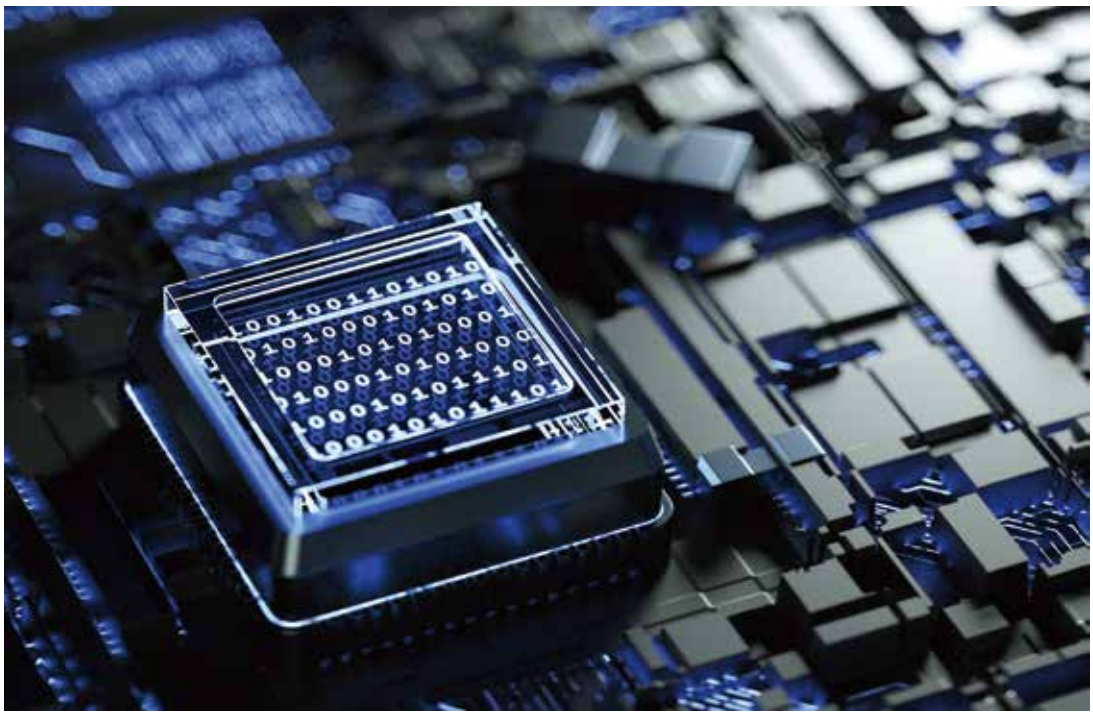
腾讯安全
Tencent Security

2020年腾讯云DDoS威胁白皮书

腾讯安全DDoS防护团队

目录



01 专家观点

专家观点

1. 在大量线下活动持续转向线上的大趋势下，DDoS威胁还将进一步增加。DDoS攻击黑产曾在2018年前后遭受司法机关重拳打击，现已出现明显复苏，而疫情防控措施导致大量线下活动转移到线上。两个因素叠加之下，互联网企业未来将面临愈来愈严重DDoS攻击威胁。

2. 小流量小包攻击成为高端攻击者的首选。为了规避检测和防护，取得更好的攻击效果，与业务流量更接近的小流量小包攻击成为高端攻击者的首选。精细化检测和深度防护技术迫在眉睫。

3. 应用层攻击呈现海量化趋势，数百万QPS的应用层攻击时有发生，常常伴随着超大流量的带宽型和包量型DDoS攻击，全方位一站式高性能防护架构成为防护刚需。

4. TCP反射成为行业公害。TCP反射不仅让被攻击企业饱受DDoS攻击困扰，而且让互联网公共服务也成为无辜受害者，CDN厂商、运营商、云计算厂商等平台服务更是成为重灾区。预计TCP反射攻击会在未来持续泛滥，需要全行业共同参与、共同治理。

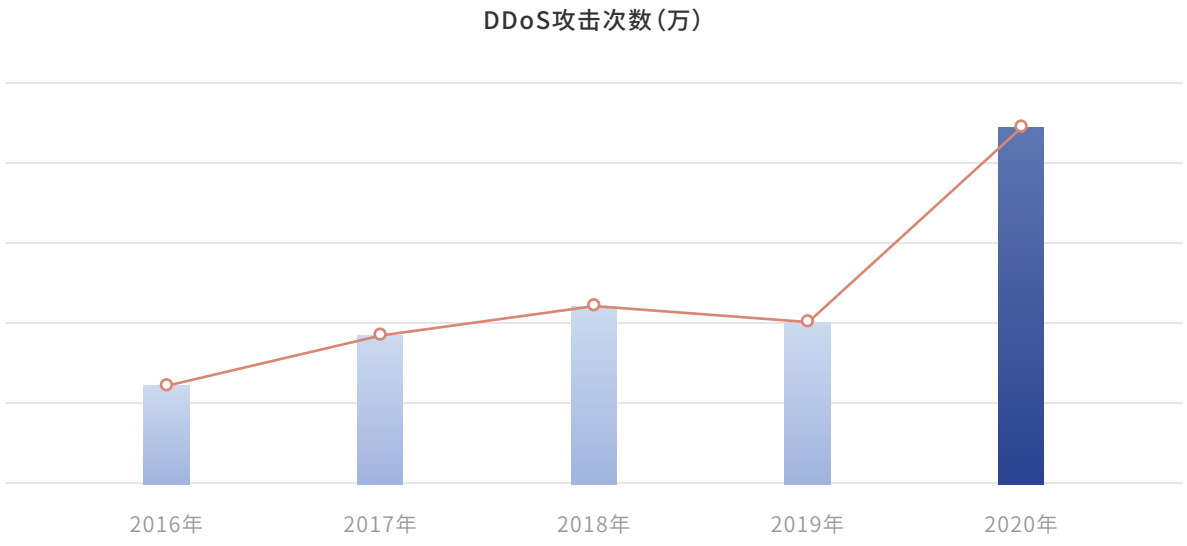
02 威胁态势分析

2.1 攻击威胁态势

关键发现1：2020年成DDoS攻击增幅最大一年。

在2018年年底，由于受到司法机关的重拳打击，国内外的DDoS攻击团伙遭受重创，大量DDoS攻击服务售卖站点被关闭。根据腾讯安全DDoS防护团队的监测结果，DDoS攻击在19年第一季度出现明显回落，但在不到半年的时间里迅速恢复。

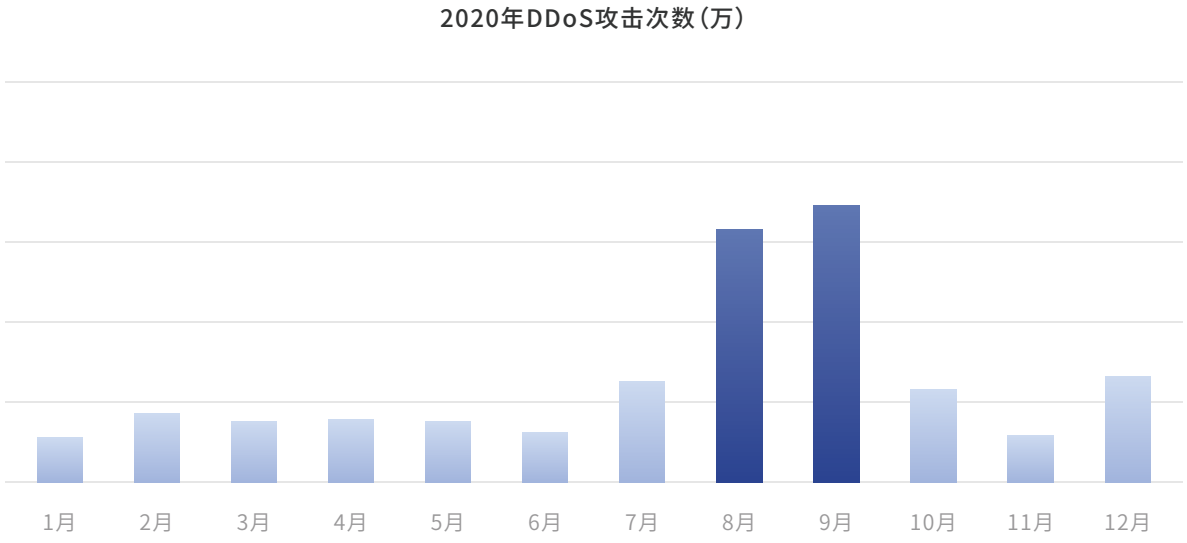
和航旅、酒店、餐饮等行业遭受疫情重创不同，2020年互联网企业迎来了难能可贵的发展机遇。行业的高速发展必然引来黑产觊觎，再加上发起DDoS攻击门槛低、来钱快，完全可以在线上完成，DDoS攻击黑产大军持续壮大。在上述两个因素叠加之下，2020年DDoS攻击次数成为历年之最，同比增幅更是达到135%，成为增幅最大的一年。



关键发现2：8月和9月DDoS攻击最密集。

从时间维度来看，2020年的DDoS攻击威胁呈如下特点：

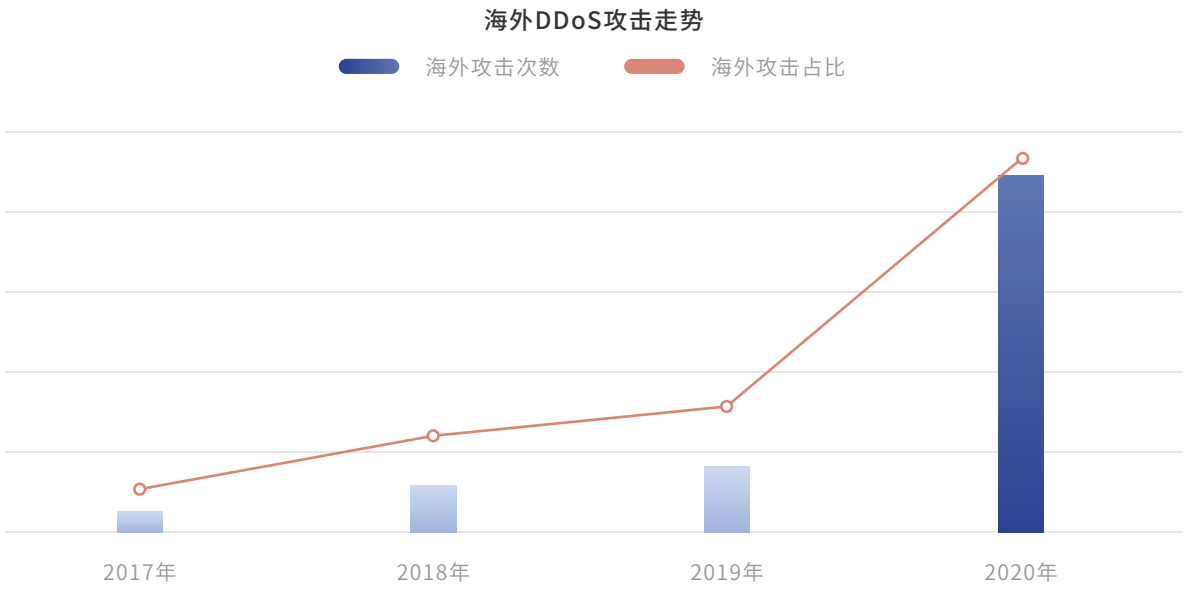
1. 下半年DDoS威胁大于上半年；
2. 第三季度DDoS威胁远大于其他季度；
3. 8月和9月成为DDoS攻击最多的两个月份，且远高于其他月份。



关键发现3：海外攻击出现大幅增长。

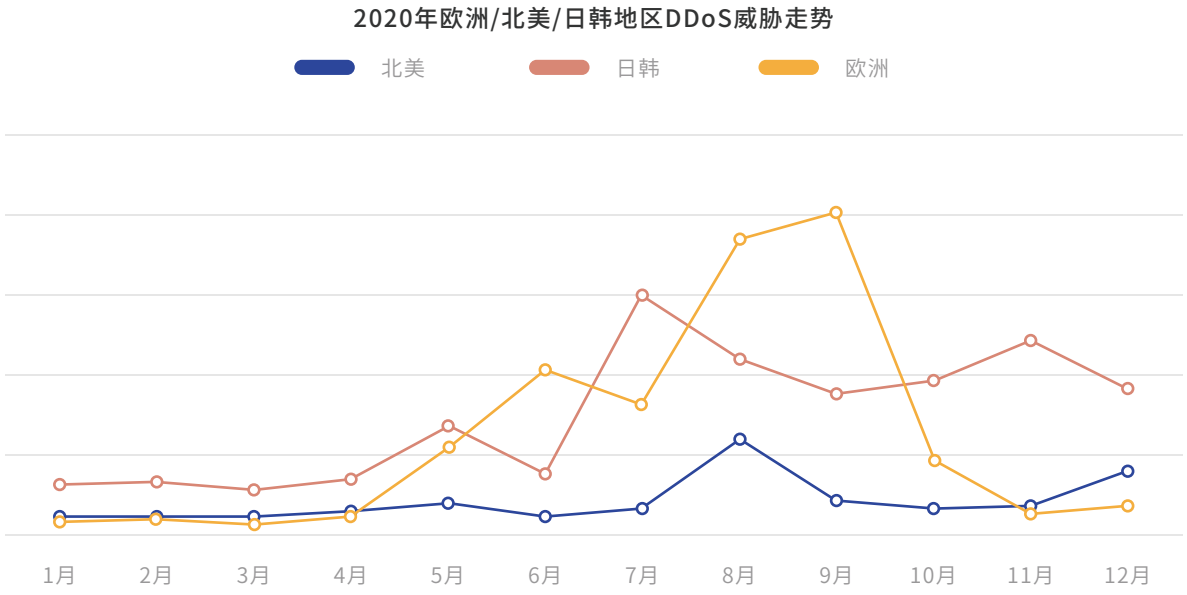
近年来海外DDoS攻击次数持续增长，2020年海外区域的DDoS攻击呈现如下特点：

1. 2020年是海外攻击次数最多的一年。
2. 2020年是海外攻击增长最为迅猛的一年。
3. 欧洲和北美成为中国以外DDoS攻击较为密集的区域。



关键发现4：DDoS攻击走势与当地疫情防控形势呈现明显相关。

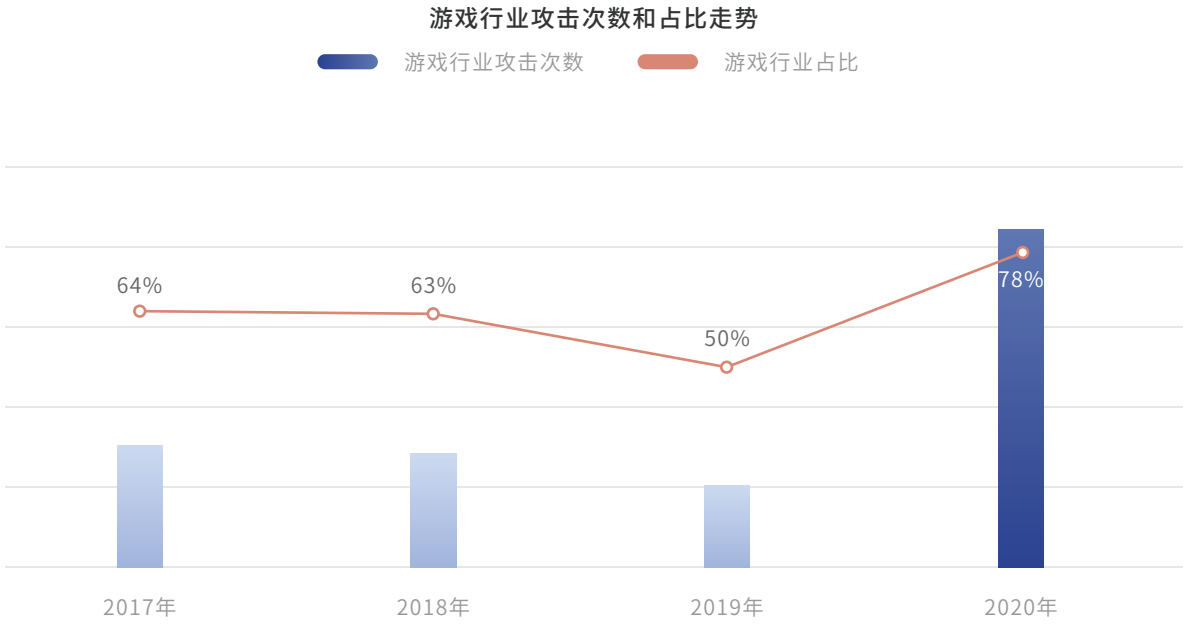
2020年，疫情给各国经济活动和人民生活带来了巨大变化，大量社交、娱乐、购物和工作等场景从线下转移到线上。一直以来，海外企业都深受DDoS攻击困扰，线上活动的增加更是吸引了DDoS攻击黑产的火力，带来大量DDoS攻击。这个趋势在欧洲，北美和日韩等地尤其明显。



关键发现5：游戏行业仍是主要被攻击行业。

尽管一直以来，游戏行业都是DDoS攻击的重灾区，但2020年的疫情加剧了这一趋势。根据腾讯安全DDoS防护团队的监测数据，2020年游戏行业的DDoS攻击次数不仅再创新高，而且在整体DDoS攻击中的占比超过7成，手游成为最受攻击者青睐的品类。

除了游戏行业之外，电子商务、直播、在线办公、在线教育等相关行业的DDoS攻击威胁也比较突出。疫情期间，大量娱乐、教育、办公等活动转到线上，这些行业在迎来行业春风的同时，也将面临更大的DDoS攻击威胁。

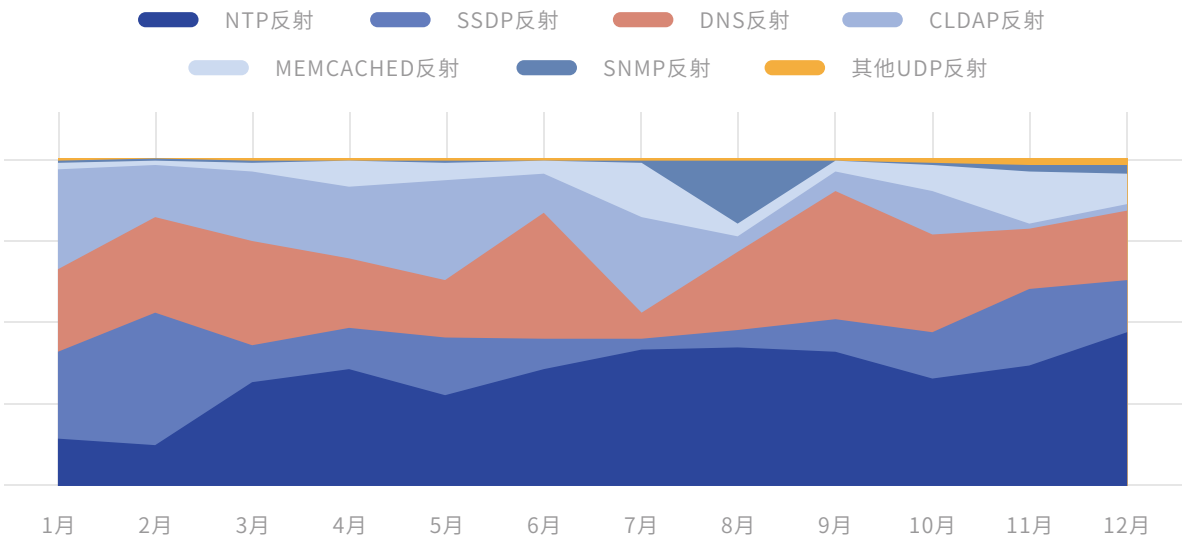


2.2 攻击手法态势

关键发现1：UDP反射攻击仍是攻击者发起DDoS攻击的主流。

UDP反射放大攻击一直是攻击者发起DDoS攻击的首选。由于可以用较小的原始攻击流量放大，取得更好的攻击效果，因此，大量DDoS攻击站点将反射放大攻击封装后，以极低的价格售卖。这样做不仅成本低廉，且操作简单，极大降低了发起DDoS攻击的门槛。根据腾讯安全DDoS防护团队的监测数据，UDP反射攻击的占比一直在6成以上，其中NTP反射、DNS反射、CLDAP反射和SSDP反射等是现网最为普遍的UDP反射手法。而在超过300G的超大流量UDP反射型DDoS攻击中，SSDP反射手法通常是最主要的攻击流量来源。

2020年UDP反射手法变化趋势

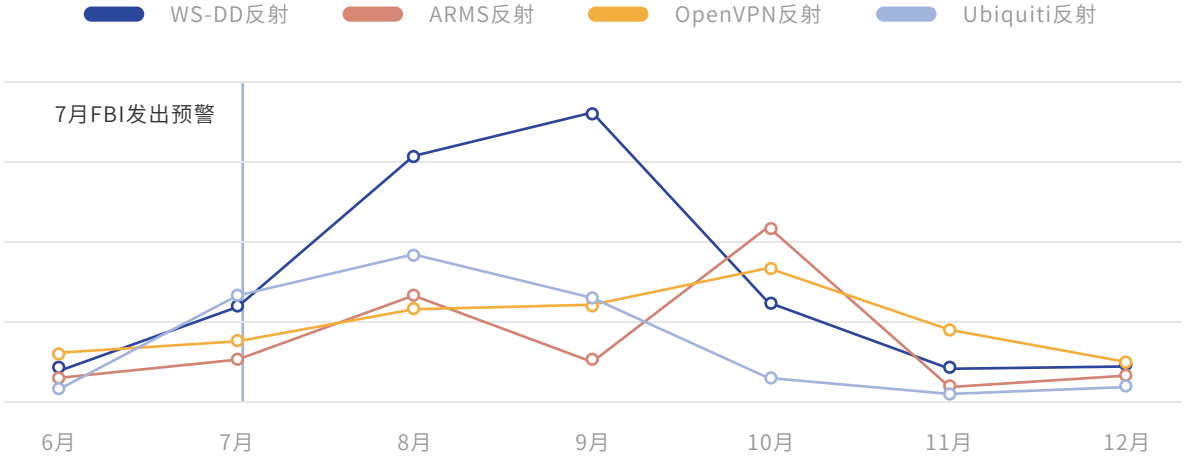


关键发现2：CoAP、WS-DD和ARMS等新型UDP反射被大量用于攻击游戏业务。

2020年7月，FBI针对基于CoAP（受约束的应用协议）、WS-DD（Web服务动态发现）和ARMS（Apple远程管理服务）等服务发起的DDoS攻击出现爆发向美国企业发出预警。

腾讯安全DDoS防护团队监测数据显示，在FBI发出预警前的6月，其中部分攻击就已较为活跃，此外还有其他新型手法被黑客挖掘出来。在FBI发出预警之后，这些新型UDP反射手法广为人知，攻击呈现进一步爆发态势。

2020年ARMS/WS-DD等新反射手法威胁走势



和DNS反射、CLDAP反射、MEMCACHED反射等手法产生大量UDP大包乃至分片包不同，一些新型UDP反射放大攻击（如CoAP反射和ARMS反射等）的包长较小。同时，这部分新型UDP反射手法，**除了DVR反射、CoAP反射、IPSec反射的反射源较多外，其余手法的反射源都在数万级别**。由于上述两方面原因，这部分攻击难以发起大流量DDoS攻击，数百M流量的攻击最为常见。

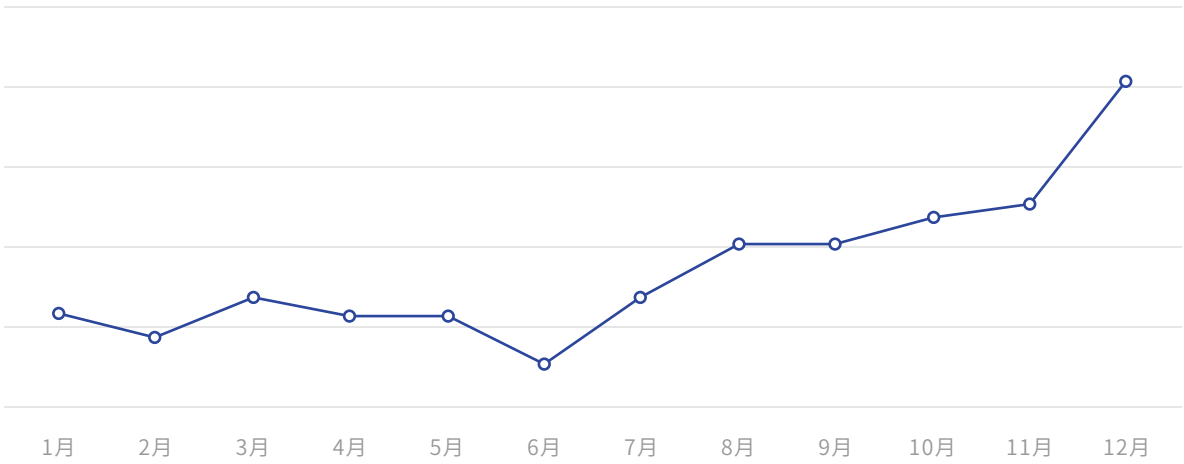
但根据腾讯安全DDoS防护团队的监测数据，这部分新型UDP反射放大攻击在下半年针对游戏行业客户的攻击中被大量使用，据分析有如下几方面原因：

1. 游戏用户对于数据延迟，网络丢包较为敏感，这部分新型反射放大攻击产生的数百M流量虽然无法拥塞机房带宽，但是挤占服务器CPU和连接数等资源则绰绰有余，可以大幅降低玩家的游戏体验。
2. 基于UDP协议的游戏较多，且这部分新型UDP反射手法利用的大多是高端口，部分协议运行在家庭网络，来源IP与真实用户IP存在重合，难以通过传统的协议+IP+端口的ACL策略进行过滤。
3. 由于攻击包的包长较小，和业务流量更为接近，可以有效穿透粗粒度的检测和防护。

关键发现3：TCP反射攻击威胁持续扩大。

根据腾讯安全DDoS防护团队的监测数据，TCP反射攻击在2020年下半年开始出现明显的持续增长态势。无论是攻击次数还是最大攻击流量，均高于去年同期和上半年。

2020年TCP反射攻击走势



据腾讯安全DDoS防护团队分析，**TCP反射**之所以受到黑客重视，并在现网大量出现，是因为**和以往常见UDP反射放大攻击和SYNFLOOD攻击相比，有如下优势：**

1. 发起攻击的都是真实的服务器，具备真实的协议栈，可以绕过传统的反向挑战等防护算法。
2. 产生的攻击包包长极小，上百G攻击流量对应的包速率可以达到数亿级别，产生更多的五元组会话，可以更大程度消耗防护方的资源。
3. 和SYNFLOOD主要来源于僵尸网络控制下的肉鸡不同，TCP攻击流量主要来源于正常提供服务的公共服务器，此外有相当部分流量来自家庭路由器。如果简单地基于源IP和端口进行过滤，会影响到客户对这些服务器的正常访问，造成严重误杀。这也是攻击者有恃无恐的重要原因。

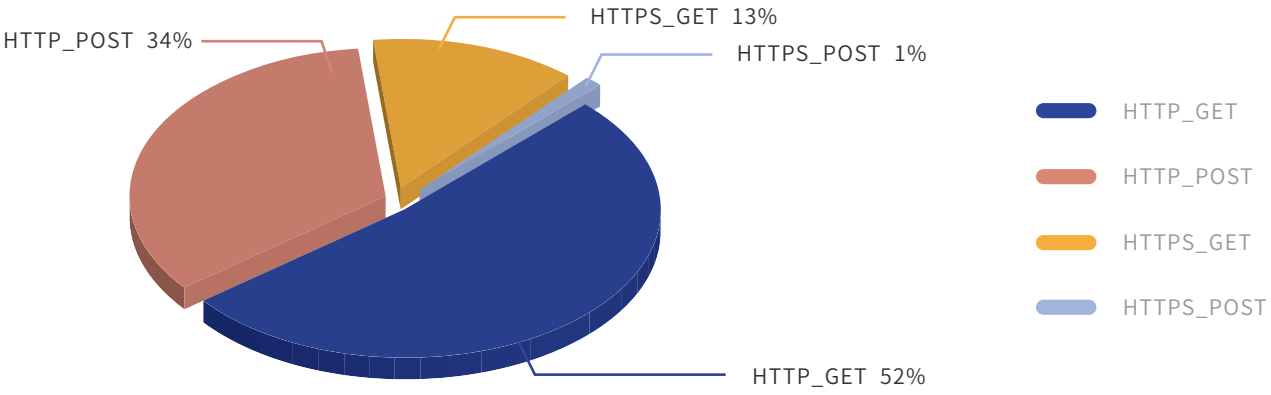
由于具有如上的特点，TCP反射较难防护，会给被攻击企业带来业务宕机、客户流失、口碑受损等严重后果。

关键发现4：应用层攻击（CC攻击）呈现海量化态势。

2020年以来，超大流量的应用层攻击（HTTP/HTTPS　CC攻击）也愈加频繁。根据腾讯安全DDoS防护团队的监测数据，应用层攻击中以HTTP协议CC攻击为主，HTTPS协议CC攻击占比为15%，两种场景下都是以GET请求为主。

尽管攻击占比相差悬殊，但二者的最大攻击流量却相差无几，**现网出现HTTP CC攻击的最大攻击流量达到了370万QPS，HTTPS CC攻击的最大攻击流量也达到260万QPS**，这说明应用层越来越呈现海量的趋势。

应用层DDoS攻击的攻击手法分布

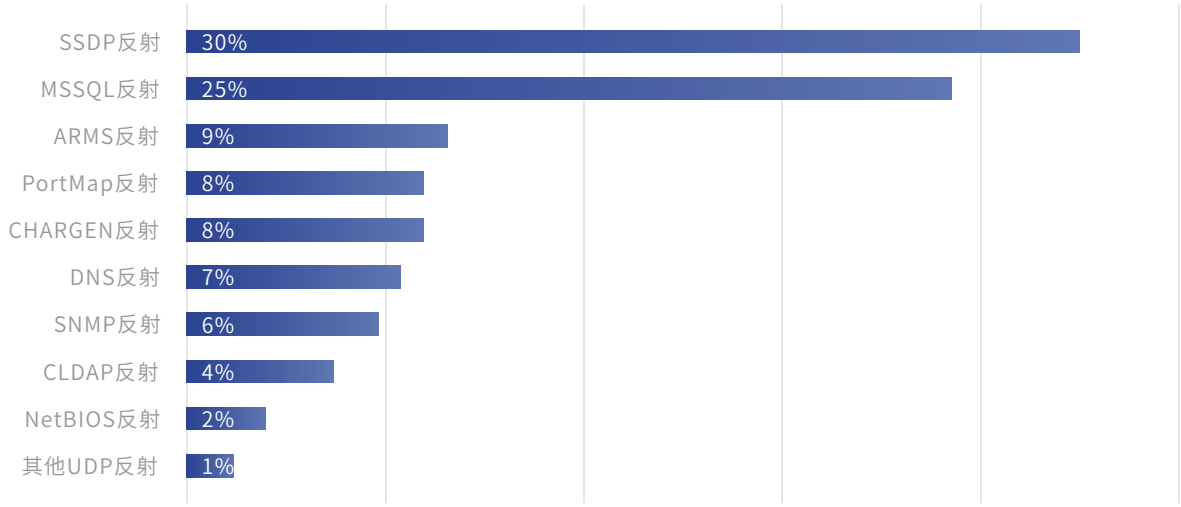


关键发现5：复合型攻击成为常态。

为了追求更好的攻击效果，攻击者不断寻找更多更强的攻击手法，将现有攻击手法组合也成为攻击者共同的选择。最常见的组合方式包括：SYNFLOOD+UDP反射放大攻击，多种不同UDP反射放大攻击组合（NTP反射、CLDAP反射、DNS反射、SSDP反射等），以及SYNFLOOD+TCP反射等。

在2020年下半年多种新型UDP反射攻击手法被黑客挖掘出来后，黑客攻击手法愈加丰富，甚至在单次持续数分钟的攻击中出现了超过10种的攻击手法。

某次攻击中各种UDP反射手法攻击流量分布



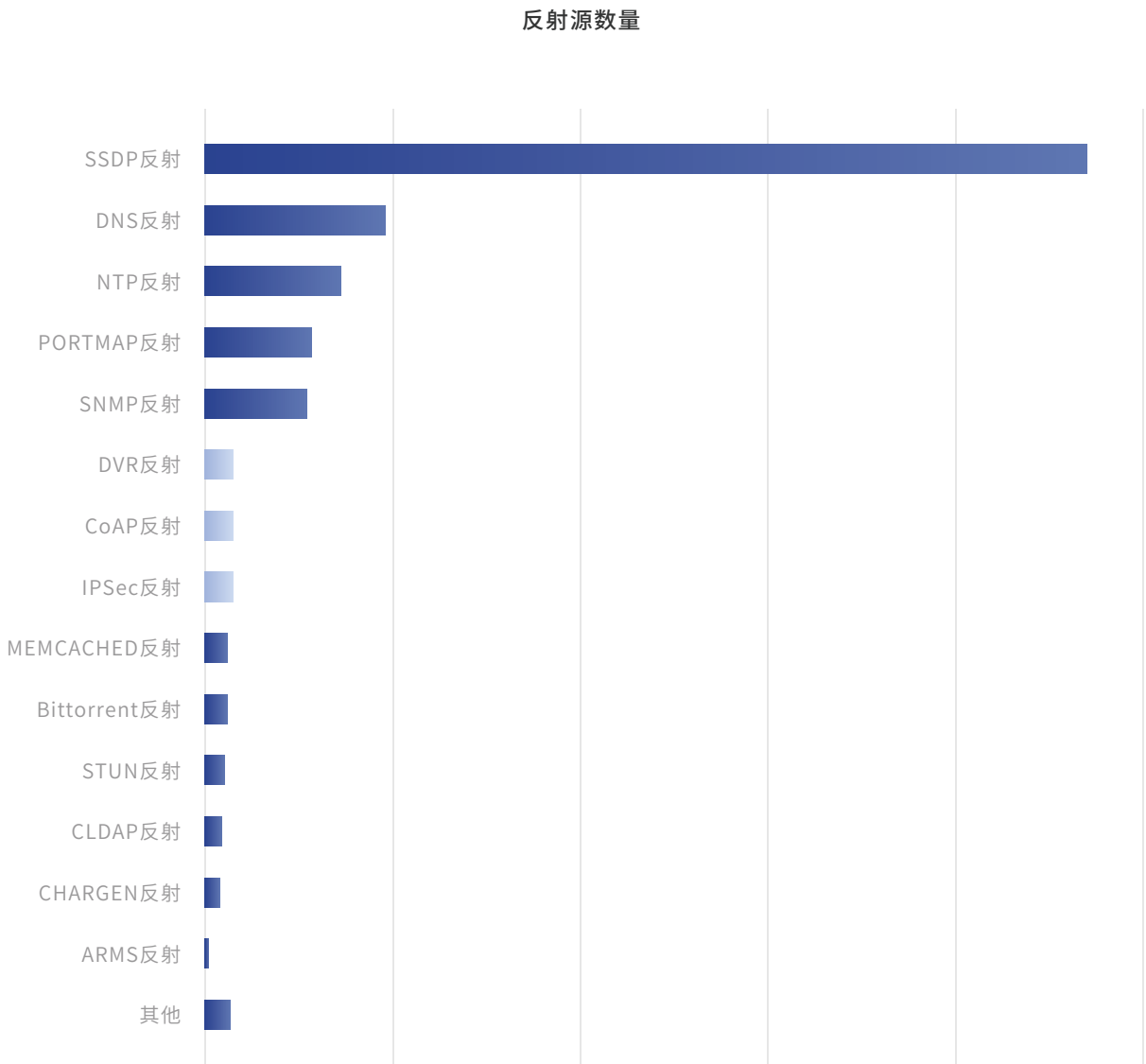
此外，在下半年针对游戏行业的攻击中，出现了一种在上百G的UDP反射流量（以NTP反射、DNS反射、CLDAP反射最为常见）掩护下，另有数十M甚至数M的UDP小包攻击的组合攻击。在这种攻击模式下，尽管绝大部分攻击流量被成功检测和清洗，但部分UDP小包攻击流量却成功避开了重重的检测和防护，像一股奇兵，直接刺入业务服务器的心脏。针对黑客这种“明修栈道，暗度陈仓”的策略，只有更精细化的检测和防护策略，才能有针对性的防护其威胁。

2.3 攻击资源态势

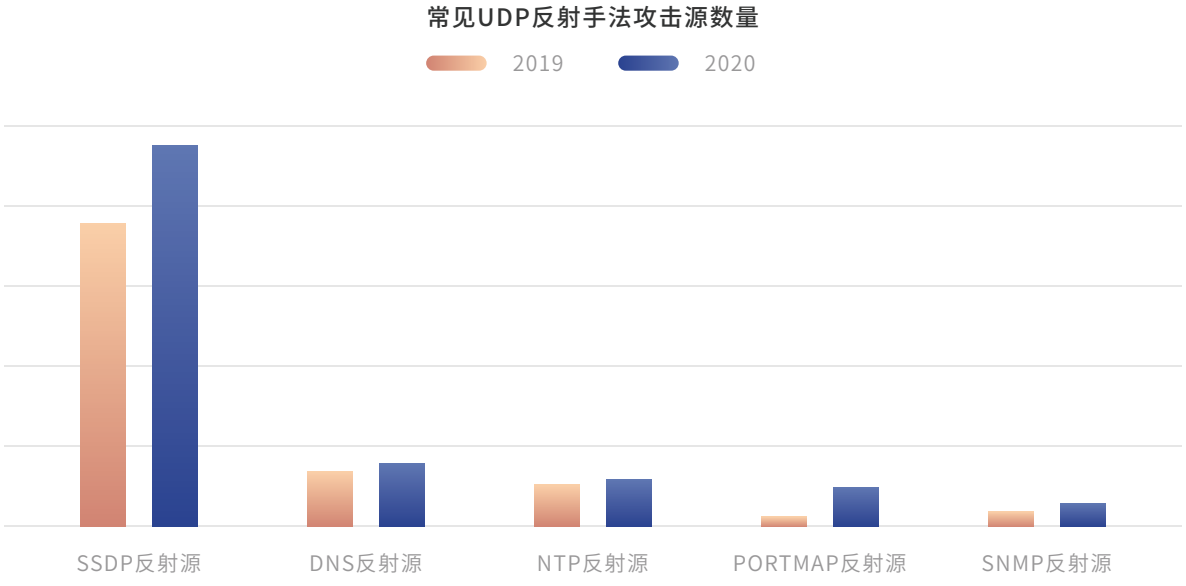
关键发现1：UDP反射源仍是最主要攻击资源。

根据腾讯安全DDoS防护团队的监测数据，UDP反射源仍是现网攻击源的主要来源，其中SSDP反射源数量最多，且总数在千万级别，远远大于其他类型。DNS反射源、NTP反射源、PORTMAP反射源、SNMP反射源则处于第二梯队，数量在50万~200万之间。其余反射源数量均在50万以下。

值得注意的是，DVR反射、CoAP反射、IPSec反射等新型UDP反射攻击手法的反射源数量也较多，甚至超过了CLADAP反射和MEMCACHED反射的反射源数量。



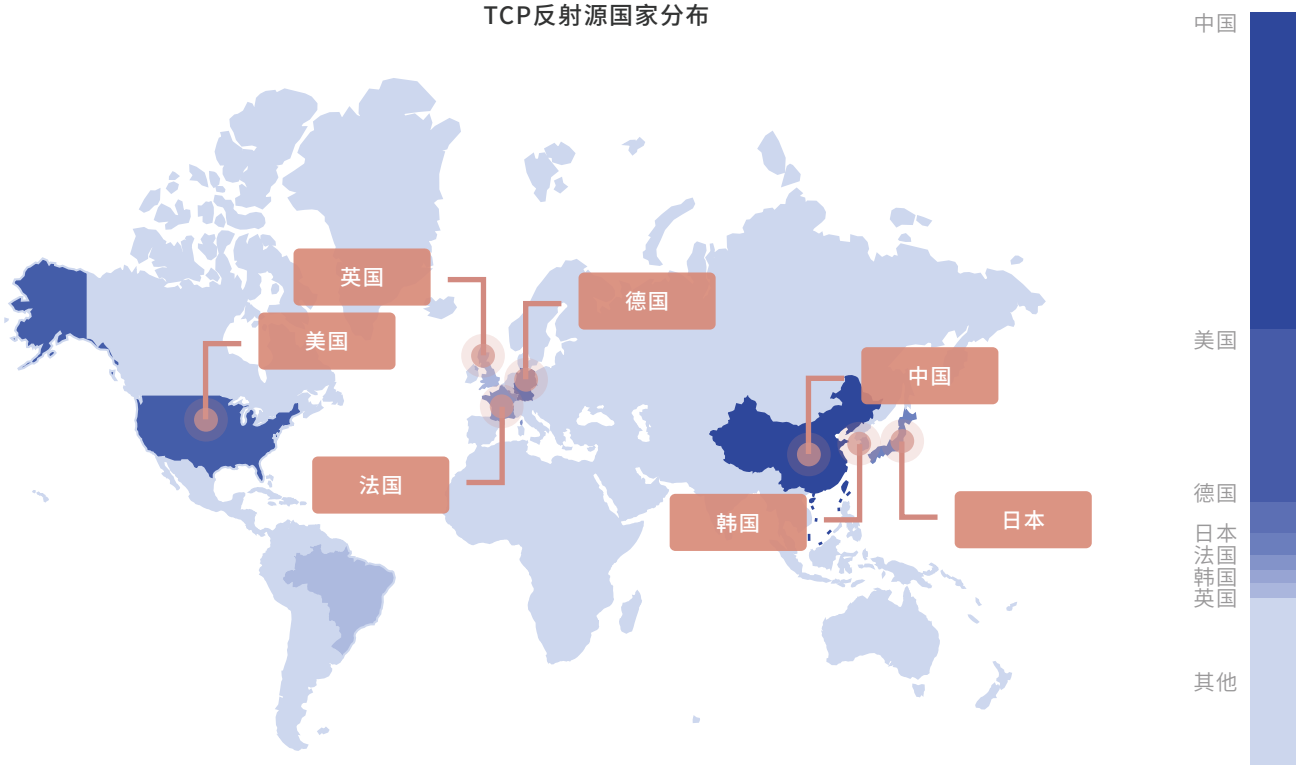
此外，和去年相比，SSDP反射源、DNS反射源、NTP反射源数量、PORTMAP反射源、SNMP反射源都有增加，其中SSDP反射源和PORTMAP反射源的增长数量最多。



关键发现2：中美TCP反射源数量遥遥领先。

根据腾讯安全DDoS防护团队的监测数据，现网捕获到的TCP反射源的总量在千万级别，成为黑产大军攻击资源的重要组成部分。

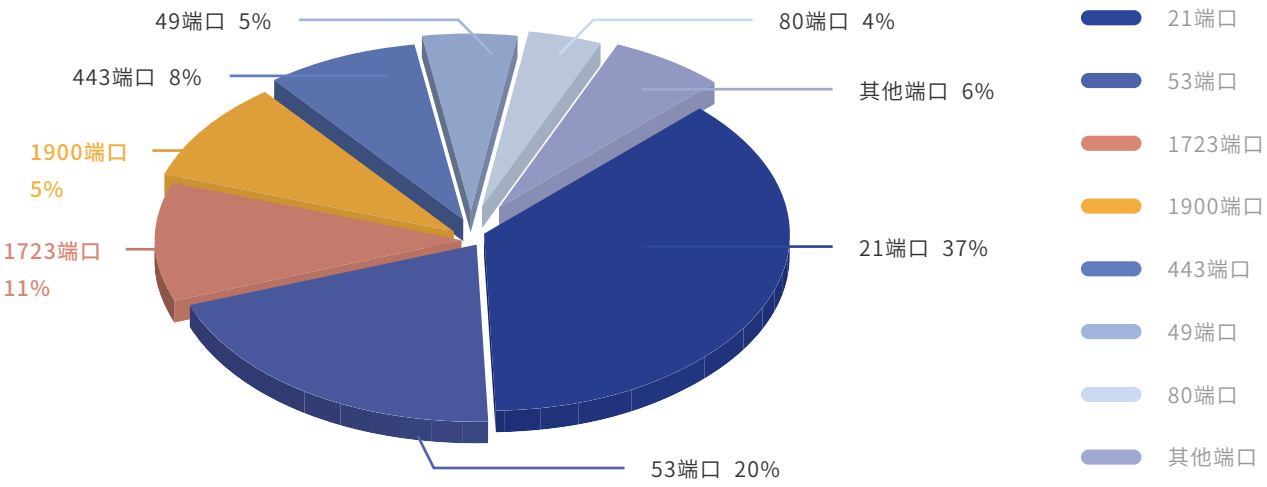
由于TCP反射源是利用互联网开放服务的服务器发起攻击，所以这部分攻击源的分布非常广泛。其中中美两国的反射源数量遥遥领先，此外，德国、日本、法国、韩国、英国等发达国家的TCP反射源数量也较多。



IDC服务器是主要的攻击来源。一些常见IDC服务器上开放的端口，如TCP 21/53/80/443等，均被黑客用于发起TCP反射攻击。

此外，一些不为人熟悉的端口，如主要是由家庭路由器开放的TCP　1723/1900等端口也被攻击者发现，用来发起DDoS攻击，让人防不胜防。

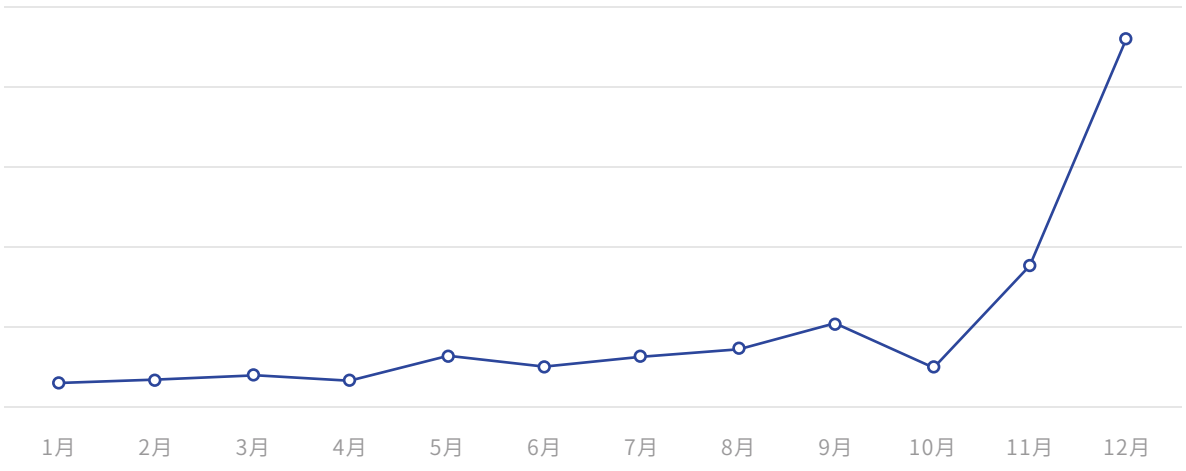
TCP反射源的端口分布



关键发现3：XOR.DDoS僵尸网络为现网最为活跃僵尸网络家族。

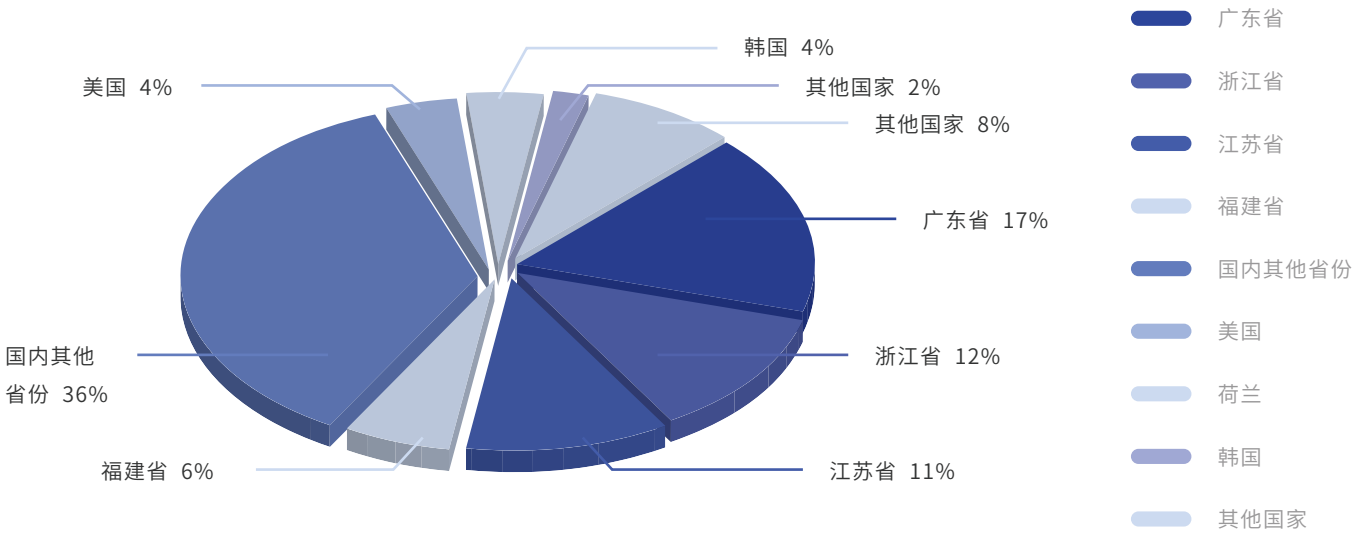
根据腾讯安全DDoS防护团队的监测数据，XOR.DDoS僵尸网络是现网最活跃的DDoS攻击僵尸网。所有参与DDoS攻击的肉鸡中，XOR.DDoS僵尸网络的肉鸡占整体比例超过6成。值得重点关注的是，进入第四季度以来，XOR.DDoS僵尸网络的活跃程度进一步加强，发起的DDoS攻击次数远远超过前几个季度。

2020年XOR.DDoS僵尸网络发起的DDoS攻击走势



据分析，该僵尸网络控制的肉鸡大部分都分布在中国国内，以经济较为发达的广东、浙江、江苏等省份为主。分布在国外的肉鸡大约占比18%左右，仍然以经济较发达的美国、荷兰、韩国等国家为主。

XOR.DDoS僵尸网络的肉鸡地域分布

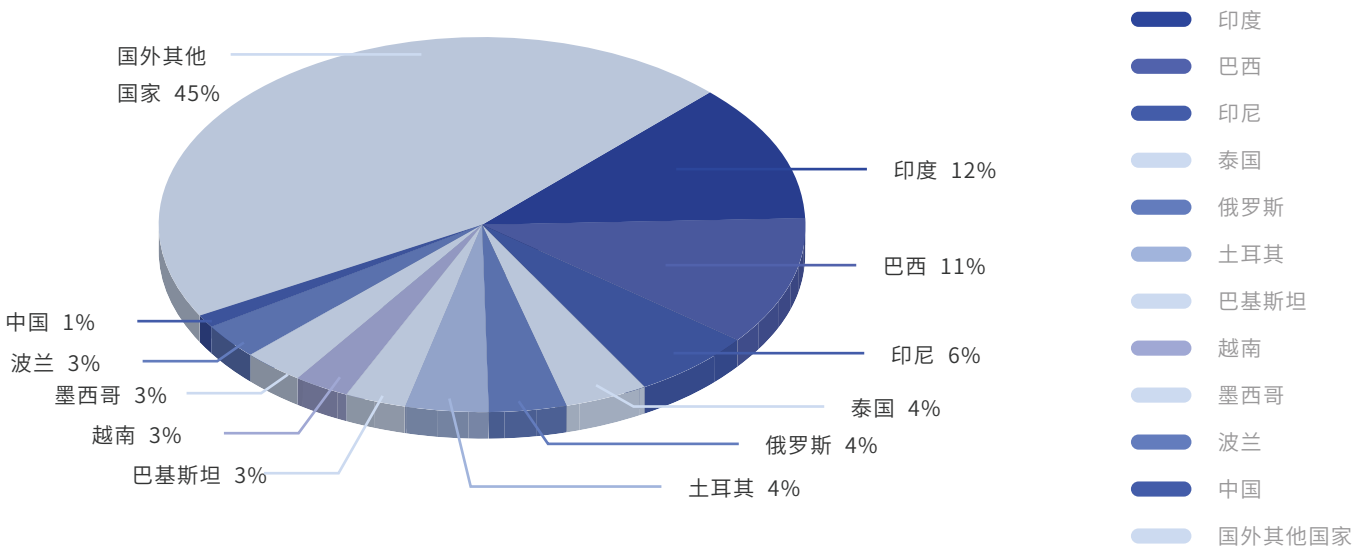


关键发现4：大量秒拨IP被黑客用于发起应用层DDoS攻击。

根据腾讯安全DDoS防护团队的监测数据，2020年的应用层DDoS攻击的最大攻击流量达到330万QPS的海量级别，远远超过历年应用层DDoS的最大攻击流量。深入分析后发现，大量秒拨IP流入DDoS攻击黑产大军，是应用层DDoS攻击达到海量的主要推手。

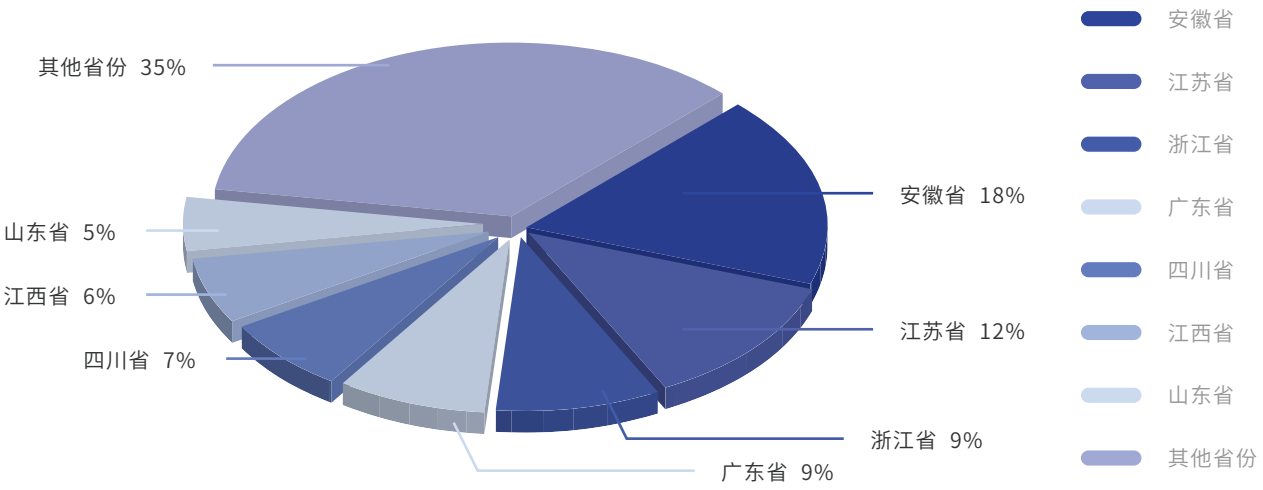
在2018年上半年，腾讯安全DDoS防护团队曾防护过一次持续时间超过9天的超大流量应用层DDoS攻击，最大流量接近50万QPS，累计捕获到的攻击源IP超过500万。尽管攻击目标是位于中国大陆的IP，但是这些攻击源IP的分布地域却主要以国外为主，主要来源国家有印度、巴西、印尼、俄罗斯等国，其中有大量的摄像头、打印机、路由器等IoT设备IP。经过进一步的分析，确认这是一次典型的黑客利用Mirai僵尸网络发起的攻击。

2018年某次攻击中捕获的Mirai僵尸网络攻击源分布



但在2020年，腾讯安全DDoS防护团队曾监测到多次最大流量超过100万QPS的应用层DDoS攻击。通过进一步分析发现，这些攻击的攻击源和以往大有不同。分析数据显示，这些秒拨IP的分布区域以国内为主，主要分布在安徽、江苏、浙江、广东等国内的经济或人口大省。除了参与发起DDoS攻击外，这些IP还大量在刷单、秒杀、养号、差评等风控场景频频出现，说明DDoS攻击黑灰产的资源和风控场景的黑灰产资源之间存在频繁流转。

秒拨IP的来源省份分布



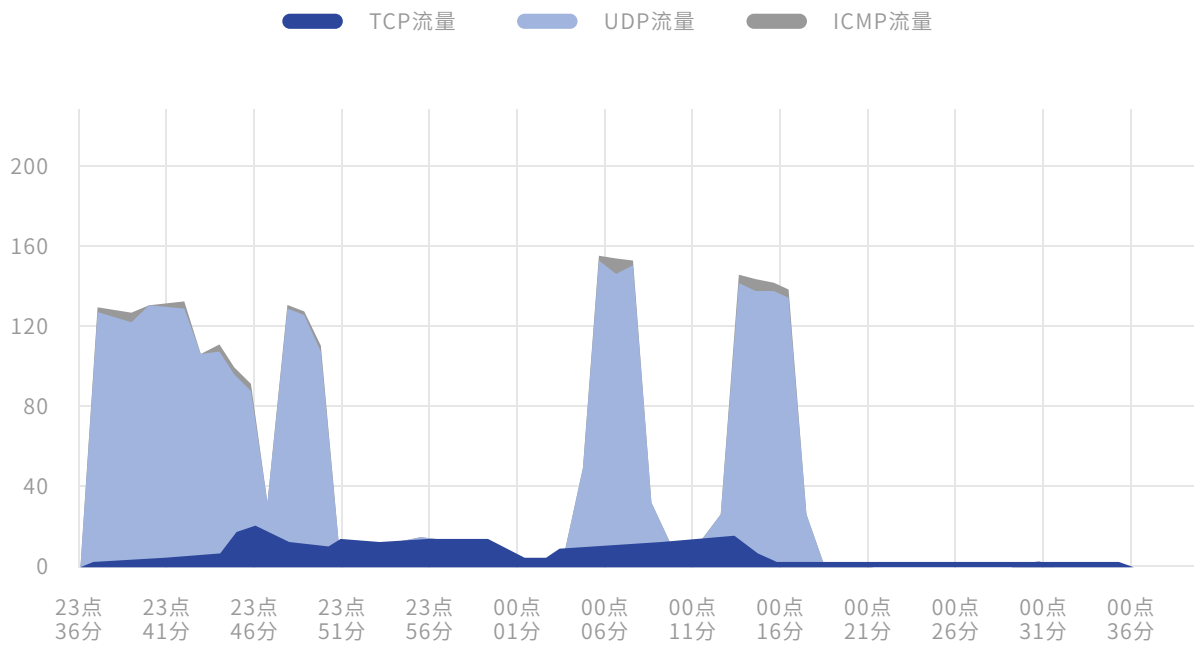
03 防护案例与建议

案例1：超大流量混合型DDoS攻击

2020年5月份，某游戏客户官网在完成HTTPS协议切换数年后，首次遭受超大流量DDoS攻击，持续时间超过1个小时。

攻击特征：

攻击手法为混合型DDoS攻击（CLDAP反射+SSDP反射放大攻击+ICMPFLOOD+HTPPS CC攻击）。最大攻击流量超过140G，另外还有260万QPS的HTTPS CC攻击。应用层攻击的攻击来源IP主要分布在国内的经济发达、人口稠密的省份，与正常的客户来源分布高度一致。



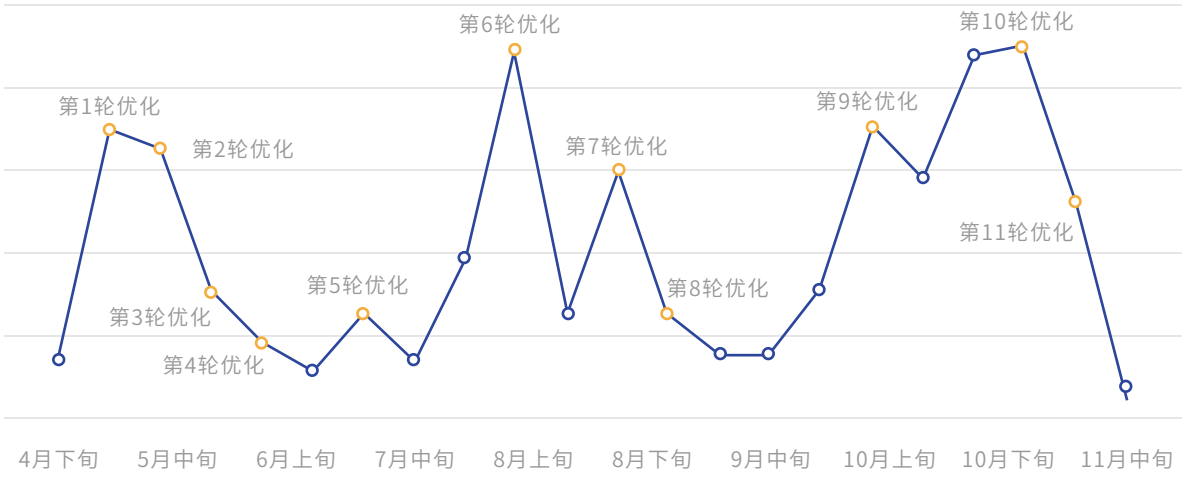
防护建议：

1. HTTPS应用层攻击大幅增长，攻击峰值动辄上百万QPS，除了影响被攻击业务，还会波及共用应用层网关的其他业务。企业在切换HTTPS后需同步关注HTTPS应用层DDoS攻击的风险。
2. 混合型攻击越来越常见，防护方案需要覆盖多种防护场景，多层防护联动，一站式解决各类攻击场景。
3. 大量具有分布广、切换快等特点的秒拨IP流入DDoS攻击市场，只有结合大数据+AI智能防护算法，结合强大的威胁情报能力，才能准确拦截攻击流量，避免误伤正常用户。

案例2：游戏企业DDoS攻防对抗

2020年Q2开始，某游戏被国外外挂团伙盯上。该团伙开发出一款“炸房挂”，通过调用第三方攻击站点发起DDoS攻击，引发游戏玩家掉线，游戏服务器宕机等严重后果。外挂团伙很快将外挂以数十美元的价格，批量售卖给恶意玩家，导致DDoS攻击在多个地域的服务器出现多轮爆发。经过近十轮紧张激烈的攻防对抗，DDoS威胁爆发的态势终于在11月份达到有效的控制和缓解。

攻防对抗走势



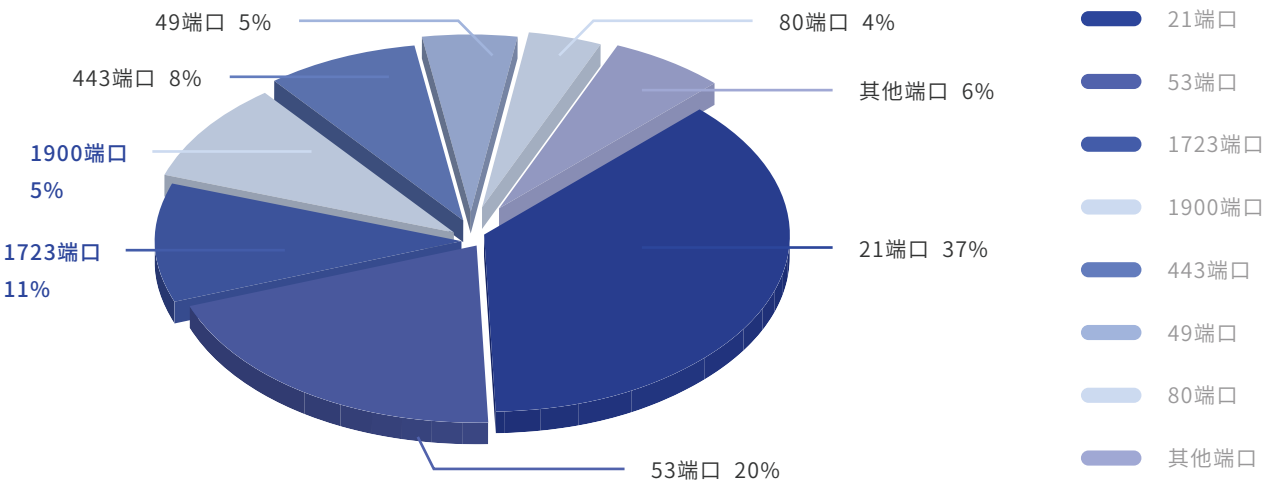
防护建议：

1. 海外DDoS攻击黑产在遭受司法重击之后迅速复苏，游戏企业出海必须重视DDoS攻击威胁，提前准备应对方案。
2. 国外黑产团伙技术实力强大、攻击资源丰富，需要有丰富经验的安全团队支持，从而和黑产团伙持续进行攻防对抗。同时，也需要储备较大的网络带宽来应对超大流量DDoS攻击，并具备高速的策略迭代效率来迅速补齐防护策略。
3. 攻防对抗具有全方位、多层次的特点，同时需要业务团队、安全团队、网络运营商等多方协作。

案例3：TCP反射危害

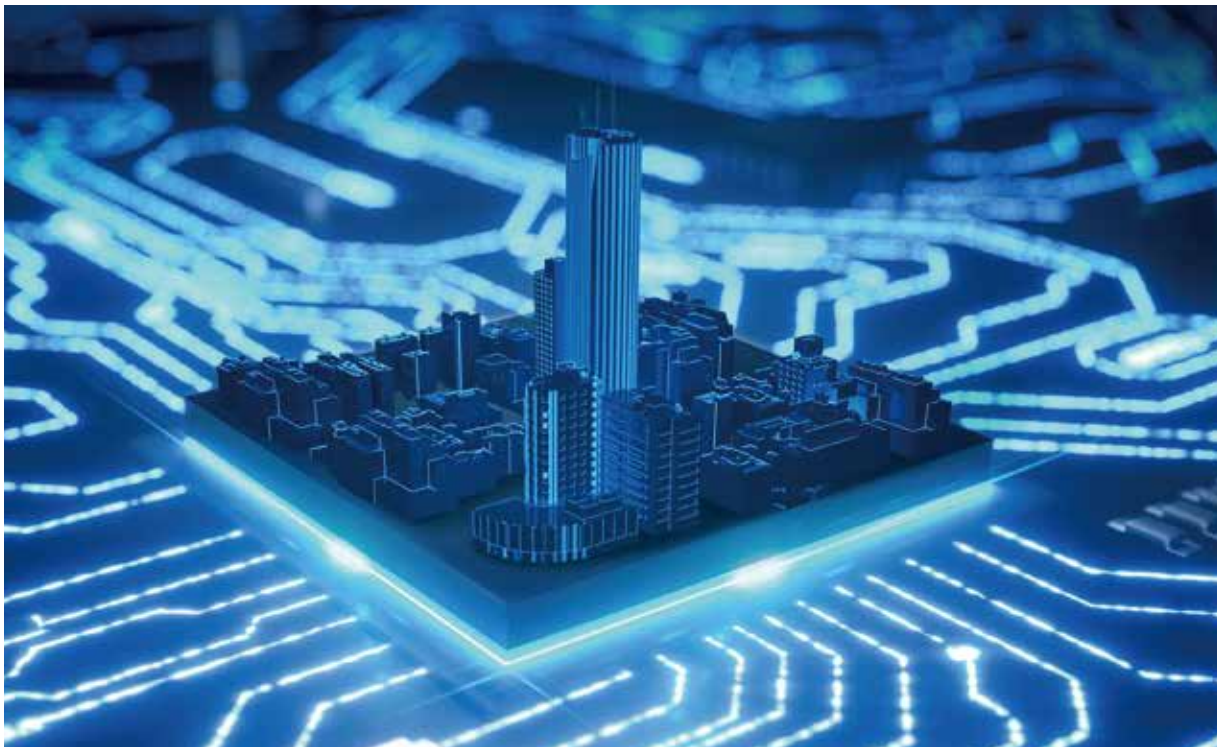
2018年以来，TCP反射手法逐渐进入攻击者的视线。但2020年第三季度以来，TCP反射攻击手法不仅越来越活跃，而且攻击流量也大幅攀升，200G以上的TCP反射攻击屡见不鲜。除了IDC服务器上常见的TCP 53/80/443/22/21端口外，家庭网络的TCP 1900/1723等端口也被攻击者挖掘出来。

TCP反射源的端口分布



防护建议：

1. TCP反射手法中的攻击源IP都是真实存在的服务器IP，因此传统的反向验证等算法很容易被绕过，需要结合大数据和AI技术的智能算法才能有效防护。
2. TCP反射攻击流量可在极短时间内迅速蹿升，且来源非常分散，需要秒级防护、秒级响应。
3. 由于TCP反射的攻击包极小，数百G流量的TCP反射攻击包量可以达到数亿pps，还需要强大的高性能处理防护平台，以便在高效清洗攻击流量的同时，降低对正常业务的处理延迟。



了解更多产品信息

请扫码关注腾讯云T-Sec DDoS 防护

04 产品介绍

产品介绍

腾讯云T-Sec DDoS防护，基于近二十年腾讯海量业务安全实践自主研发，具备覆盖全球的秒级响应延迟和T级清洗能力。

通过IP画像、行为模式分析、Cookie挑战等多维算法，并结合AI智能引擎持续更新防护策略，可有效防御IP层到应用层的各类型DDoS攻击场景。

同时支持IPv4/IPv6双栈防护，为企业组织提供 DDoS 高防包、DDoS 高防 IP 等多种 DDoS 解决方案，一站式解决各类DDoS 攻击问题。

防护场景覆盖游戏、互联网、视频、金融、政府等行业。