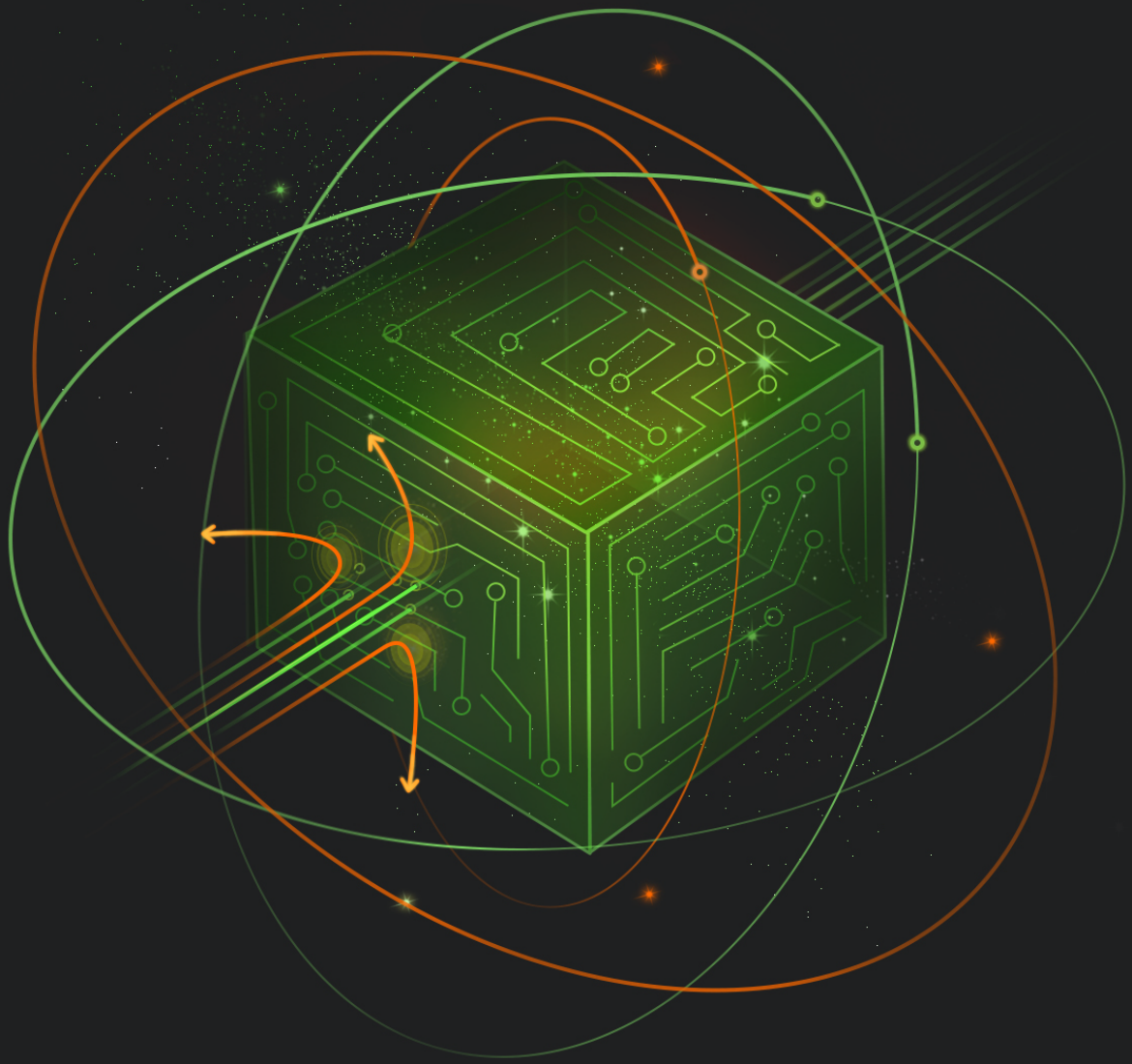
阿里云



2019年
上半年DDoS攻击态势报告

阿里云安全团队

时间：2019.7

2019年上半年，阿里云安全团队平均每天帮助用户防御2500余次DDoS攻击，与2018年持平。目前阿里云承载着中国40%网站流量，为全球上百万客户提供基础安全防御。可以说，阿里云上的DDoS攻防态势是整个中国攻防态势的缩影。阿里云安全团队基于2019年上半年云上的DDoS攻击数据，从DDoS攻击事件、僵尸网络中控、DDoS肉鸡、攻击事件情况等多个维度做了统计分析，希望为政府和企业客户提供参考。

概述

据阿里云安全团队监测到的数据发现，虽然2019年上半年DDoS攻击数量与2018年下半年持平，但峰值流量在300Gbps以上的攻击比2018年增长30%，500Gbps攻击比2018年增长了50%，并且连续2个月持续出现峰值近Tb级别的攻击。同时Memcached反射放大攻击比2018年增长40%，并在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%。

应用层攻击形势依然严峻，伪装成正常应用的恶意APP已让海量移动设备成为新一代肉鸡。据阿里云监测到的数据显示，目前已有五十余万台移动设备被用来当做黑客的攻击工具，达到PC肉鸡单次攻击源规模。攻击规模和肉鸡数量庞大且源IP不固定，攻击源分布极散，且多为基站IP，让传统的简单粗暴的将攻击IP拉黑防御手段失效，这就要求防守方采用更为纵深、智能的防护手段。企业需要具备快速的应用层流量分析能力，同时必须准确且自动化的产出多维度的防御策略。

一.攻击态势

1.1 攻击趋势

阿里云安全团队统计了2019年1-6月峰值流量超过50Gbps以上的DDoS事件分布，如图1-1所示。从图中可以看出，2019年DDoS峰值流量大于50Gbps事件有5500余次，其中300G以上攻击占比20%，同时已连续2个月出现近Tb级攻击，如图1-2所示，Tb级别攻击已然成为常态，相比2018年攻击强度，攻击目的性有所增强。

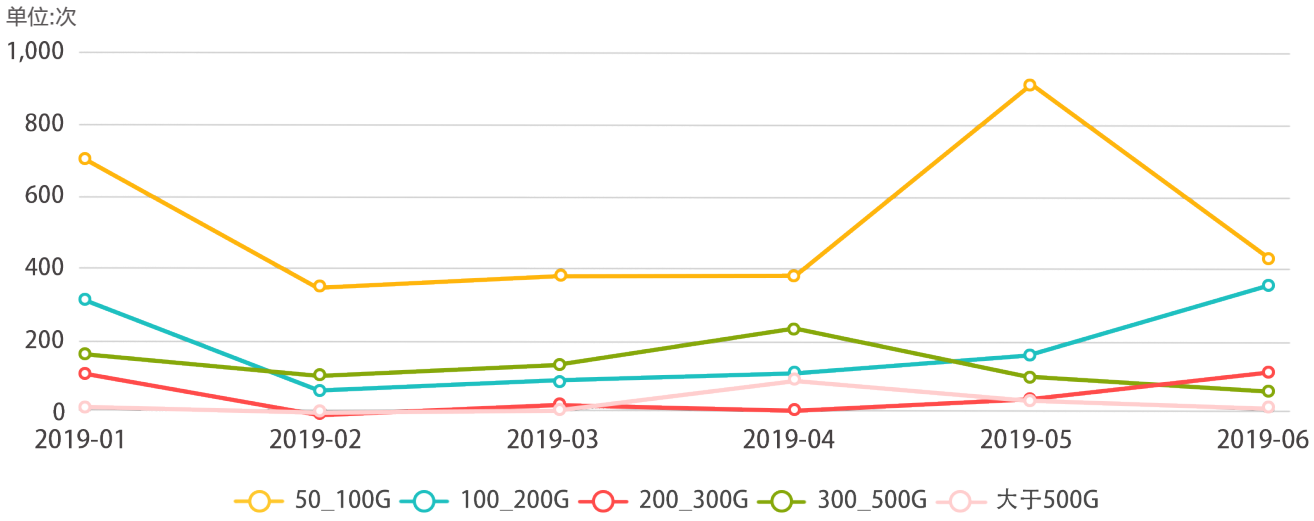


图1-1 2019年1-6月峰值流量大于50Gbps事件分布

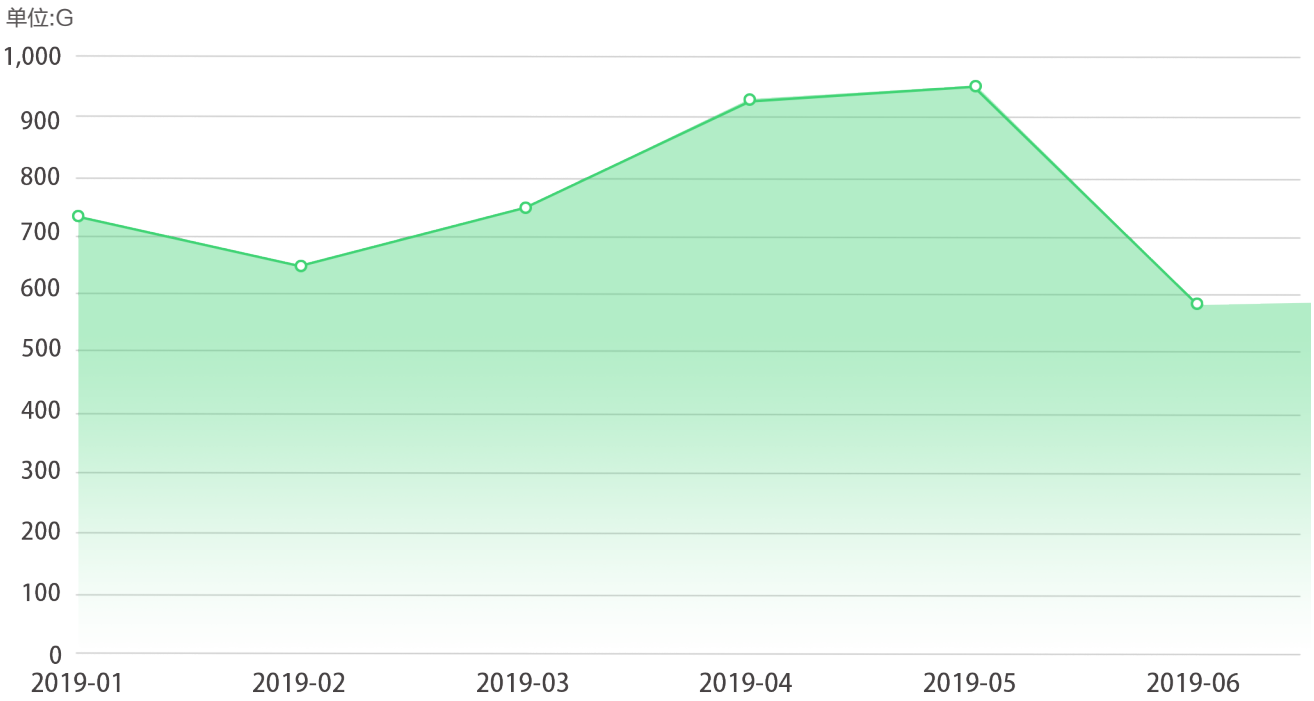


图1-2 2019年1-6月DDoS攻击峰值流量趋势

1.2 攻击行业分布

网站和游戏行业仍然是主要的DDoS攻击目标，两者共占据DDoS攻击目标的50.55%，如图1-3所示。

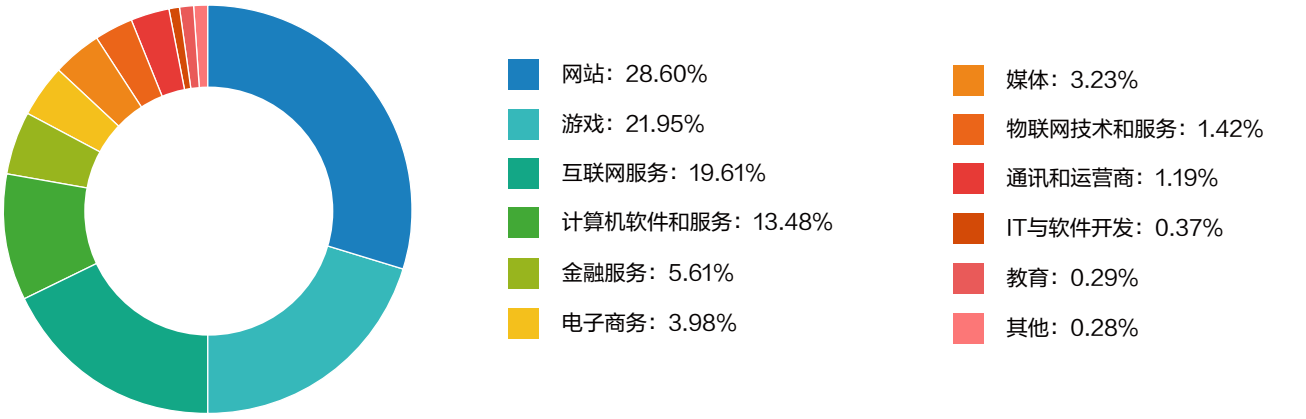


图1-3 DDoS事件行业分布

1.3 攻击种类分布

当前存量反射源最多的攻击类型分别是Memcached、NTP、SSDP、CLDAP，反射放大攻击整体占比呈下降趋势，同时UDP_Flood攻击仍然是最常见攻击类型，如图1-4所示。相比2018年，Memcached反射放大攻击占比有所上升，但主要集中在1-2月份，1月Memcached反射利用达到峰值，得益于运营商、云厂商和IDC对于Memcached反射源的治理，目前整体呈下降趋势，趋于稳定，如图1-5所示。

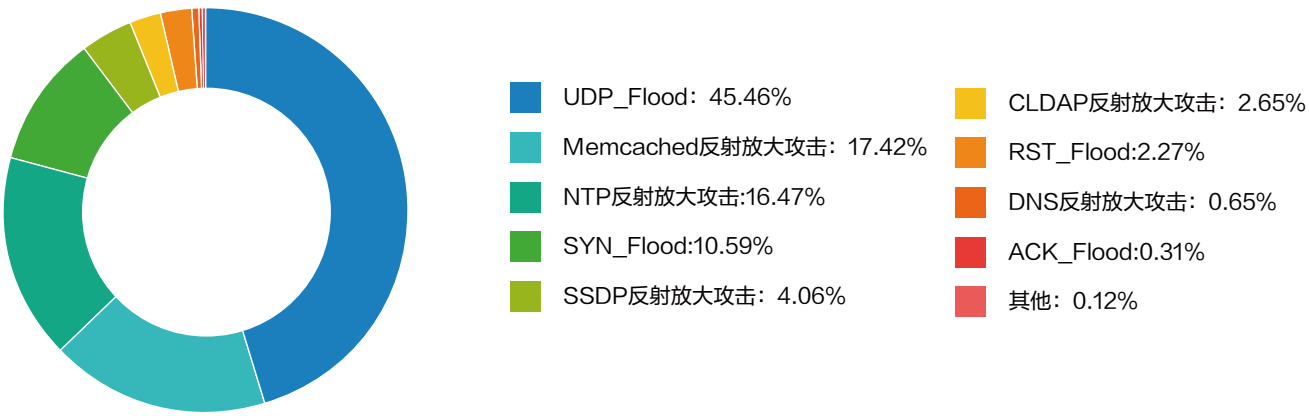


图1-4 2019 1-6月 DDoS攻击种类分布

[1] 网站：指的是以网站为主要载体提供产品或服务的企业

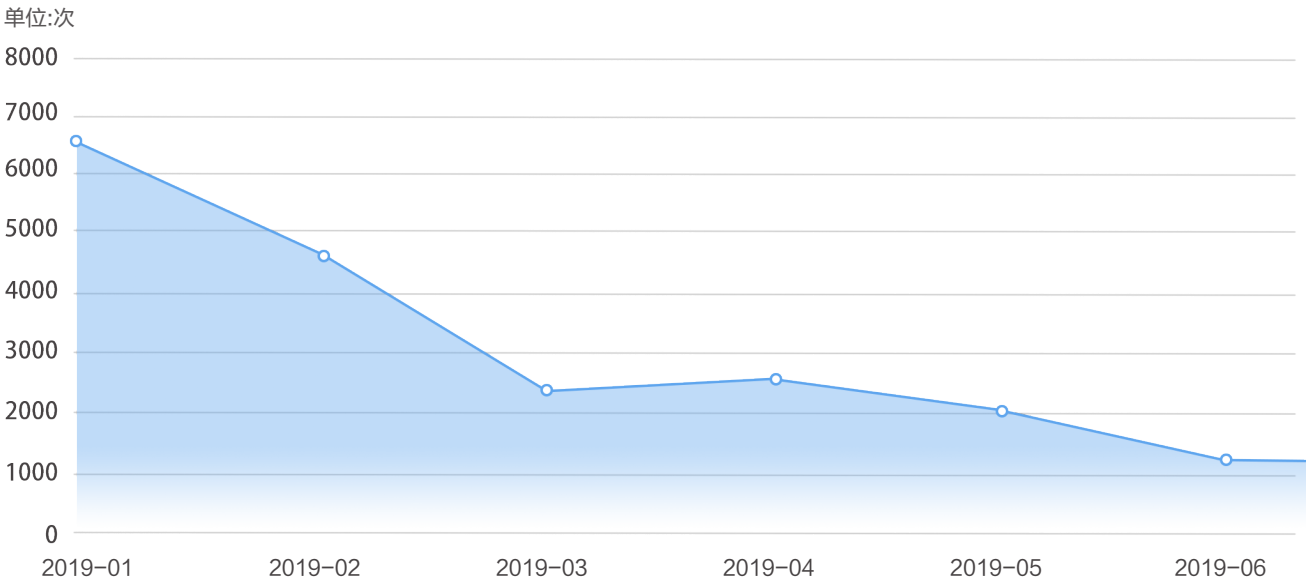


图1-5 2019 1-6月 Memcached 反射放大攻击次数

1.4 攻击目标端口分布

Web类服务和游戏端口的DDoS攻击仍是主要的攻击目标，分别占比20%和18%，如图1-6所示。

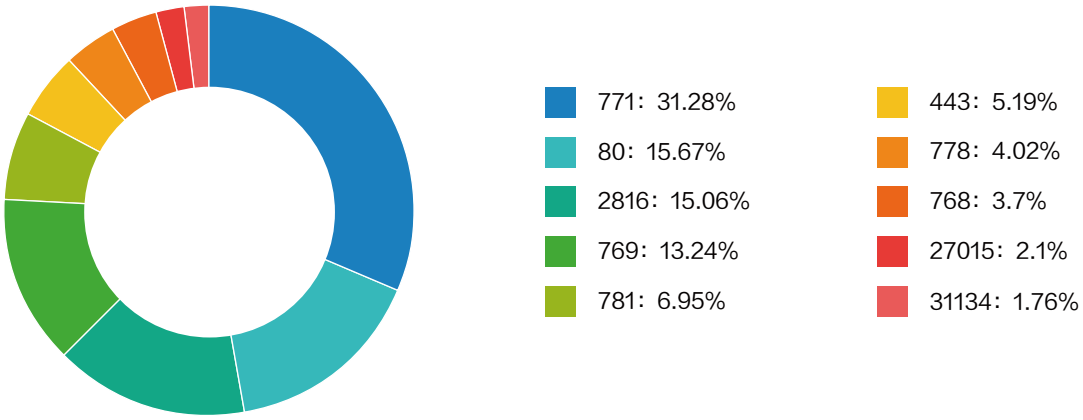


图1-6 DDoS攻击目标端口分布

1.5 核心观点

与2018年相比，2019年上半年DDoS攻击的数量基本持平，但攻击强度变化更为激烈。主要表现在以下几个方面:

1.Tb级攻击时代已经到来。2019年上半年已经出现持续2个月攻击接近Tb级，大流量攻击以TCP类攻击为主，单一网段攻击流量持续且流量大，目前已监控到单一C段流量近200G。

2.Memcached反射放大攻击在1月份攻击数量达到峰值，后续2-6月份反射放大攻击数量呈现持续下降趋势，得益于各机构对Memcached反射源的治理，目前整体呈下降趋势，趋于稳定。

3.应用层攻击对抗。攻击者通过变化多种攻击特征加大攻击量，企图绕过防御规则，压垮防护设备性能。针对百万级连接耗尽型攻击，企业需要根据攻击量进行快速隔离防护，并根据攻击量防护动态快速扩容，不让单一节点性能成为防御瓶颈。

4.伪装成正常应用的恶意APP已让海量移动设备成为新一代肉鸡。攻击者可以轻易在不触发限速防御策略的情况下实现攻击，让限速和黑名单在PC肉鸡时代曾是“一键止血”的防御方式失效。对于个人用户而言，切勿从非正规渠道安装未经审核的APP，让自己手机沦为黑灰产的工具。

二.DDoS僵尸网络分析

2.1 木马家族分布

在TOP10的木马家族中，Mirai、Gate、Nitol三大家族共占据半壁天下，达到60%，如图2-1所示。

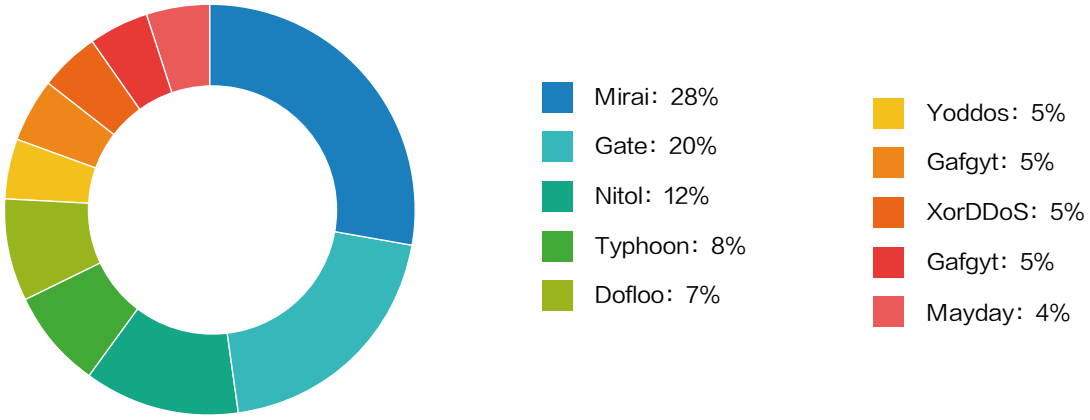


图2-1 DDoS木马家族分布

2.2 CnC地区分布

针对国内进行DDoS攻击的僵尸网络中，59%来自中国大陆，来自美国和中国香港地区的分别占18%和6%。相比2018年，中国占比下降10%，控制端有逐步向海外转移趋势，美国上涨了5%，如图2-2所示。

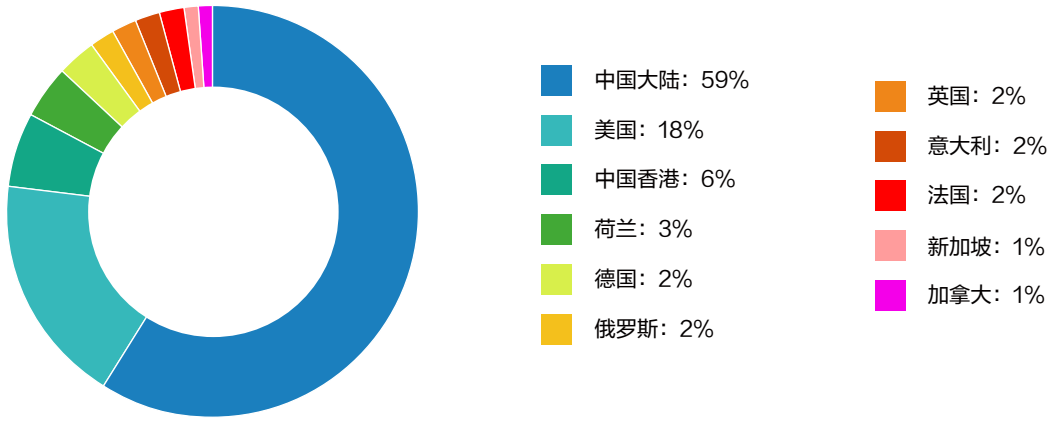


图2-2 CnC国家和地区分析

2.3 CnC存活时间分布

通过对CnC的存活时间进行分析发现，CnC的更新很频繁。60%以上的CnC存活时间不超过1周，如图2-3所示。

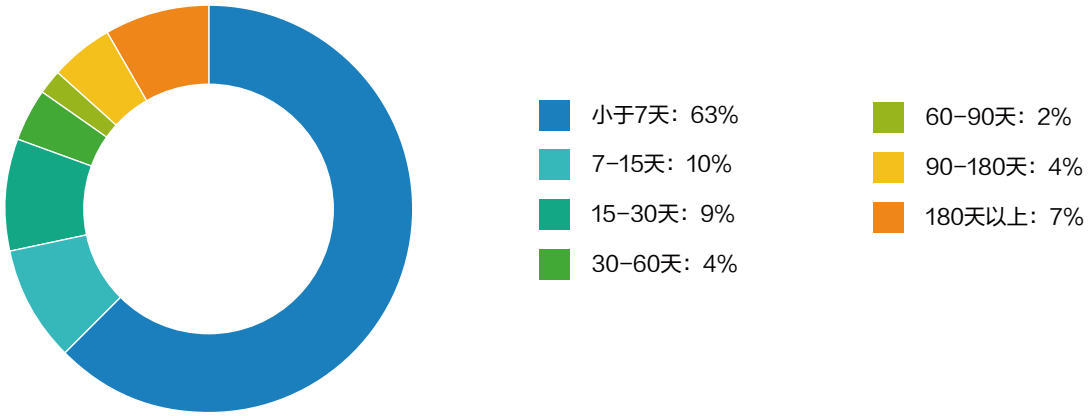


图2-3 CnC存活时长分布

三.DDoS肉鸡分析

3.1 UDP反射源国家及地区分布

当前进行DDoS攻击的UDP反射源有50%来自中国大陆，俄罗斯和美国分别占15%和8%，如图3-1所示。

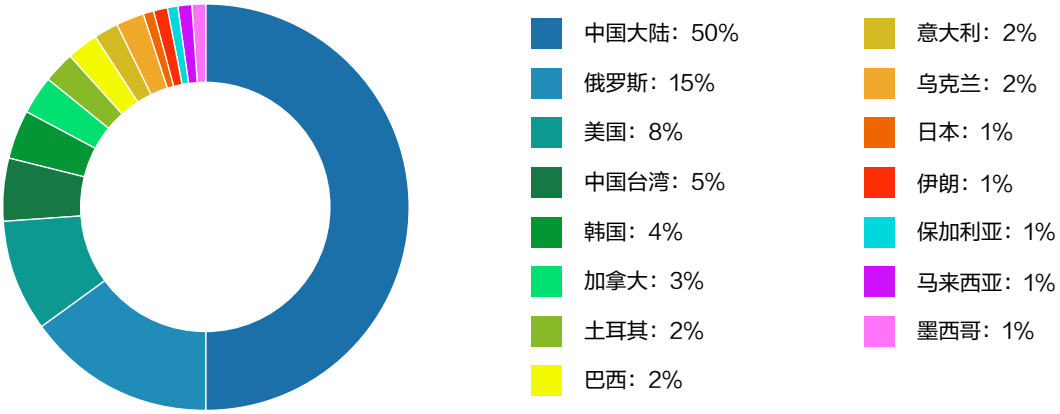


图3-1 UDP反射源国家及地区分布

3.2 肉鸡国家分布

在2019年1-6月对全球发起DDoS攻击的肉鸡IP中，美国和中国分布占比36%、32%，如图3-2所示。鉴于近68%的攻击来自于海外，阿里云安全团队建议用户根据自身业务情况，可选择性封禁海外访问区域来应对DDoS攻击。

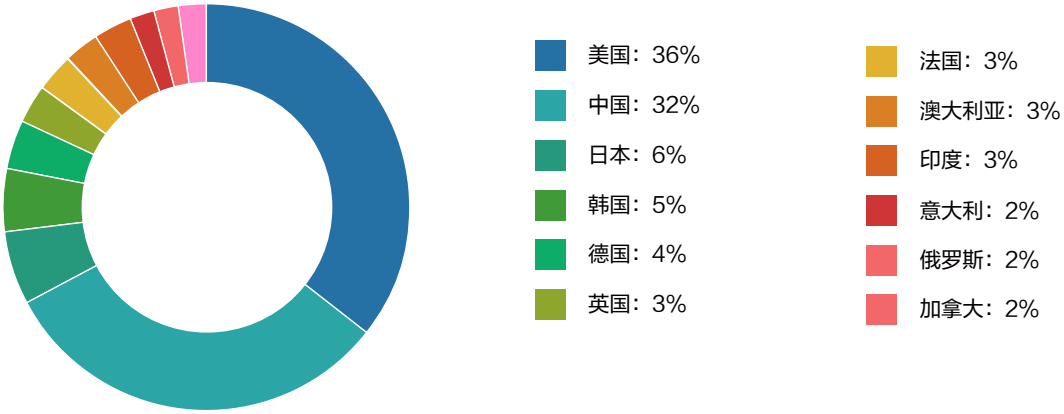


图3-2 肉鸡国家分布

3.3 DDoS攻击运营商分布

在国内的DDoS攻击流量中，中国电信是主要的DDoS攻击流量来源，如图3-3所示。

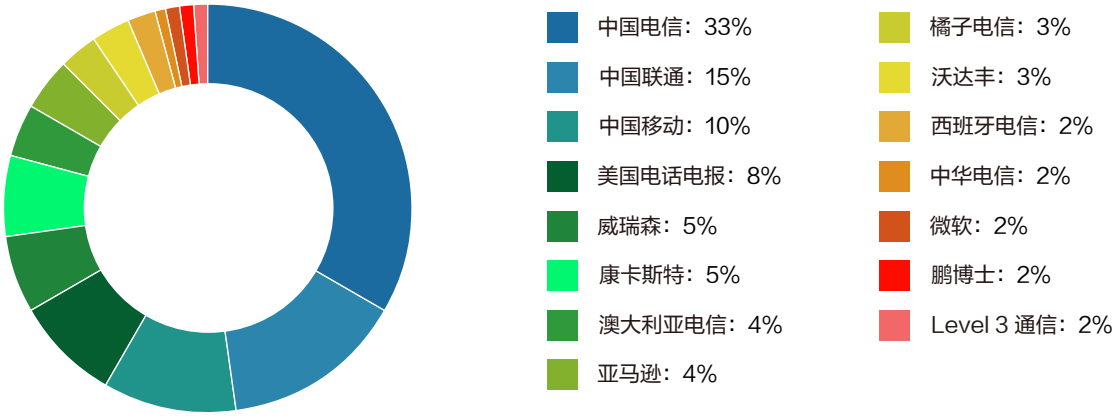


图3-3 DDoS 流量运营商分布

四.典型案例

4.1 长时间压制

如果要说DDoS对抗最为激烈的行业，游戏行业一定是其中之一。攻击量大，持续时间长，对抗激烈，这些攻击特征一直伴随着游戏行业的发展。用户在2019年初接入，业务一直很稳定，在5月份遭受了高强度的连接型的DDoS攻击。从5月5日到5月8日的三天时间里，客户每天遭受峰值100Gbps以上、新建超过100万cps的Connection Flood攻击，同时攻击的持续时间每天长达15个小时以上，对客户业务产生了极大威胁。

阿里云DDoS团队监控到攻击后快速介入，基于客户自身业务现状、业务规模定制专属防护方案，为客户提供最大限度的防护服务，保障客户业务稳定运行。

攻击从5月5日14:20开始，到5月6日07:45结束，持续约17小时，如图4-1所示。

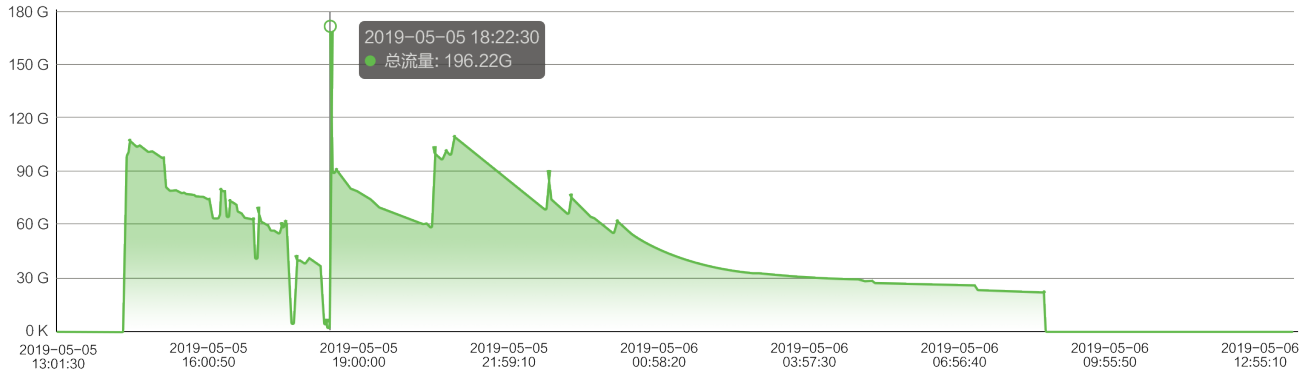


图4-1

攻击从5月6日15:59开始，到5月7日08:22结束，持续约16小时，如图4-2所示。

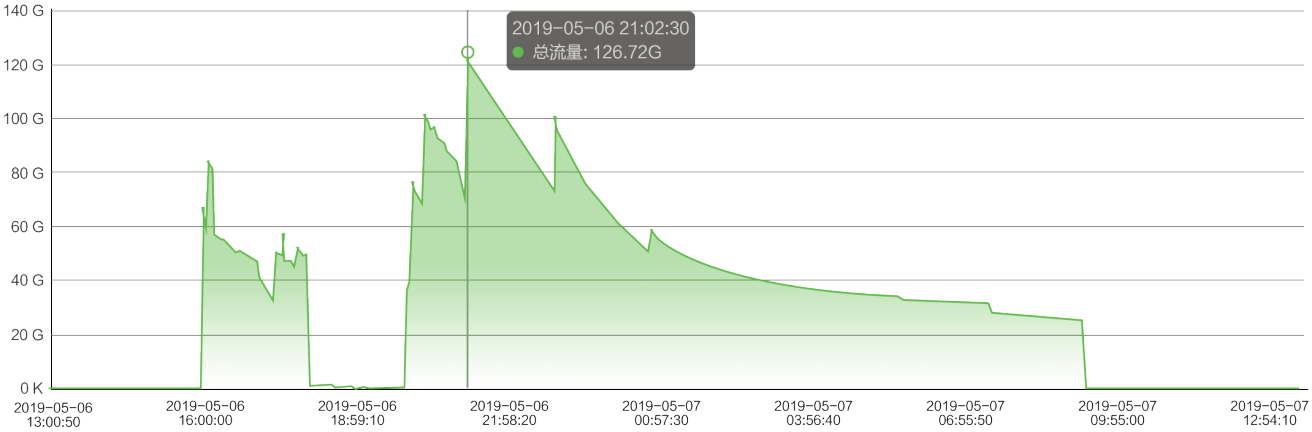


图4-2

攻击从5月7日13:42开始，到5月8日07:15结束，持续约17小时，如图4-3所示。

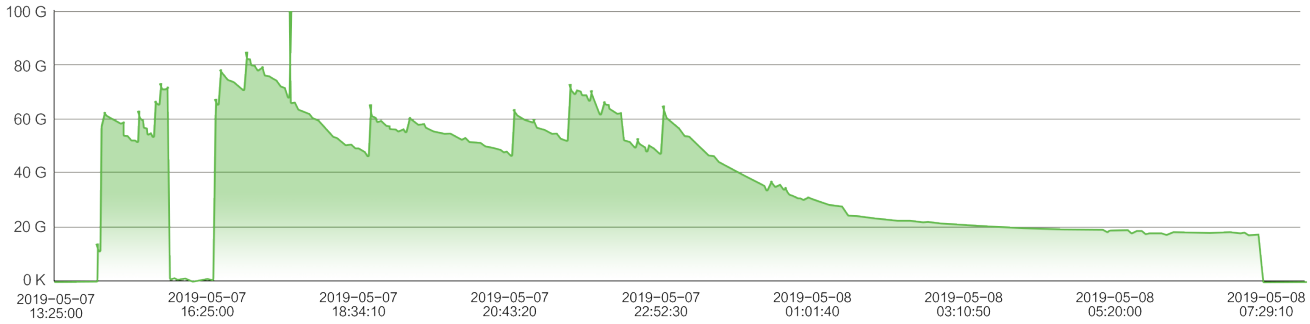


图4-3

阿里云安全专家建议:安全始终是为业务服务，建议企业能够结合自身业务特点、规模、客户访问情况提前设置DDoS防护策略，以保障在攻击到来时，快速抵抗住。同时建议企业选择BGP带宽，游戏用户对于网络延迟、抖动敏感，在大流量攻击下，单线带宽存跨网拥塞问题容易导致游戏用户网络质量急剧下降，严重者将有可能丧失得来不易的活跃用户。

4.2 攻击变化多且快

2月中旬，阿里云上一个电商客户的多个域名同时遭受到CC攻击。攻击时间持续了20分钟左右，攻击者动用了国内外几十万以上的肉鸡资源，攻击峰值超过150万QPS，具体如下:

16:15，第一波，攻击者伪造Baidu爬虫
16:20，第二波，攻击者变化UA特征，企图绕过防护规则
16:27，第三波，攻击者采用多种攻击方式进行混合攻击
16:32，第四波，攻击者动用更多肉鸡，攻击峰值一度达到150万QPS，企图利用高QPS压垮防御系统处理性能

阿里云的七层智能防护能力经受住考验，全程保障了客户的电商平台访问顺畅，相比平时并未有其它异常现象出现，攻击者未能达到攻陷网站的目的。此后一段时间，该电商客户陆陆续续遭受过几次试探性CC攻击，客户业务也一直保持平稳运行。

阿里云安全专家建议：通过主流的WEB服务器来对外提供服务可以帮助企业在稳定性和处理性能上满足正常的业务需要。在服务上线时，企业还应该考虑处理性能冗余问题，要留有余量，以应对异常情况的发生，同时进行压力测试以了解对外服务能力。同时在选择DDoS防护产品时，除了关注带宽能力，还需关注应用层攻击防护能力。

4.3 攻击设备演变

自今年年初，阿里云安全团队观察到数起大规模存在一些共同特征的DDoS攻击。几经溯源发现，这些攻击事件源于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。

在PC肉鸡时代，企业抵御肉鸡DDoS攻击的做法相对简单粗暴：
检测单元：请求频率
执行动作：限速和黑名单
防御逻辑：请求频率过高后开始进行源限速或拉黑源IP

在无法有效防御的情况下，还需要人工介入抓包分析，根据攻击具体情况配置防护规则，但这种响应方式相对较慢，业务普遍已经严重受损。

当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。因此，黑灰产可以轻松绕过上述防御逻辑。

阿里云安全专家建议：企业不应该再对“限速+黑名单就能一招制敌”抱有幻想，而应该采用更为纵深、智能的防护手段：
1.丰富攻击流量识别的维度，将每个请求实时的解析出多维度的检测单元；
2.防护策略的执行需要与多维度的识别相匹配，需要有精细、灵活、丰富的访问控制单元，让各个维度有机组合，层层过滤攻击流量；
3.机器智能替代人工排查，提升响应速度，降低业务中断时间。

阿里云高防诞生之初的目标就是消灭互联网DDoS。目前，阿里云针对企业用户提供24小时免费应急支持服务，如果您被DDoS攻击，请加入阿里云应急支持群，为您的业务快速止损。

钉钉扫码加入应急支持

阿里云安全团队