阿里云

2019年
DDoS攻击态势报告

阿里云安全

2020. 01

2019年， 阿里云安全团队监测到云上DDoS攻击发生近百万次，日均攻击2000余次，与2018年整体持平，但相比2019年上半年有所下降。同时，应用层DDoS（CC攻击）成为常见的攻击类型，与2018年相比，攻击手法也更为多变复杂。阿里云为全球上百万客户提供了基础安全防御。本报告中将以多个维度对2019年全年发生的DDoS攻击进行全方位分析，希望能够为政府、企业客户及科研机构提供一定的参考价值。

01 概述

SUMMARY

相比2018年DDoS攻击数量持平。经过分析发现，百G以上攻击呈现成倍增长，成为标准攻击流量，相比于2018年上升了103%。500G攻击相比2018年增长了50%，并出现持续2个月的近Tb级攻击。同时利用Memcached反射攻击相比2018年增长40%，在2019年1月达到峰值，经过有关部门以及企业的联合治理，目前已经呈现明显下降趋势，下降至峰值的20%。应用层DDoS的攻击同样猛烈，半数以上的攻击QPS超过2W，20%的攻击QPS超过10W，峰值突破数百万QPS的攻击事件也屡屡出现。

02
攻击态势
ATTACK

1. 攻击趋势

根据阿里云安全团队监测到的攻击数据分析，2019年全年，100Gbps以上大流量攻击事件达到了1.8万余次，相比于2018年上升了103%，与此同时，持续2个月最高攻击流量达900Gbps，单次流量超百G呈现快速增长趋势，成为了标准攻击流量，如图2-1所示。应用层DDoS的攻击同样猛烈，半数以上的攻击QPS超过2W，20%的攻击QPS超过10W，最近半年每个月最高攻击QPS均超过百万。

攻击类型中UDP反射攻击仍然为主要攻击手段，得益于国家安全部门、运营商、云厂商和IDC对于反射源治理，大流量攻击的整体情况呈现下降趋势，如图2-2所示。

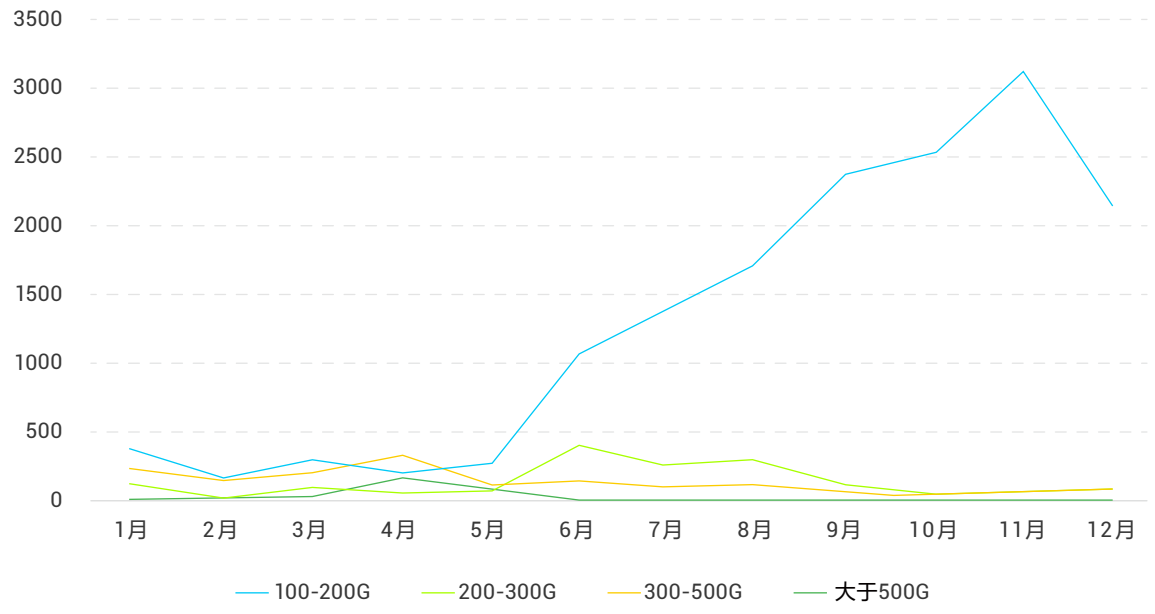

图2-1 2019年峰值流量大于100Gbps事件分布

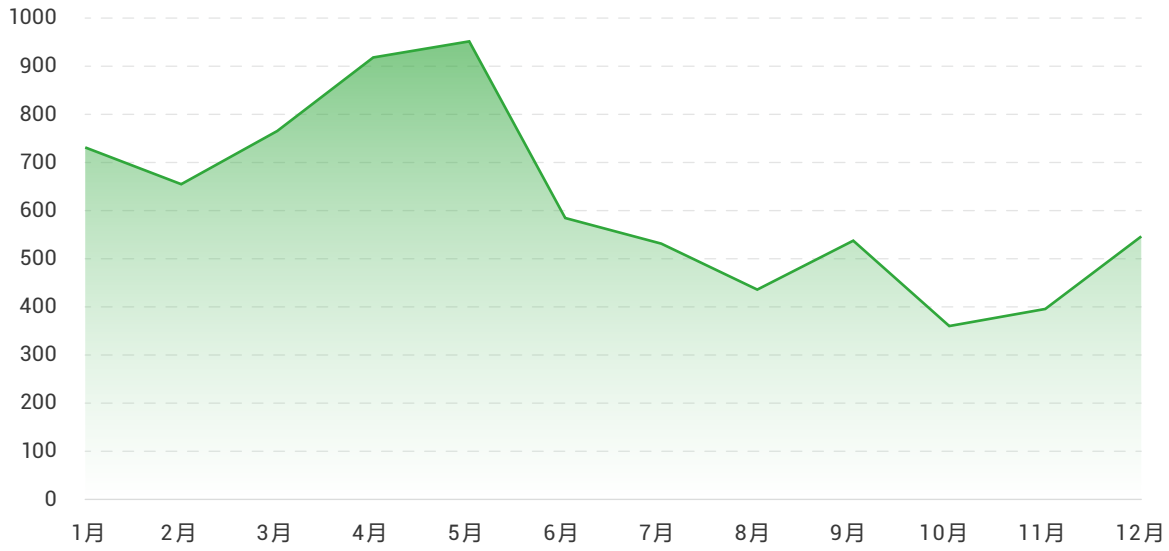

图2-2 2019年大流量攻击峰值流量趋势

2. 攻击行业分布

互联网服务及游戏行业，在2019年依旧为主要的攻击目标，二者遭受了60%以上的攻击，如图2-3所示。

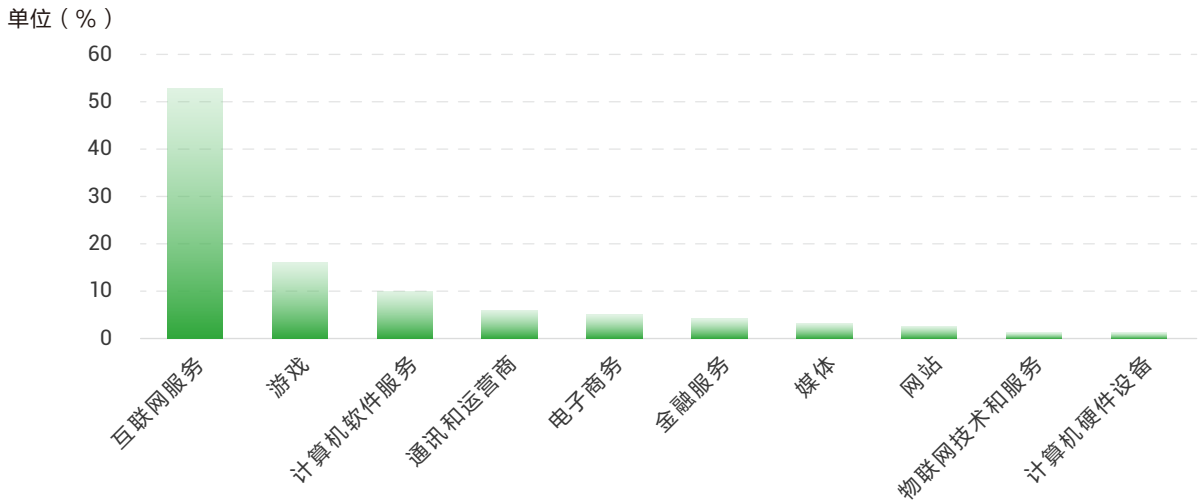

图2-3 DDoS事件行业分布

3. 大流量攻击种类分布

当前检测到的大流量DDoS攻击类型中，分布最多的分别是 UDP Flood、SYN Flood、以及Memcached、NTP 等反射攻击，如图2-4所示。

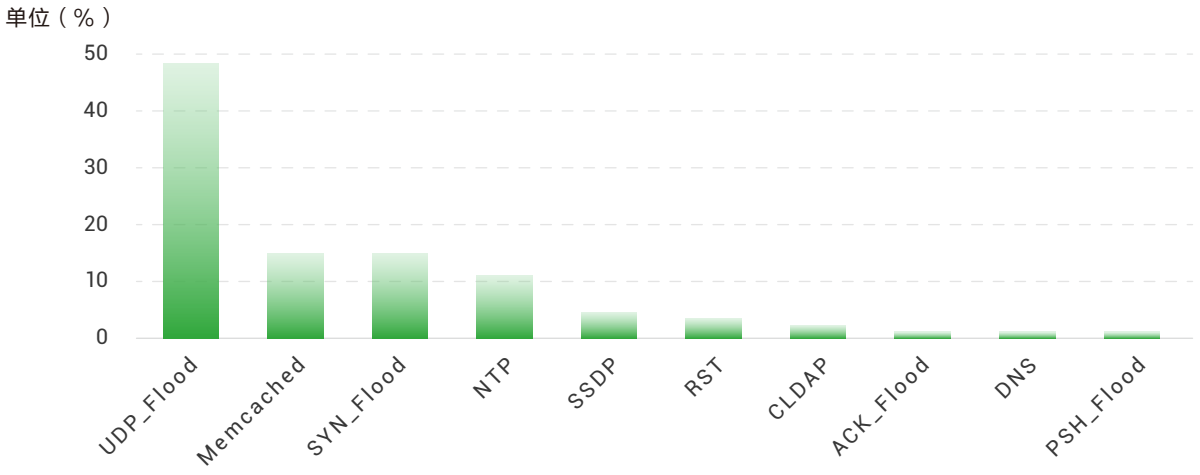

图2-4 2019 年 大流量DDoS攻击种类分布

从全年的整体攻击趋势来看，Memcached反射放大攻击次数在1月达到了顶峰，随后有了明显的降低，下半年攻击次数相比于上半年，整体呈下降趋势，原因与全国范围内的网络安全治理有关，如图2-5所示。

图2-5 2019年Memcached反射放大攻击事件数

同时NTP反射攻击在6月份达到峰值7000余次，后续逐月降低，目前稳定在千余次，如图2-6所示。

图2-6 2019年NTP反射放大攻击事件

4. 应用层DDoS攻击手法及演变

应用层DDoS的攻击手法在2019年变化极大，且不同的攻击手法对防御能力要求均不相同。下面列举几个2019年常见攻击手法：

1）被挂马设备植入攻击脚本调用系统浏览器发起攻击

此类攻击方式相对传统，设备被植入木马沦为肉鸡。但由于攻击脚本调用的是系统浏览器，往往可以简单粗暴地绕过一些简单的人机校验手段，这要求防御系统要更为智能地精准判断恶意流量，并直接做出阻断或采用更严格的校验手段，在压制攻击的同时避免对正常用户的打扰。

2）热门网页嵌入攻击代码

大量用户在相近的时间浏览了一些不正规网站的热门网页，页面被攻击者事先嵌入了攻击代码。用户浏览网页的过程中，页面会不断请求目标网站的资源，对目标网站发起攻击。年初特别频繁的利用HTML5的ping特性发起的攻击就属于此类攻击方式。由于浏览网页的用户不断进入、离开，传统拉黑IP的方式无法完全压制攻击流量，要求持续的安全攻防研究，以及智能的防护手段。

3）山寨APP植入攻击代码

大量用户在手机上安装了某些伪装成正常应用的恶意APP，该APP在动态接收到攻击指令后便对目标网站发起攻击。此类攻击方式使得海量移动设备成为新的攻击源，黑灰产无需让单个源IP高频攻击，同时由于攻击源多为大型出口IP，传统的防御方法简单粗暴的将攻击IP拉黑，这些IP背后的大量正常用户也将无法访问。此类攻击方式打破了“限速+黑名单就能一招制敌”的幻想，要求更为纵深、智能的防护手段。

4）通过高匿代理发起攻击

该方式本身比较传统，但通过高匿代理发起的攻击，攻击调度快，成本较低，更易控制攻击节奏及攻击量。2019年此类攻击手法发起的攻击，有明显的攻击量大、攻击复杂多变的特性，要求更为智能、体系化的防御系统。

上述这些攻击手法除了挂马设备攻击，均在2019年存在明显的阶段性热度。2019年年初热门网页嵌入攻击代码的占比较高，并逐步出现山寨APP植入攻击代码这一攻击方式，后者在第二季度初热度到达巅峰，之后此类攻击出现频率下降。2019年下半年通过高匿代理攻击变得极为常见，此类攻击在2019年上半年占比不到10%，该比例在下半年急剧攀升至60%+。

从攻击时长看，2019年下半年单次攻击的攻击时长明显下降，从平均单次攻击数个小时缩短至不到一小时，并开始出现针芒状的应用层DDoS攻击，如图2-7所示。同时，在更短的攻击时间内，出现多种攻击手法混合。

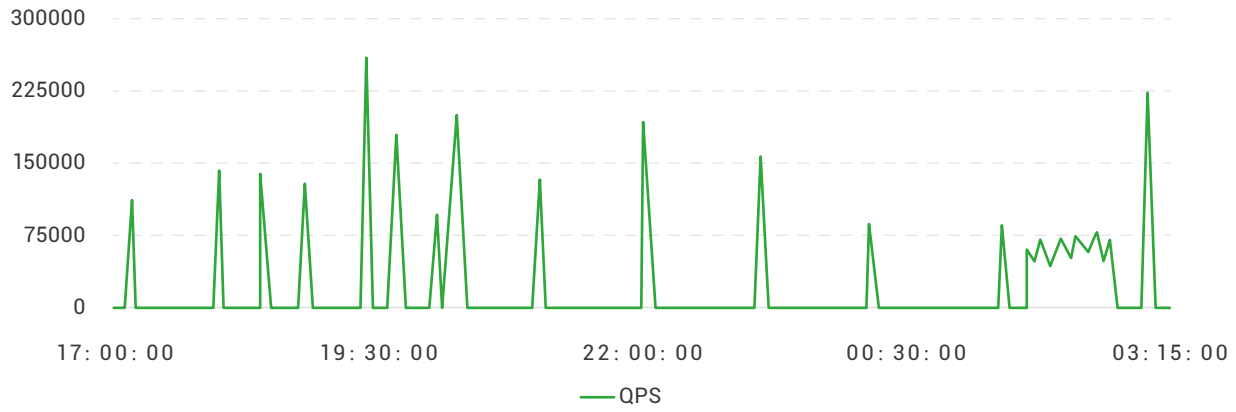

图2-7 针芒状应用层DDoS攻击

5. 核心观点

与2018年相比，2019年DDoS攻击的数量虽然持平，但DDoS攻击的攻击强度变化更为激烈。百G以上攻击成倍增长，同时Tb级别流量，千万级并发攻击出现，让DDoS攻击对抗更为激烈。得益于云计算原生的资源弹性可扩展优势，云上企业在应对DDoS攻击时不会受到传统带宽资源的限制，只要采取合理正确的防护措施，都能成功应对攻击。

法律法规：

得益于政府、运营商等对于网络安全的重视，以及对互联网环境的治理，对于大流量DDoS攻击有着显著的抑制作用；

攻击手法：

随着防护手段的演进，黑客们的攻击手法也同样地发生变化。去年有效的防护方式，在今年可能已经不再具备防护效果。人工调整策略在当前的攻击态势下越来越无法抵御住攻击，防御系统需要自动化地快速区分恶意和正常访问，并从中提取出攻击模式，快速下发，压制攻击。与此同时，更快的攻击节奏也使得默认防御能力日趋重要，需要对攻击手法、攻击源进行自动化分析，在此基础上构建信誉系统，默认压制攻击流量；

攻击对象：

互联网上的攻击，不仅仅是基于对利益的追逐。互联网的基础设施也不会因为只是提供基础服务不存在利益冲突就会免遭攻击。由于各种原因，例如是炫耀、误伤、甚至是故意为之等因素，互联网基础设施也同样会成为间接或者直接的攻击目标对象；

攻击团队：

通过对部分DDoS攻击进行溯源，我们发现海外团伙发起的DDoS占比呈现上升趋势，其中以东南亚地区分布较为集中；

攻击地域：

从全球的攻击态势来看，随着国内业务出海趋势的增多，东南亚地区遭受的攻击最为密集。

03

DDoS僵尸网络分析

ANALYSIS

1. 木马家族分布

在TOP10的木马家族中，2019年除了之前常见的Mirai和Gafgyt之外，DDoSTF也进入前三，三者的总占比达到了65%左右，如图3-1所示。

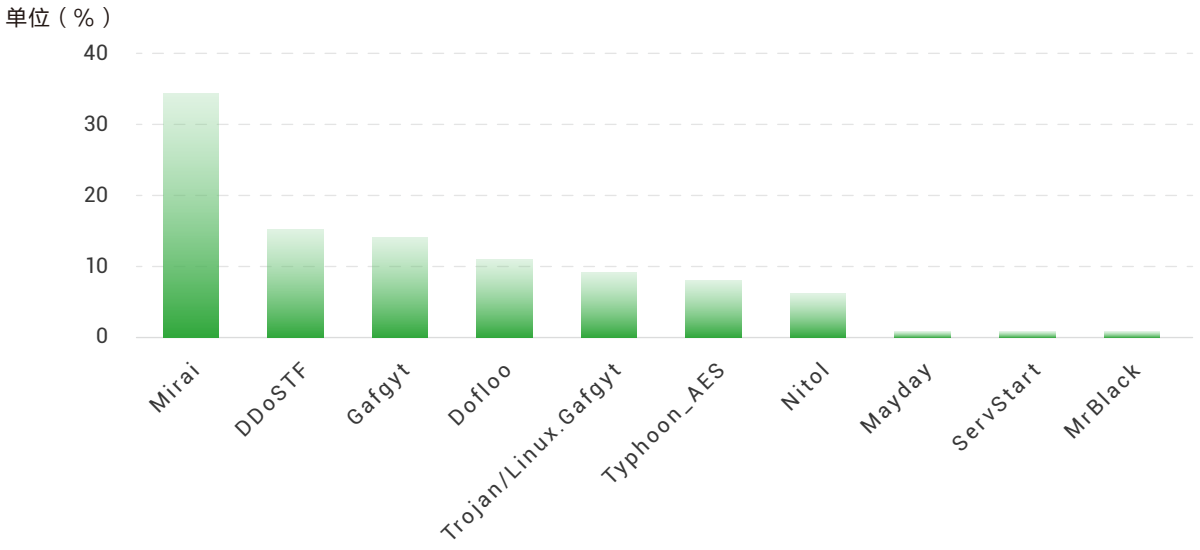

图3-1 DDoS木马家族分布

2. CnC国家及地区分布

在僵尸网络分布情况方面，有53%来自中国大陆，相比于2018年，下降了近20%，与此同时，来自美国和中国香港的僵尸网络分别占比21%和8%，相比于2018年，都有不同程度的上升。由此可见，僵尸网络的控制端在逐渐向大陆以外的地区进行转移，详情见图3-2。

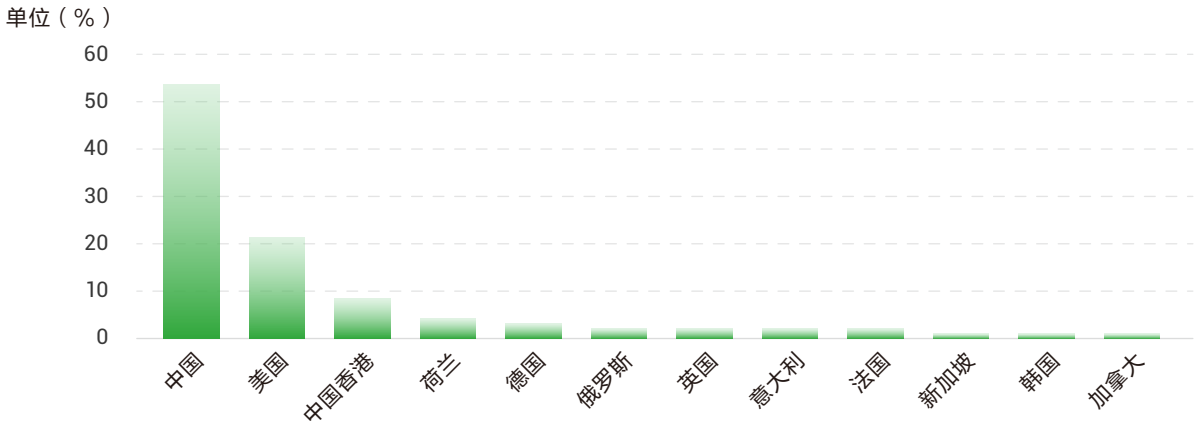

图3-2 CnC 国家及地区分析

3. CnC存活时间分布

通过对CnC存活时间进行分析和整理，存活一周以上的CnC占到了33%，相比于上半年下降了14%，对比整个2018年度，有小幅度上升。

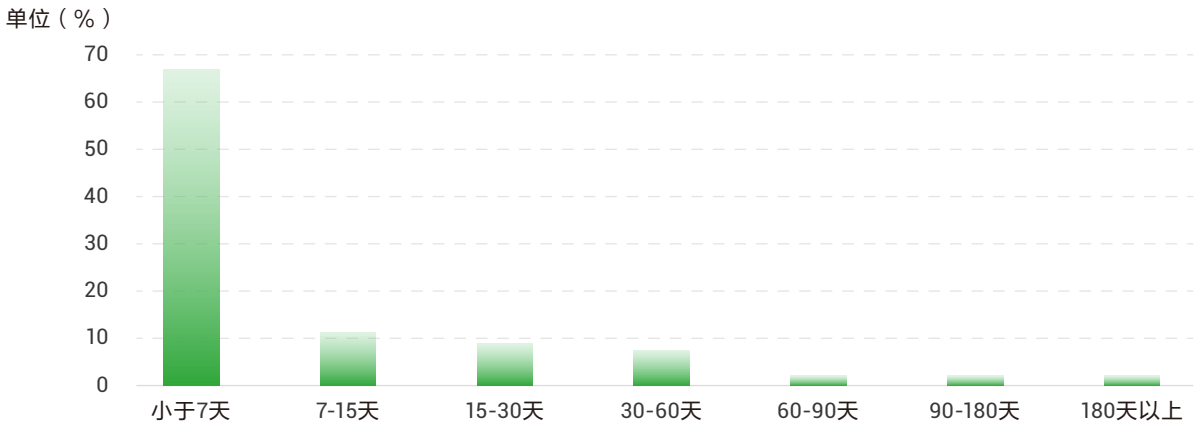

图3-3 CnC 存活时长分布

04

DDoS肉鸡分析

ANALYSIS

1. UDP反射源国家及地区分布

2019年，UDP反射源主要还是来自于国内，俄罗斯和美国分别占5%和4%，相比于2018年，俄罗斯和美国的反射源数量有所降低，而国内反射攻击源大幅增加。

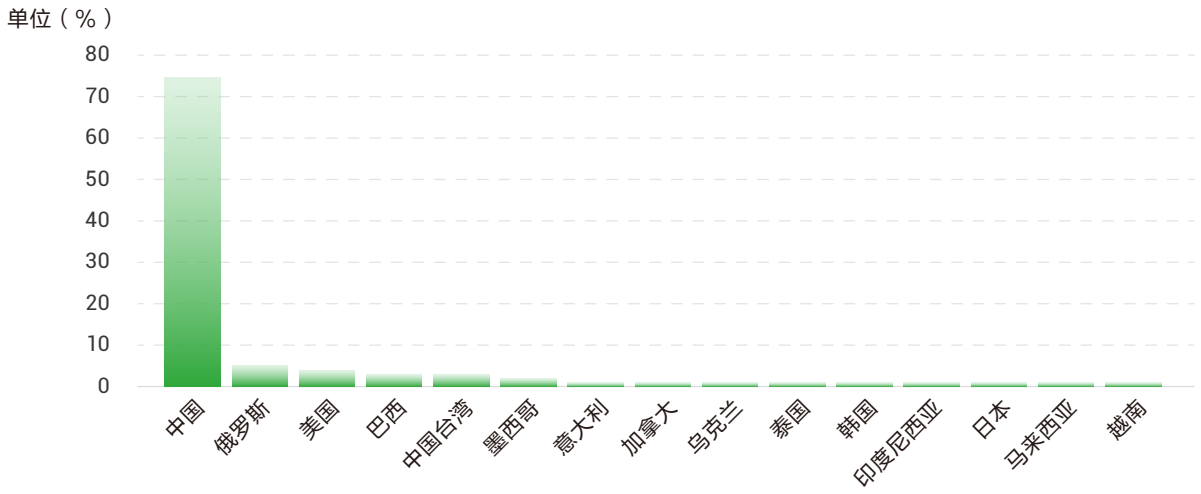

图4-1 UDP 反射源国家及地区分布

2. 肉鸡国家分布

据统计，2019年全年对全球发起的DDoS攻击事件中，美国和中国分别占有了35%和34%的肉鸡IP总量。有近65%的肉鸡IP来自于海外地区。因此在进行DDoS防御时，可进行一定程度上的海外封禁，从而降低攻击对用户带来的影响。

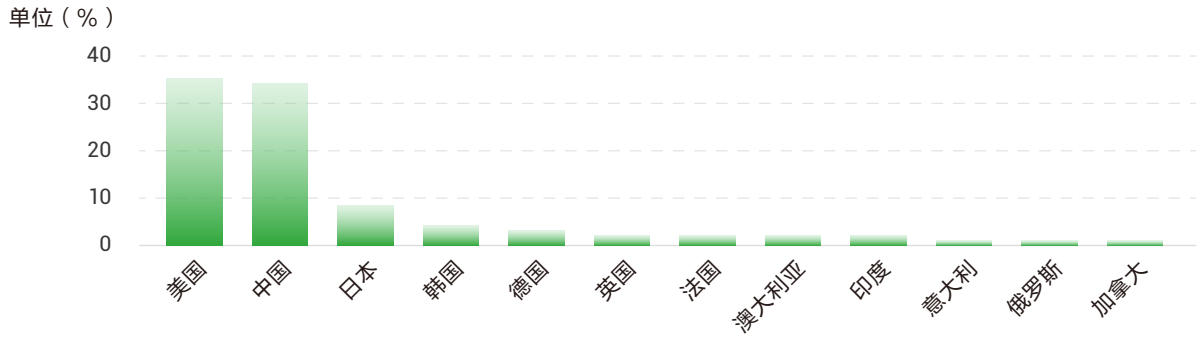

图4-2 肉鸡国家分布

3. DDoS攻击运营商分布

DDoS的攻击运营商分布方面，国内的三大电信运营商为主要的攻击流量来源。

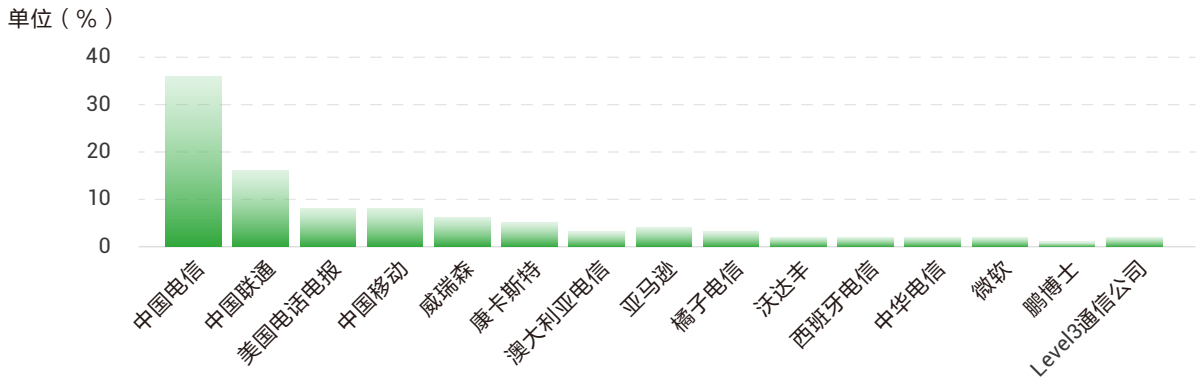

图4-3 DDoS 流量运营商分布

05

典型案例

CASE

1. 高并发连接型DDoS攻击

2019年10月，阿里云的单个云上租户遭遇了高并发的连接性DDoS攻击，黑客动用了数十万的肉鸡资源，攻击手法为建连之后向服务器发起高频率的恶意请求。当时的连接型DDoS攻击流量将近100Gbps，并发连接数峰值超过了1200万，同时每秒新建连接数也高达170万。

这个量级的攻击在传统网络当中，不光会影响被攻击的IP地址，而且可能会影响到用户的其它应用，甚至可能会波及到其他用户。阿里云云盾高防充分利用云上灵活快速的调度特性，迅速识别出被攻击对象并进行自动隔离，保证攻击流量不会影响用户的其它业务，控制影响面，有效保障云上其他用户的稳定性。同时防护机制自动启动，准确识别出攻击流量并实施清洗，客户业务在分钟级别内恢复正常。

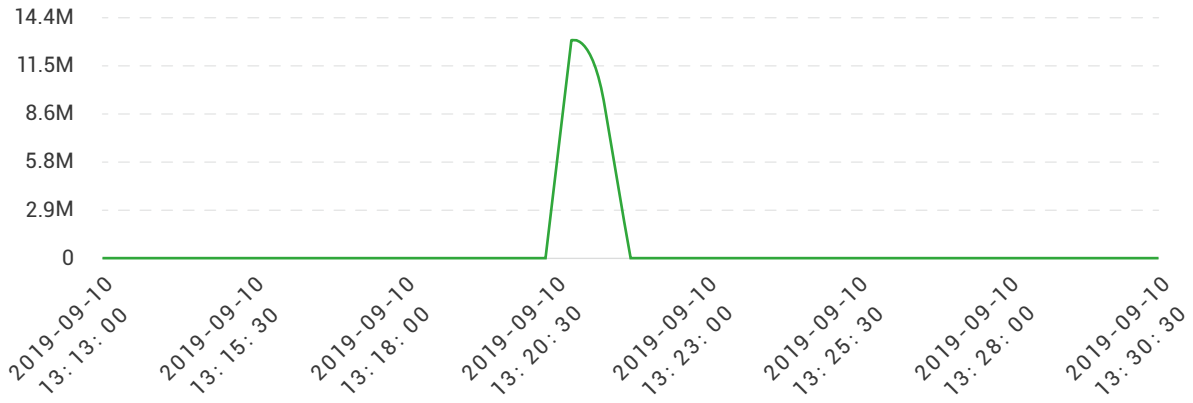

图5-1 高并发连接型攻击

2. 社会责任

DDoS攻击是公认的网络毒瘤，在互联网的虚拟社会当中，是典型的“以大欺小，仗势欺人”的不公平行径。为了尽到社会责任，**自2019年开始，阿里云DDoS高防团队面向所有企业承诺提供全球24小时免费应急服务。**5月中旬的一个周末，广州某初创公司，遭到一个黑客组织的勒索。黑客通过DDoS攻击方式致使公司业务中断，并主动联系该公司，声称缴纳一笔赎金之后，就可以保障公司的业务顺利运行。

如果向黑客屈服的话，这一幕难保不会在将来再次上演，因此该公司并未向黑客缴纳赎金。在了解到阿里云的24小时免费应急服务之后，当天晚上，该公司创始人就找到了阿里云高防团队，以寻求帮助。高防团队第一时间与客户进行了沟通，并按照承诺提供了免费的防护服务。之后，勒索组织果然如期再次发动攻击，攻击持续了30分钟左右，最初攻击手法以反射攻击为主，采用了DNS反射等手段，攻击峰值数十G；由于有阿里云高防的防护，客户业务未出现异常状况。黑客见大流量攻击无法凑效，便开始对客户的业务域名实施应用层DDoS攻击，QPS最高将近10K，在阿里云安全团队的协助下，客户业务域名始终处于正常在线状态。

在面对黑客勒索时，我们不能向黑客妥协，因为这样不仅不利于解决问题，反而会助长黑客的气焰；建议企业寻求专业的DDoS防护团队的帮助，来应对黑客的攻击。同时在条件允许的情况下，保留相关的证据，在合适的时机报案，净化网络空间环境。

阿里云为遭受DDoS攻击的企业，提供免费24小时黄金急救服务，如果您有需求，请钉钉扫码联系我们。

阿里云