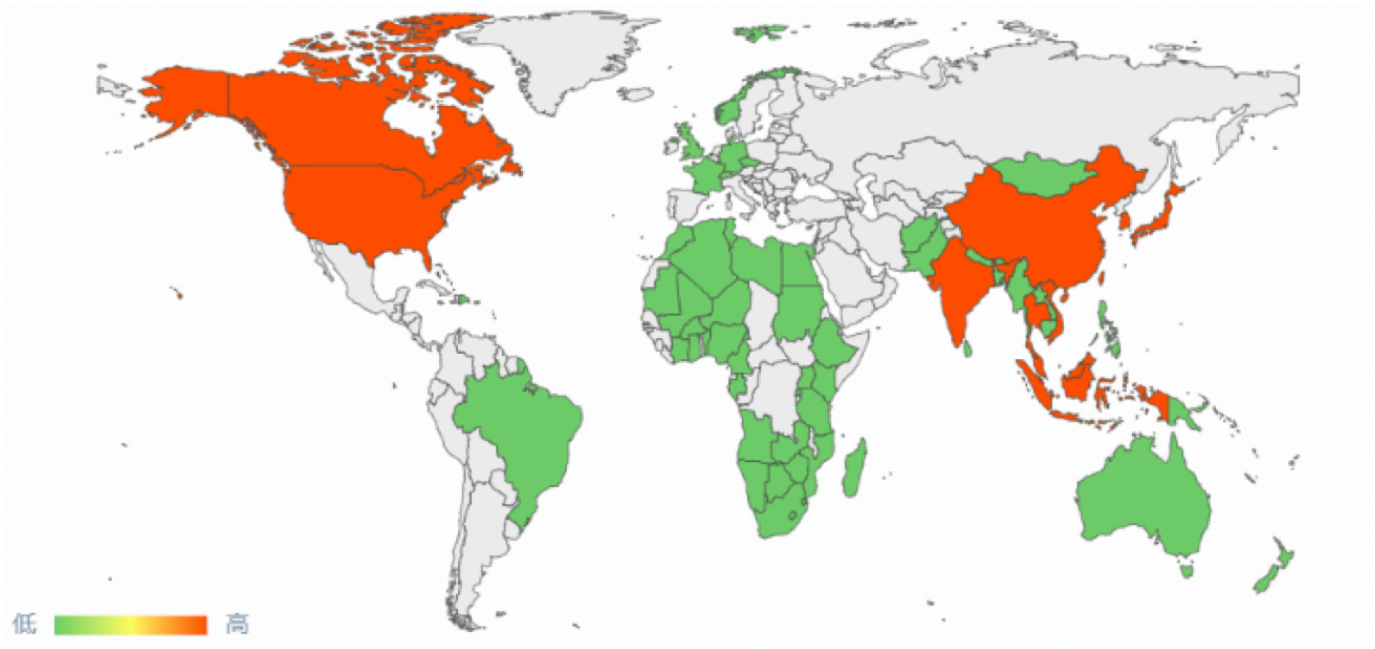
对2020年中国境内参与DDoS攻击的终端和设备进行溯源分析和数量统计，山东成为具有最多活跃攻击资源的省份，所拥有参与DdoS攻击主机数量占全国总量的10.5%，此外辽宁、河北、河南、北京也是拥有活跃攻击资源较多的省份。攻击资源主要集中在沿海省份和东北三省。

国内攻击源情况

1.8全球攻击活跃资源分析

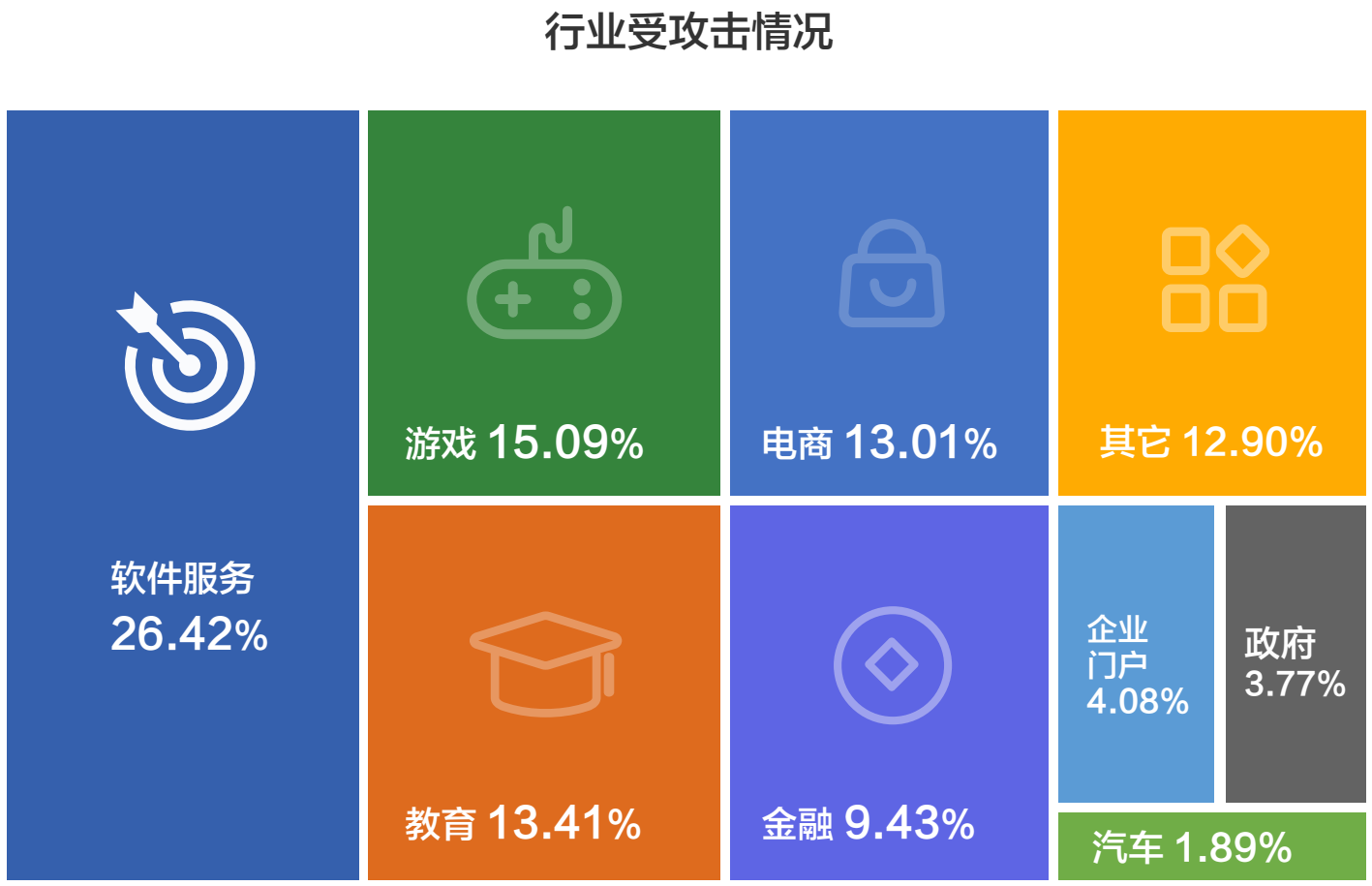
从活跃攻击资源的全球分布来看，中国和美国存在较多的攻击活跃资源，其次为韩国、日本、越南、加拿大、印度等国家和地区。

国际攻击源情况



1.9行业受攻击分析

2020年，依据客户遭受DDoS攻击监测结果统计，发现软件服务、金融，电商，游戏，教育行业是最受黑客青睐的行业，在此提醒各行业客户加强攻击监测，做好攻击防护。



02

反射攻击

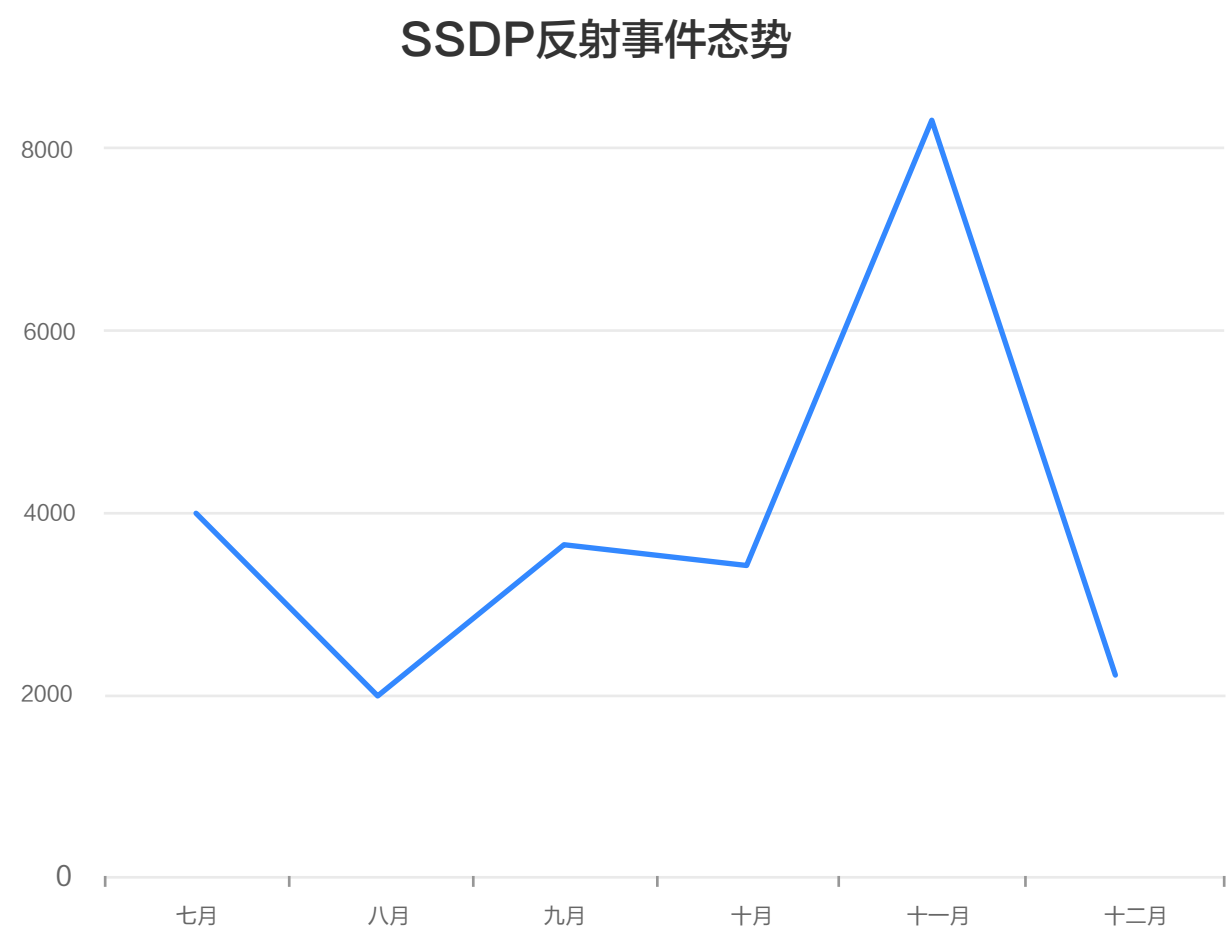
2020年2月，亚马逊AWS 表示遭遇了迄今为止最大的DDoS攻击，攻击流量最高达到了2.3Tbps，这次的攻击是基于CLDAP协议的反射攻击，CLDAP反射攻击是攻击者利用CLDAP协议没有身份认证的一种反射放大攻击。目前，CLDAP协议被Windows服务器的活动目录服务（AD）广泛使用，通常AD服务会使用CLDAP协议在UDP389上接受查询请求并不经过身份认证直接回应大量的服务器信息，放大倍数70倍以上。

从2020年智云盾观测到反射型攻击的TOP5来看，SSDP反射攻击占比超过51%，NTP反射攻击占比超过26%，是最为活跃的两类反射攻击类型。

2.1 SSDP反射攻击

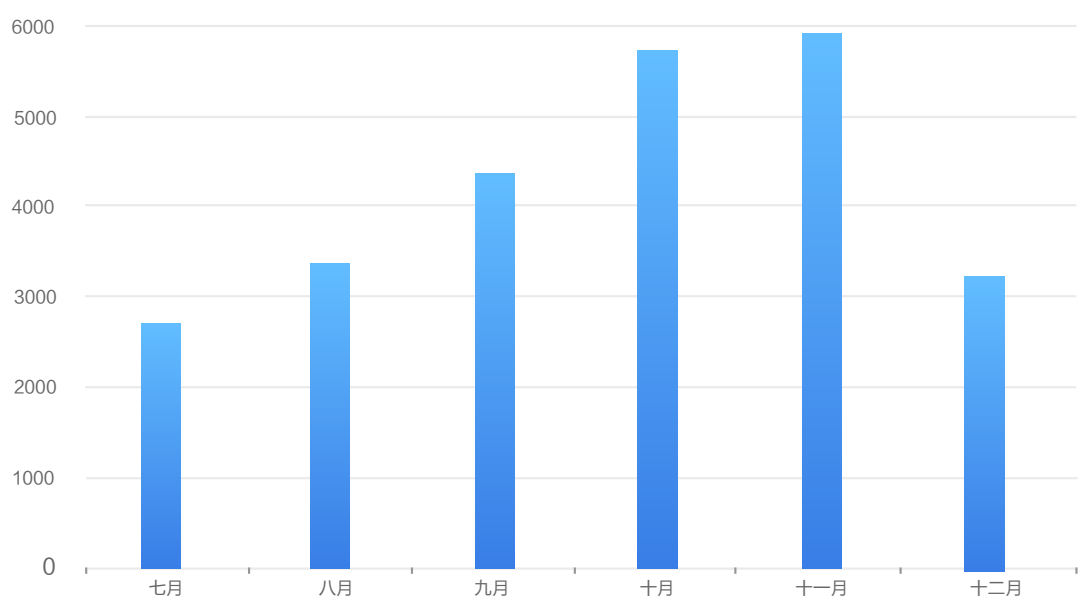
SSDP协议是局域网内的简单服务发现协议，在多播地址239.255.255.250和UDP1900上提供服务，SSDP服务的请求包小于响应包。RFC规定SSDP服务应用于局域网内部，但是一些服务使用者未按照规范，将SSDP绑定于互联网地址上，导致被黑客利用发动反射放大攻击，攻击放大倍数在30倍以上。

经统计，2020年发生的SSDP反射攻击事件在11月份达到顶峰，共计8301次。下图是下半年SSDP反射攻击事件统计数据：



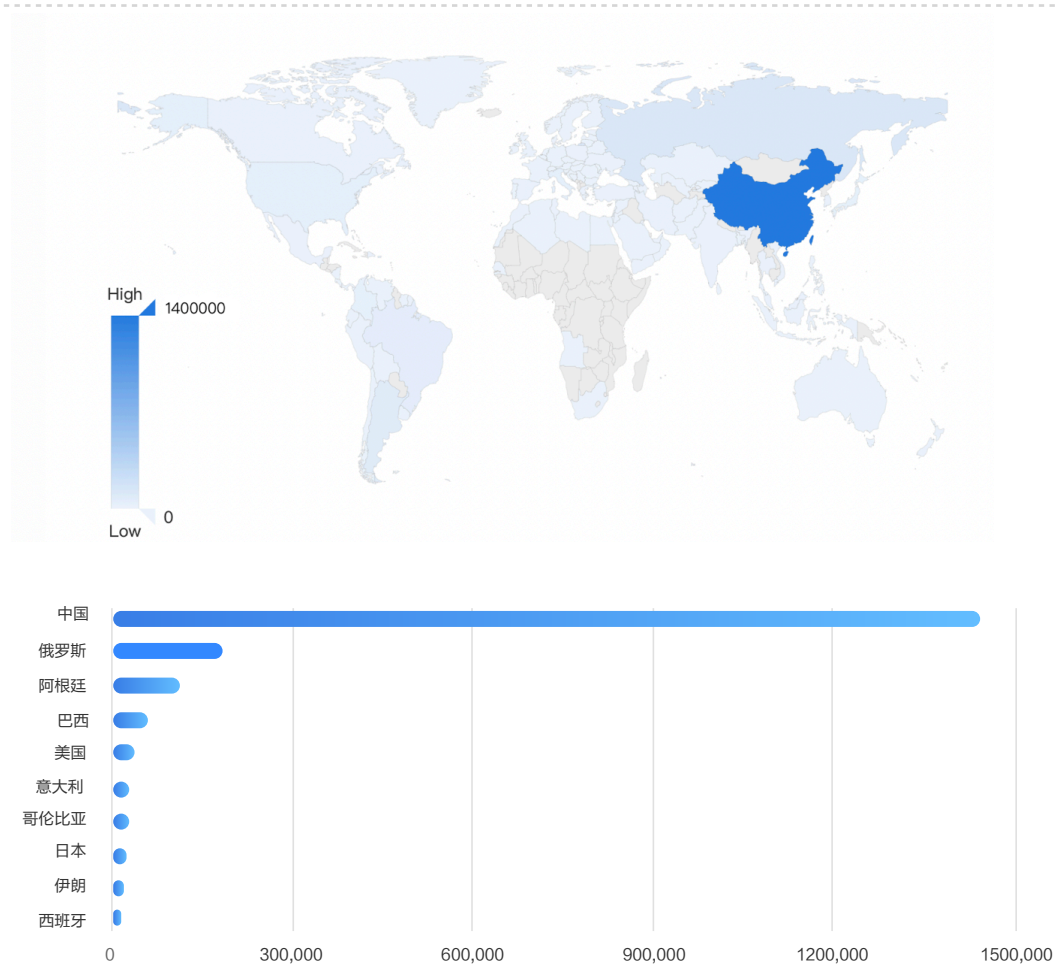
参与SSDP反射攻击的IP，极易被利用，威胁度较高。2020年攻击资源在11月份达到顶峰，达到了593672个，下图展示了高活跃IP的攻击态势：

下半年参与SSDP反射的IP分布

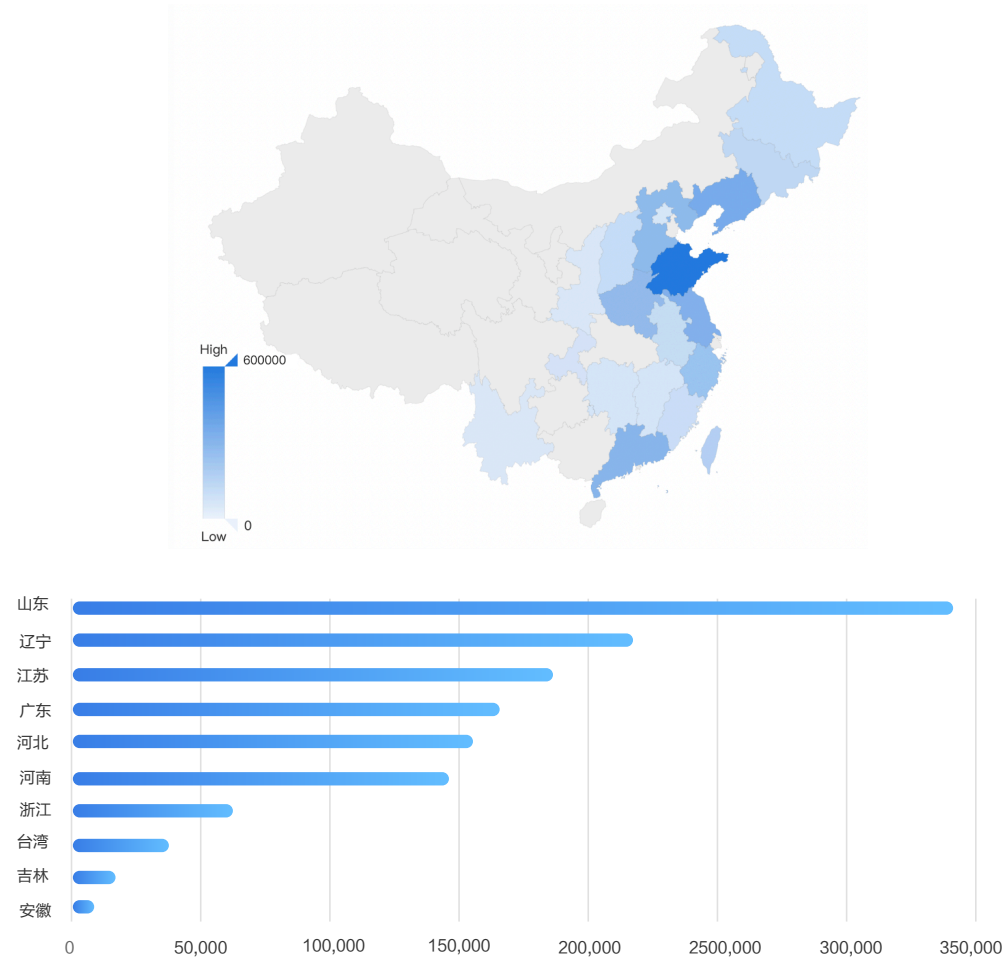


从全球分布来看，参与SSDP反射攻击的IP主要来自于中国，其次是俄罗斯。从国内来看，反射源IP主要分布与经济发达和沿海地区，其中山东、辽宁和江苏的反射源最多。这些地区往往部署了大量的网络基础设备，存在安全隐患的资源也较多。

SSDP反射源IP全球分布情况



SSDP反射源IP全国分布

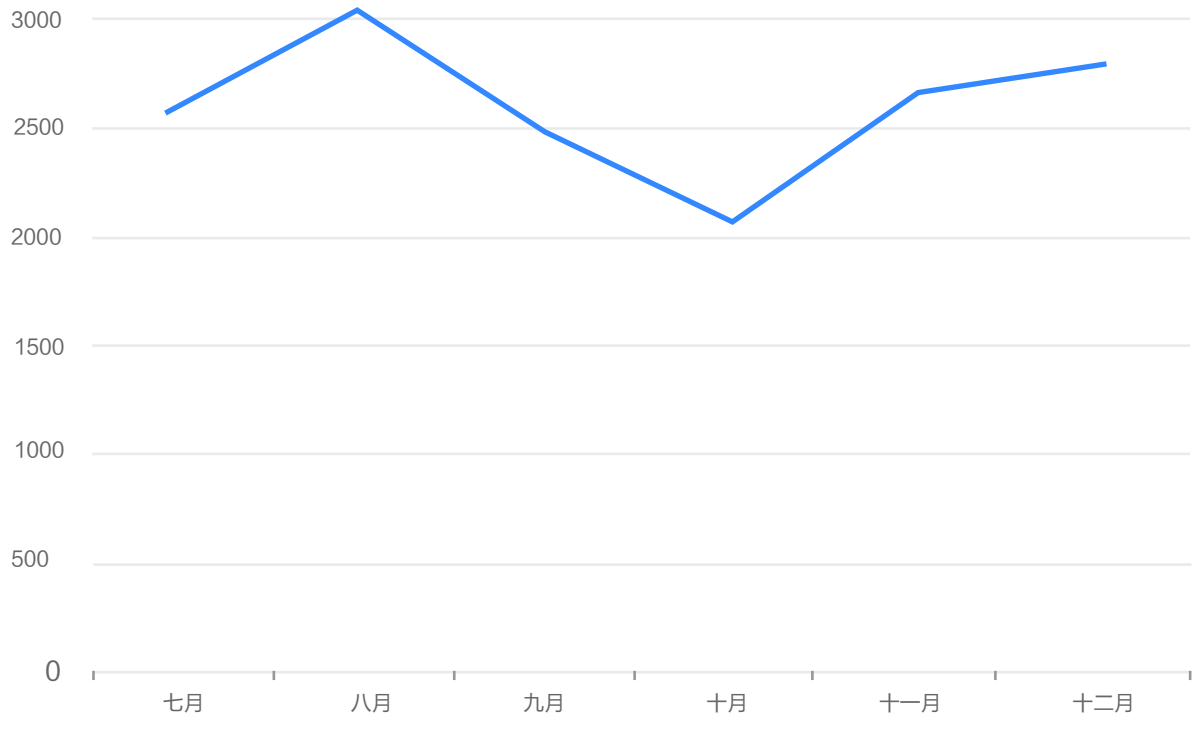


2.2 NTP反射攻击

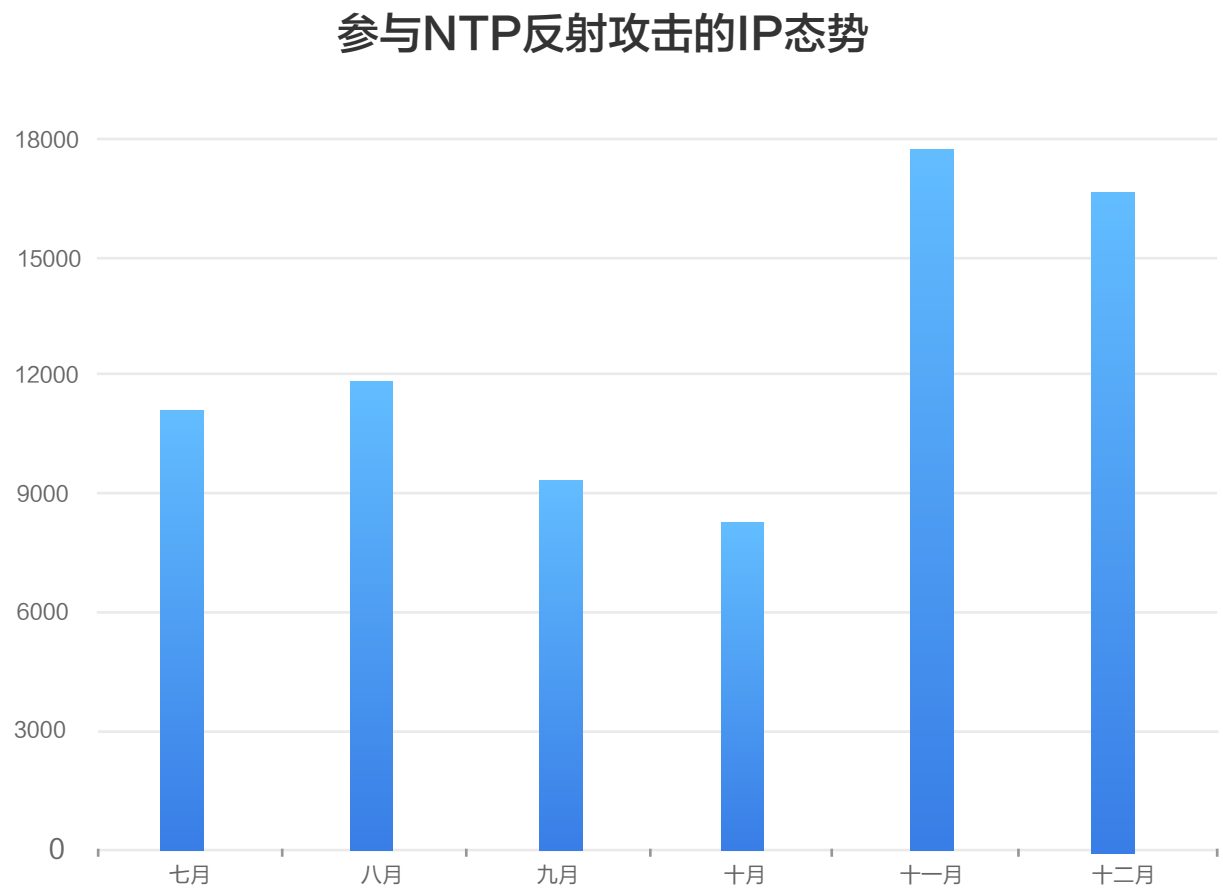
NTP是网络时间协议的简称，提供计算机之间时间同步服务，NTP反射攻击的原理是攻击者利用了NTP服务器实现的默认配置特征：提供monlist查询指令能够查询到默认高达600个历史IP信息的超大响应流。NTP反射放大倍数可以达到550倍。

经统计，2020年发生的NTP反射攻击事件在8月份达到顶峰，共计3097次。下图是下半年NTP反射攻击事件统计数据

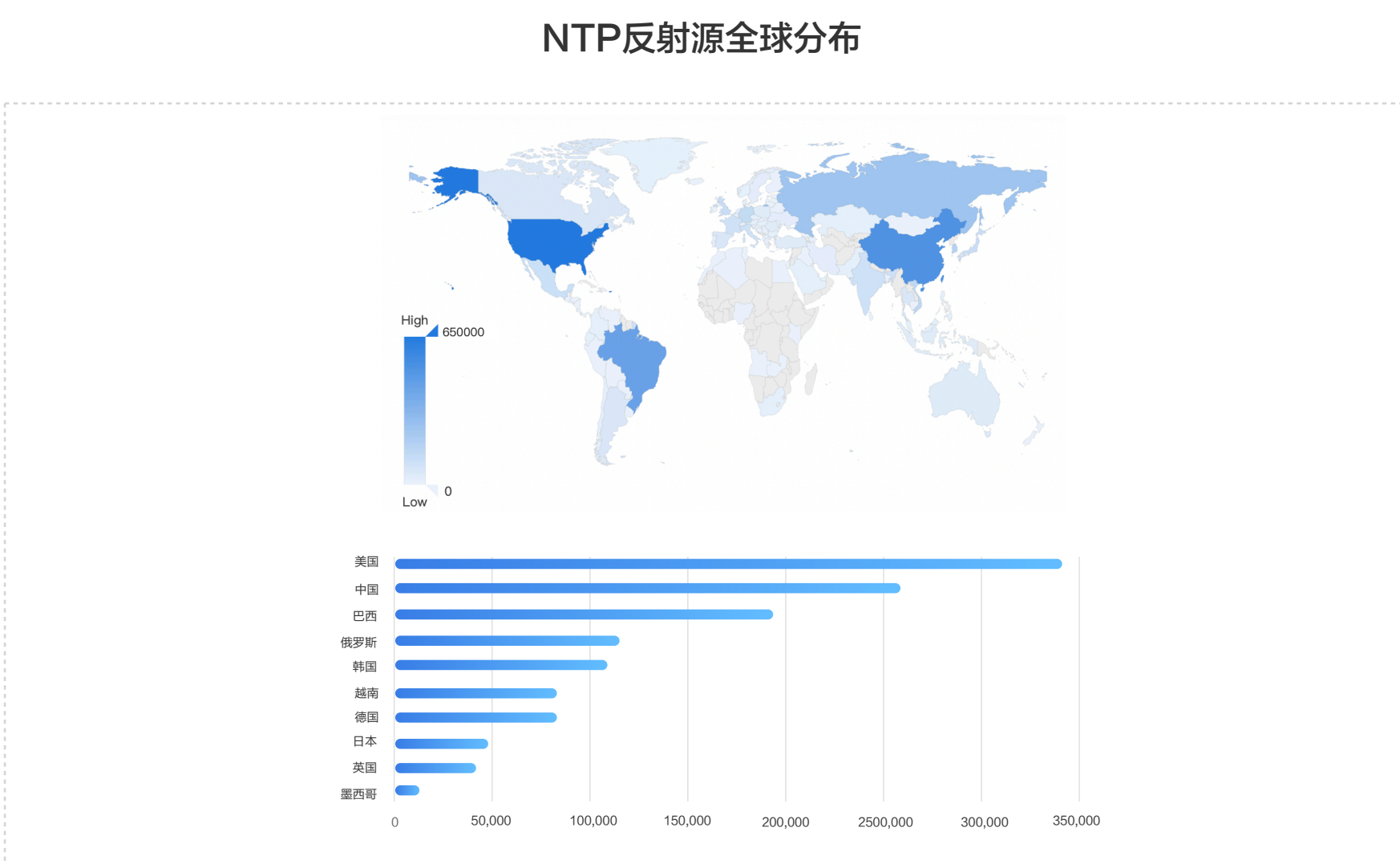
NTP反射攻击事件态势



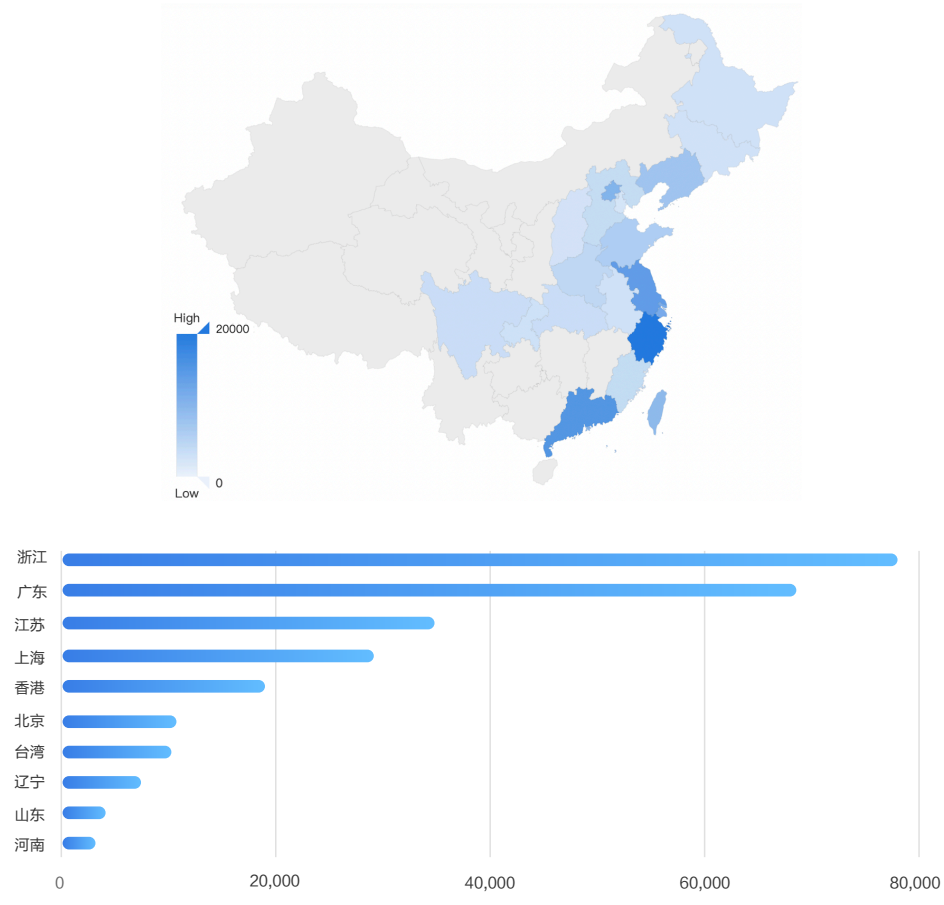
参与NTP反射攻击的IP，极易被利用，威胁度较高。2020年攻击资源在12月份达到顶峰，达到了593672个，下图展示了高活跃IP的攻击态势：



从全球分布来看，参与NTP反射攻击的IP主要来自于美国，其次是中国、巴西和俄罗斯。在全国范围内来看，主要分布在经济发达地区，其中浙江、广东和江苏被利用的反射源数量最多，由于发达地区的网络基建更加完善，网络设备数量较多，存在安全隐患的NTP服务也更多。



NTP反射源IP全国分布情况



03 新型攻击

3.1 ARMS反射攻击

2020年2月，智云盾团队发现了一种利用ARMS网络调试助手服务发起的反射放大攻击，ARMS服务运行在UDP3283端口，虽然不是网络公共服务，也没有被定义在RFC，但在网络上的分布情况具有跨平台的特性，客户端在向ARMS服务发送一个UDP最小包，ARMS服务会返回携带主机标识的超大包。攻击者利用这一特性发起反射放大攻击。攻击的放大倍数在12.7倍以上。

攻击首次发生以来智云盾系统多次监测到ARMS反射攻击，捕获到的反射源总计4865个。

参考链接：https://anquan.baidu.com/article/1050

3.2 黑客自建数万倍的反射源发动攻击

2020年3月底，智云盾团队在一次攻击事件审计中，发现其中一次DDoS反射攻击事件对应的采样报文中存在异常的反射数据包。经过研究发现，这些反射源接受单个UDP请求都会响应多个UDP大包，每个包长固定，响应数据包内容没有任何规律，并且单IP上开启了多个UDP端口提供类似服务。攻击的放大倍数接近4万倍。

参考链接：https://segmentfault.com/a/1190000022327366

3.3 RangeAmp攻击

2020年，中国研究人员发布了一种新型DDoS放大攻击，攻击者利用CDN对HTTP范围请求机制的实现存在安全缺陷的特点发动攻击，如果构造一个小字节范围的范围请求发起攻击，会造成CDN服务器不断的请求消耗源站服务器的带宽资源，如果构造具有重叠范围或具有许多小范围的范围请求，会造成CDN服务器之间传输非常的流量，从而消耗CDN节点的带宽资源。

RangeAmp攻击的攻击成本很低，影响范围广，而且放大倍数很高，这类攻击会严重威胁网站和CDN服务的可用性，研究人员针对主流CDN测试发现均存在安全漏洞，但是截止目前，仍未发现黑客利用该漏洞发动大规模的攻击。

参考链接：https://shenkaiwen.com/zh/news/2019_geekpwn_cdn/

3.4 NXNS攻击

2020年5月，以色列研究人员发布了一个新的DNS放大攻击，被称为NXNS攻击。攻击者利用DNS递归服务器发起指向恶意NS服务器的DNS查询请求，恶意的NS服务器返回包含大量的伪造域名的NS记录，使得DNS递归服务器又向受害的DNS授权服务器发送大量查询请求包从而拒绝服务，NXNS攻击可使流量放大1620倍。NXNS攻击比NX攻击更加高效和隐蔽，危害巨大，新版本的DNS服务器软件已经修复了此类漏洞。

参考链接：https://www.freebuf.com/articles/web/237392.html

3.5 TCP反射攻击

TCP反射攻击是攻击者把CDN、WEB站点类服务器当成反射源，向这些服务器发送连接请求，服务器收到请求后向被攻击目标IP地址发送SYN-ACK，如果攻击者伪造大量相同SYN报文并随机设置seq号，就很容易出发TCP服务器反射ACK。如果TCP服务器端口不开放则会回应RST-ACK。现网遇到的TCP反射攻击流量已经从SYN-ACK转变为ACK、RST与RST-ACK，这些反射数据包都是真实IP的流量，较难防护。

2020年智云盾监测到的TCP反射攻击事件总计达到44103次，与2019年相比有明显增长，可见这种攻击方式有愈演愈烈之势。

3.6 Plex反射攻击

2021年1月，智云盾团队发现了一种基于Plex媒体播放平台的DDoS反射攻击，正常工作的Plex服务监听的32410和32414端口在收到一个小包查询请求时会响应包含服务器信息大包。

智云盾后续跟踪发现，Plex在1.2版本后修复了问题，不过通过搜索全网数据库的数据发现，仍然有大量的Plex服务存在安全漏洞，容易被黑客利用发动攻击。

参考链接：

https://www.bleepingcomputer.com/news/security/plex-media-servers-actively-abused-to-amplify-ddos-attacks/

3.7 DTLS反射攻击

2021年1月，智云盾团队跟踪研究了一种基于DTLS协议的反射攻击，经过深入分析，这种攻击是黑客利用DTLS协议未启用HelloVerifyRequest安全认证机制的漏洞发起的反射攻击。DTLS协议反射攻击放大倍数在26倍以上。

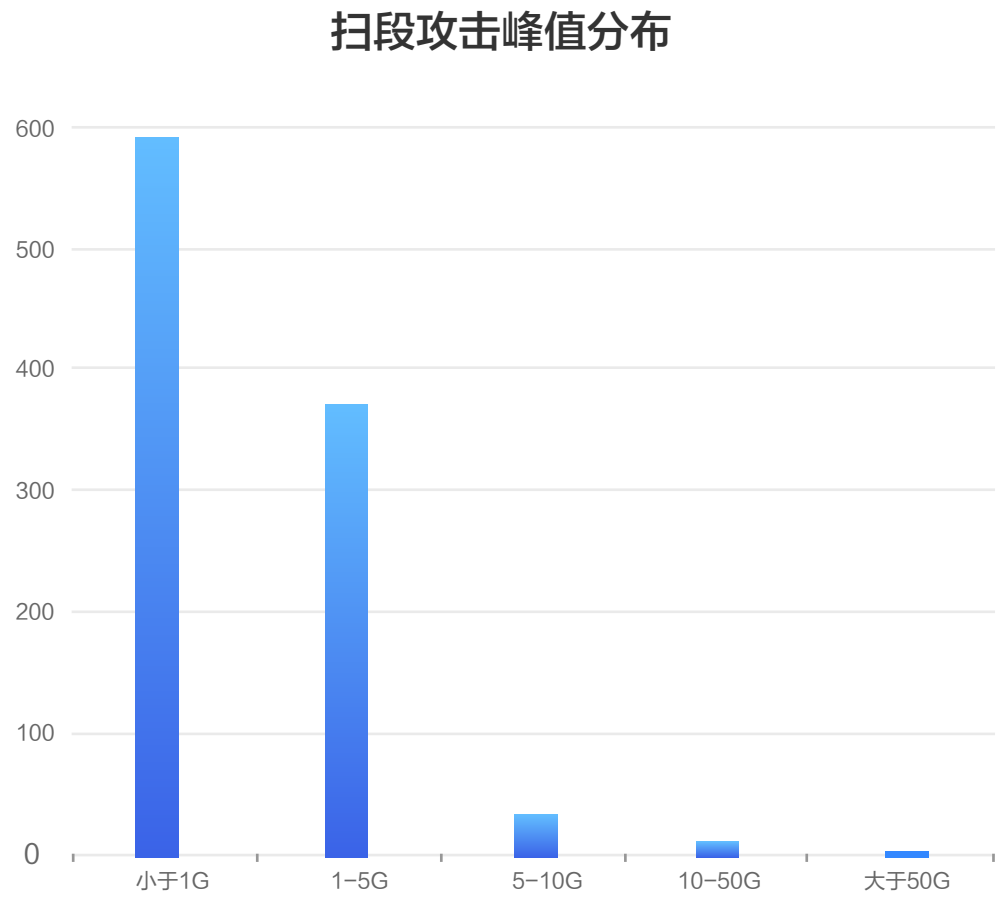
攻击首次披露以来，智云盾系统总计监测到多次DTLS反射，总计捕获的反射源达8904个。

参考链接：https://paper.seebug.org/1482/

3.8 扫段攻击

扫段攻击顾名思义是对一大段IP同时或顺序地实施DDoS攻击，同时攻击的情况下每个目标IP所受攻击流量较小，全部加一起则很大；顺序攻击时，每个IP遭受攻击流量很大，但持续的时间很短。也可以说扫段攻击是一系列关联的DDoS攻击事件的组合，但是攻击者会对攻击目标、攻击时长，攻击频度进行不断的变化，这给传统的DDoS监测和防御提出新的挑战。

智云盾监控到此类攻击态势全年达到了974次，其中9月份出现的次数最多，达到了218次，下面是全年扫段事件的趋势



04 典型案例

DDoS攻击与防御是一场没有硝烟的网络战争，我们每一次的检测与防御，所面对的不仅仅是一个个简单的字符与协议，而是一个个有真正犯罪分子组成的黑客团体。他们为了勒索、同行竞争、或其他利益相关的驱使。使用骚扰或大流量的攻击，对受害者进行威胁恐吓，以达到其不可告人的秘密。

在2020年度，百度安全智云盾团队针对这些攻击，进行分类和大数据分析后，也发现了形形色色的各类黑客团体。他们大多，手法专业，拥有大量的攻击资源。其中一个名为“七色光”联盟的团伙在2020年度尤为活跃，大量的中小站长深受其害。

“七色光”联盟黑产团伙

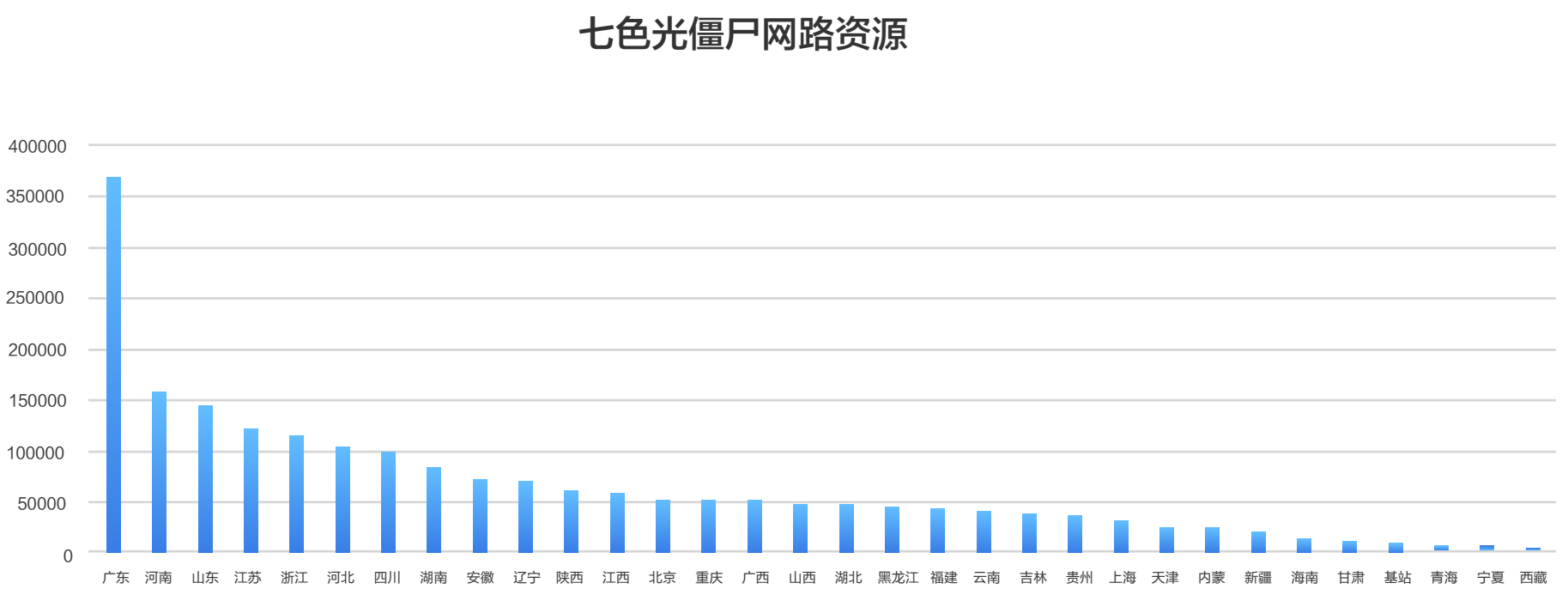
"七色光"联盟是2020年兴起的黑客团伙，使用DDoS和CC攻击对大量的中小站长进行敲诈，并勒索站长挂违法广告。粗略估算受害网站超过1000家，逐步演变成互联网的“毒瘤”。

掌握资源

七色光联盟掌握超过200万个恶意IPv4资源，30万个恶意IPv6资源。

能够发起超过500万QPS的CC攻击和400Gbps的DDoS攻击。

对整体的恶意IP资源进行汇总分析，国内遍布32个省，位于广东省的恶意IP以绝对优势排行第一。



从恶意IP资源的属性角度分析，99%以上的恶意资源是动态IP。

攻击特征

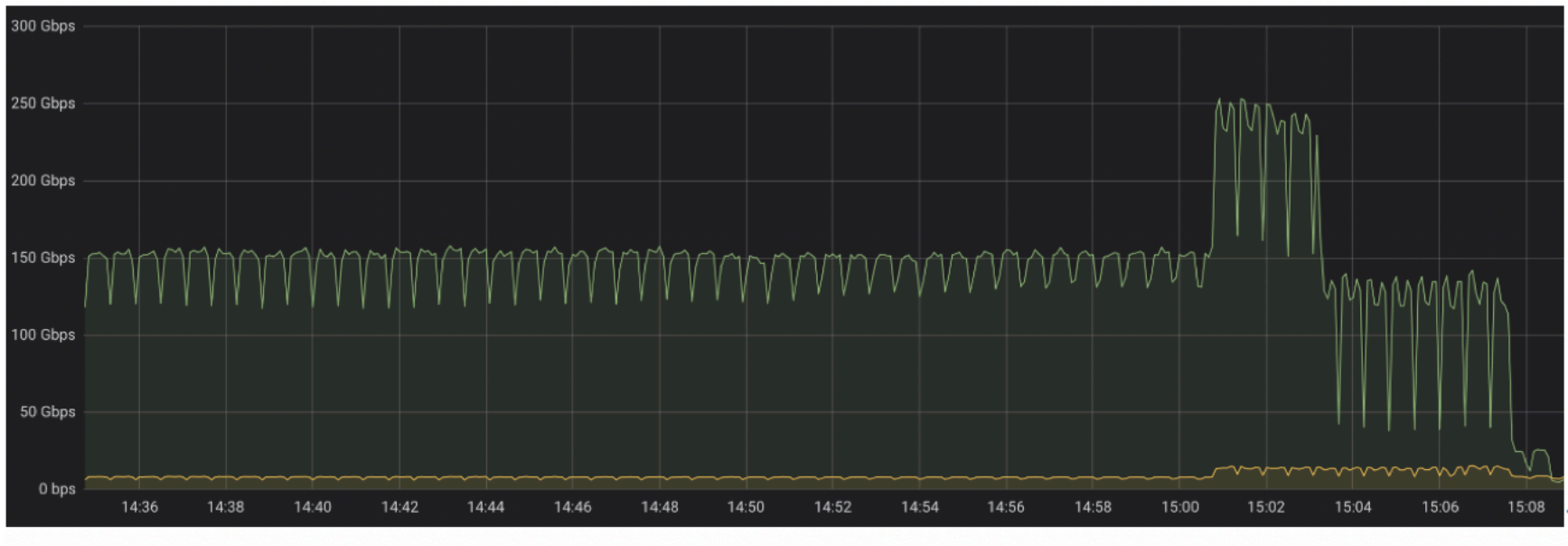
主要使用DDoS攻击和CC攻击，对网站进行攻击。
DDoS攻击：
攻击类型：使用SYN Flood，ACKFlood以及ICMP反射攻击
攻击时长：多为持续发起6个小时以上的大流量攻击
攻击特点：不使用反射倍率较大的反射攻击
攻击能力：大于300Gbps

CC 攻击：
攻击类型：单URL或者首页访问
攻击时长：多为持续发起6个小时以上的超大请求攻击
攻击特点：CC攻击有明显的特征，UA为GBK编码的中文字符’\xB2\xBB\xCA\xCA\xD3\xC3UA’（中文编码：不适用UA）。
攻击能力：大于500WQPS

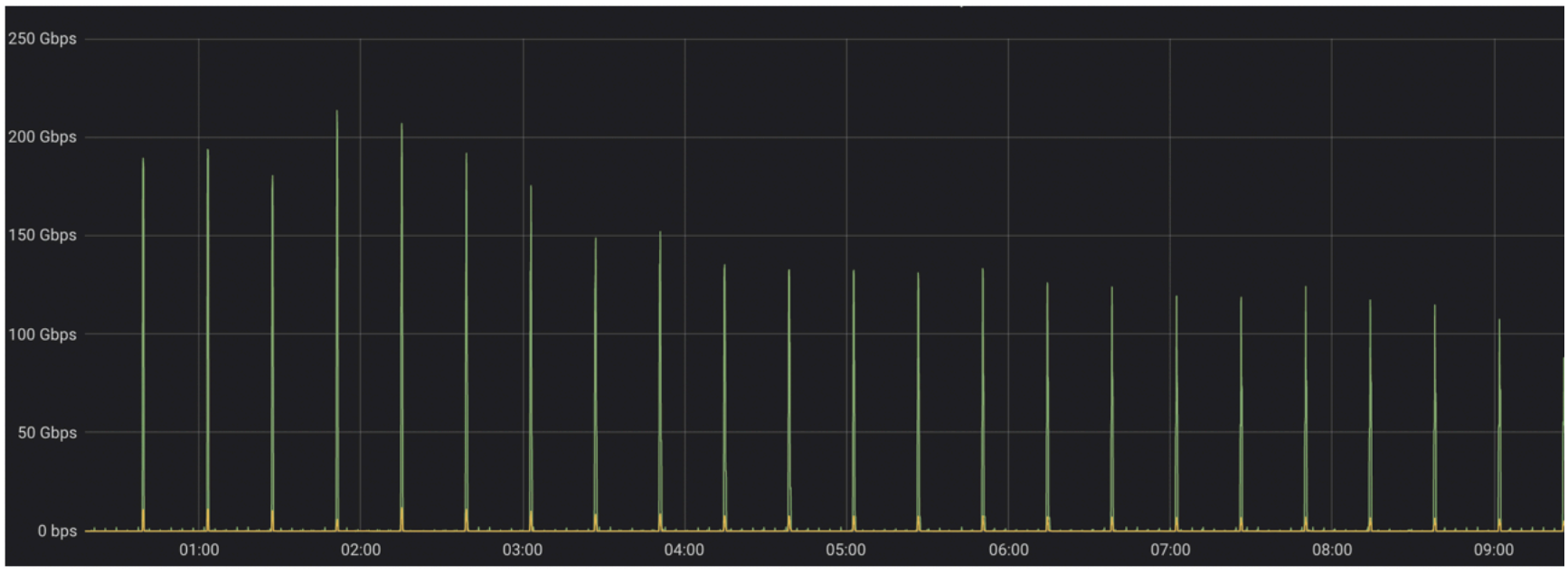
攻击手法

勒索途径主要使用非法盗用的校园邮箱发送威胁邮件，胁迫站长发布欺诈广告，传播非法违规恶意APP等。攻击方式主要是流量攻击和CC攻击混合，当普通的流量攻击失效时，会采用余弦式或者脉冲式攻击手法动态攻击网站，攻击方式如下图：

余弦式攻击



脉冲式攻击


250 Gbps
200 Gbps
150 Gbps
100 Gbps
50 Gbps
0 bps
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00

结语

2020年攻击统计分析数据告诉我们，网络安全形势依然严峻。尽管公安部“净网”行动效果显著，尽管工信部网络安全威胁信息共享平台增强了网安事件的协同处置能力，但黑产处心积虑利用各种攻击手段获取高额利益，致使DDoS攻击和各种网络入侵攻击依然频发，APT攻击也更多的发生。同时，AI、物联网、5G等各种高新技术的不断兴起和应用，加大了网络安全边界泛化的程度，让攻击者有了更多可乘之机，境外APT组织也从未停止对我国境内重点网络设施的各种渗透和攻击。面对日益复杂的网络安全空间环境，唯有不断推陈出新，研究创新且行之有效的安全应对策略和手段，才能做到魔高一尺道高一丈，洁净网络空间，保障国家网络关键基础设施安全。