腾讯安全 Tencent Security | NSFOCUS

2021年上半年
全球DDoS威胁报告

腾讯安全DDoS防护团队 | 绿盟科技国际云清洗服务团队

目录

01 专家观点

1.1 DDoS攻击连续4年高速增长

受疫情影响，日常工作生活和休闲娱乐等活动从线下更多的转移到线上，也间接促进了如在线办公、在线游戏等业务的发展。同时游戏DDoS攻击黑产团伙已经从2017年底的重创中恢复，DDoS攻击连续4年呈高速增长态势。

1.2 大流量攻击挑战加剧

网络带宽持续增长，新的攻击资源不断被黑客团伙挖掘出来， 100G以上的大流量攻击次数大幅增长，且增长幅度高于整体攻击次数的增长幅度。特别是TCP反射的攻击手法更是会伴随非常大的包速率，能取得更好的攻击效果，大流量 TCP反射攻击成为防守方面临的严峻挑战。

1.3 虚拟货币价格与攻击趋势涨跌呈负相关

通常情况下，DDoS攻击与互联网产业的发展呈正相关。互联网越发达，网民数量越多的区域，通常也是DDoS攻击越多，DDoS攻击源数量越多的区域。此外，各国政府对黑产团伙的司法打击力度，以及对网络安全的立法也会对DDoS攻击活动造成影响。

但近年来，通过进一步研究发现，由于肉鸡资源既可以发起DDoS攻击，又可以用于挖矿，挖矿活动和DDoS攻击活动对于肉鸡资源存在竞争关系。如果虚拟货币价格持续走高，肉鸡资源就会大量流入到挖矿活动，反之则会大量流入到DDoS攻击活动。因此部分主要利用肉鸡发起的DDoS攻击（如SYN大包）与虚拟货币的价格呈现明显的负相关关系。而最近2年数据表明，新冠疫情的防控形势，除了会对当地的经济造成巨大的影响外，对DDoS攻击活动也有明显的扰动。

1.4 恶意竞争、敲诈勒索、游戏作弊是攻击主要动机

除了在互联网各行业普遍存在的恶意竞争和黑客团伙敲诈勒索引发的DDoS攻击外，恶意玩家为了作弊发起DDoS攻击也成为游戏行业的一个挥之不去的阴影。

1.5 UDP反射放大攻击成最受欢迎手法

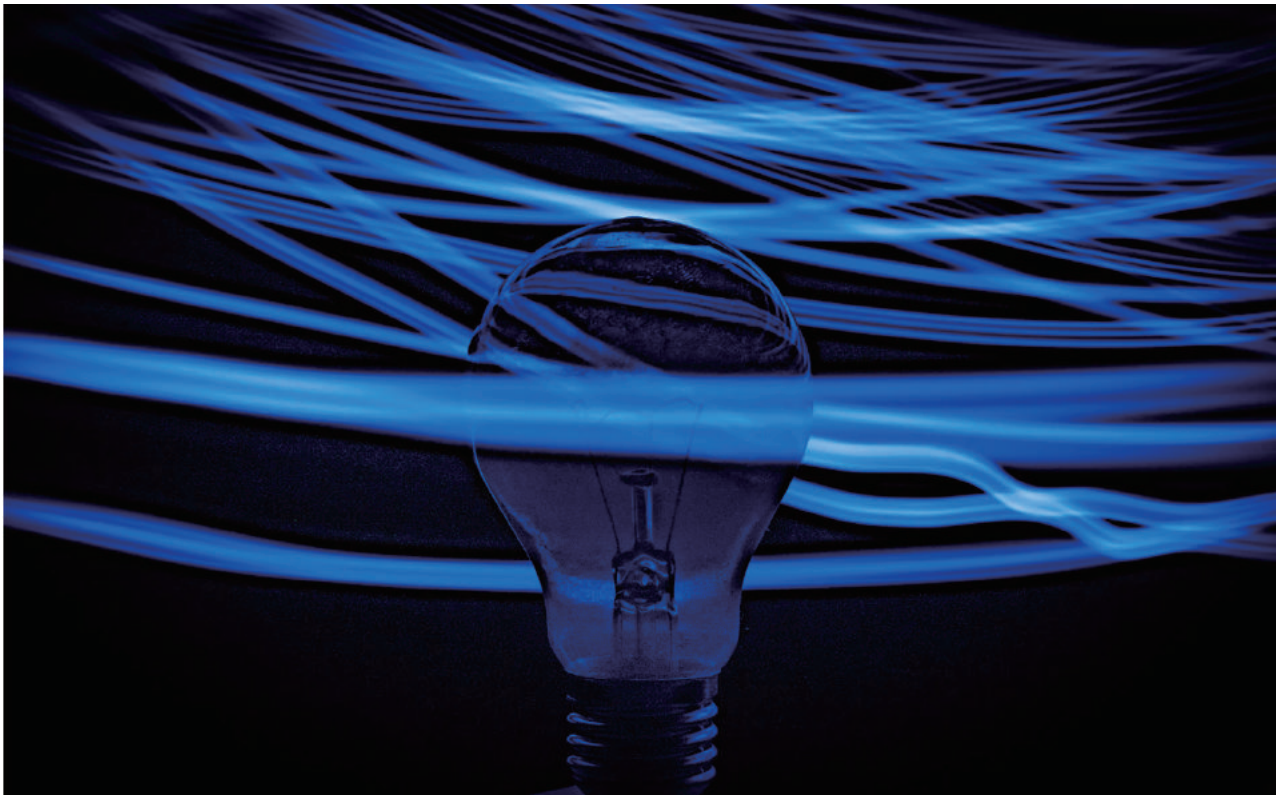
UDP反射放大攻击既有大量的攻击资源又有较为可观的放大倍数，且很难溯源；另外，黑产产业链对UDP反射放大攻击进行了充分的封装，进一步降低了攻击的门槛。以上两个因素导致UDP反射放大攻击成为最受攻击者欢迎的攻击手法，其中最为突出的手法为NTP反射。随着疫情和远程办公的影响，客户正常业务中OpenVPN流量占比逐渐增大，而OpenVPN则因为拥有超过100万的攻击源数量，逐渐成为新型UDP反射攻击中的黑马。

1.6 TCP反射受黑客青睐

由于有数量巨大且分布广泛的攻击资源，TCP反射越来越受全球黑客的钟爱，攻击次数及攻击规模都在持续增长，新的服务端口（如TCP 7547/3306等）也被不断挖掘出来。2021年以来，百G以上的TCP攻击屡见不鲜，包速率动辄数以亿计，对上下游网络设备、防护设备以及云端清洗服务的性能造成了严峻挑战。

1.7 云平台DDoS防护日趋重要

为了突破防护、提升攻击效果，DDoS攻击团伙除了不断地挖掘新攻击手法外，也会独辟蹊径，利用现有的手法针对防护方的薄弱点发起攻击，两种最为典型的手段就是针对平台发起扫段攻击以及针对网关IP发起攻击，这导致云平台自身的DDoS防护成为一个非常重要的防护场景。



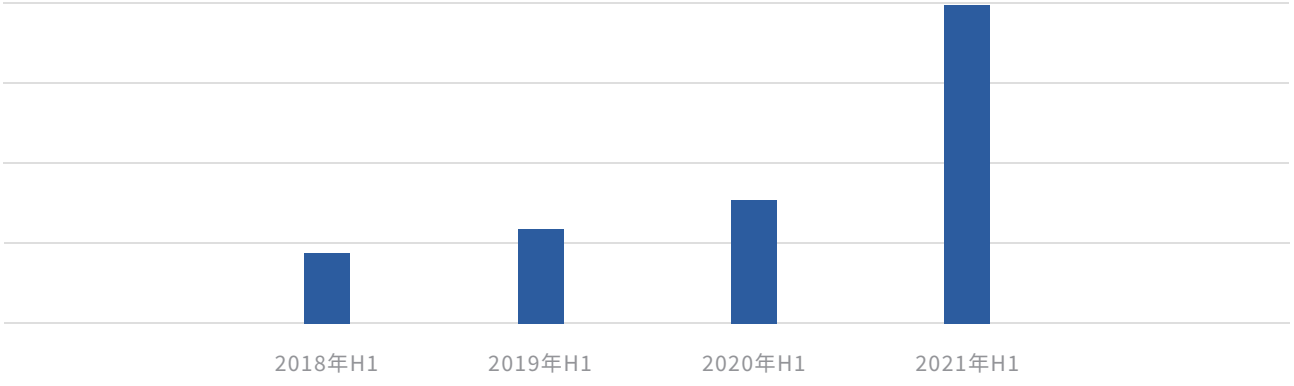
02 整体威胁

2.1 互联网业务持续繁荣，攻击次数连增4年

尽管新冠病毒疫情给各行各业均带来较大冲击，但是互联网业务相对受影响较小，加上大量的经济活动持续向线上迁移，游戏、直播、电子商务、线上教育等行业持续繁荣，同时黑产团伙也从17年下半年的司法打击重创中复苏，上述因素推动DDoS攻击次数呈现连增4年的趋势。

云上攻击走势

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

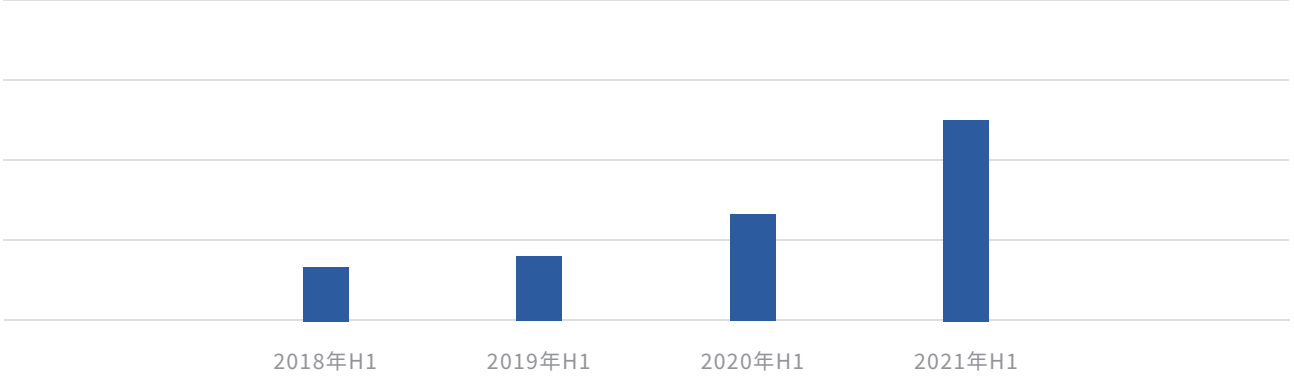


2.2 百G以上流量攻击大幅增加

云计算大数据以及5G的快速普及，推动互联网网络带宽持续高速增长。而大量存在安全缺陷的IoT设备/IDC服务器以及个人PC等持续被黑客利用，沦为黑客的攻击资源。充足的攻击资源导致黑客发起100G以上大流量的攻击次数大幅增加。

100G以上大流量攻击次数

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

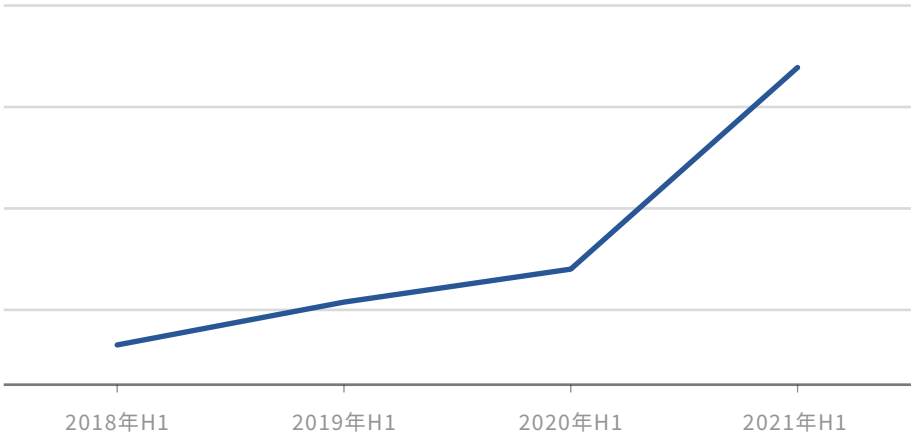


2.3 国外攻击次数持续增加

疫情的影响遍及全球，线下业务持续向线上迁移的趋势在中国以外的其他国家也很明显，线上业务的繁荣免不了引来DDoS攻击黑产团伙的觊觎，因此中国以外区域的DDoS攻击也呈持续增加的趋势。

中国以外其他国家攻击次数

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

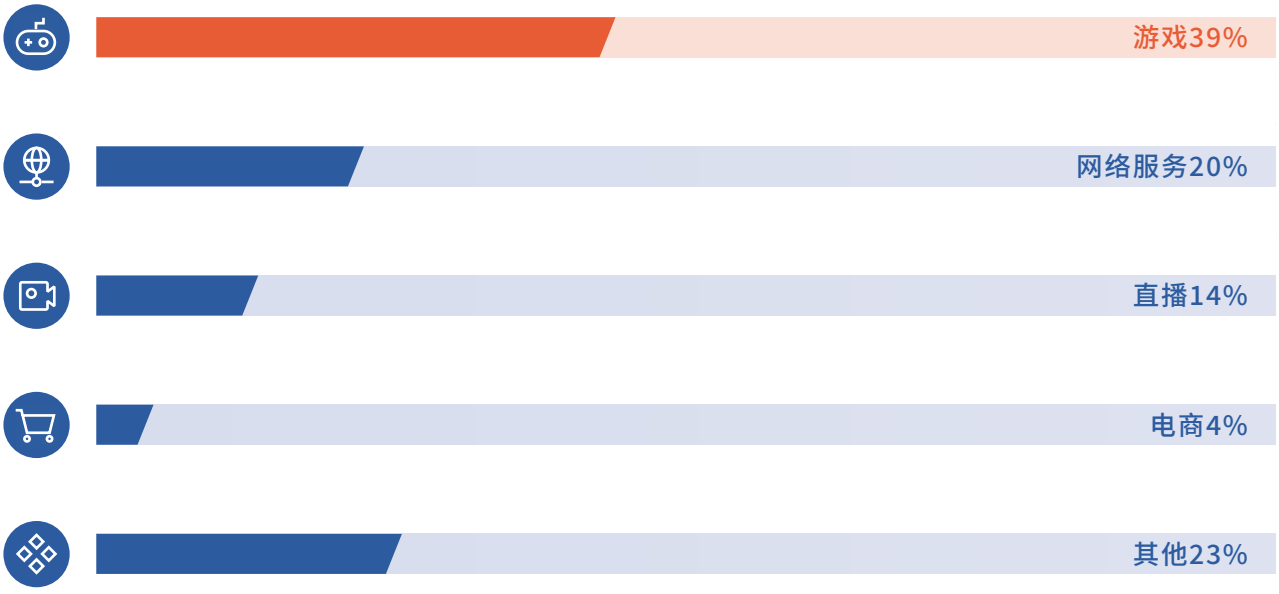


2.4 游戏行业首当其冲

游戏服务器对DDoS攻击较为敏感，同时游戏行业竞争较为激烈。上述因素导致游戏行业成为DDoS攻击最多的行业。

DDoS攻击行业分布

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

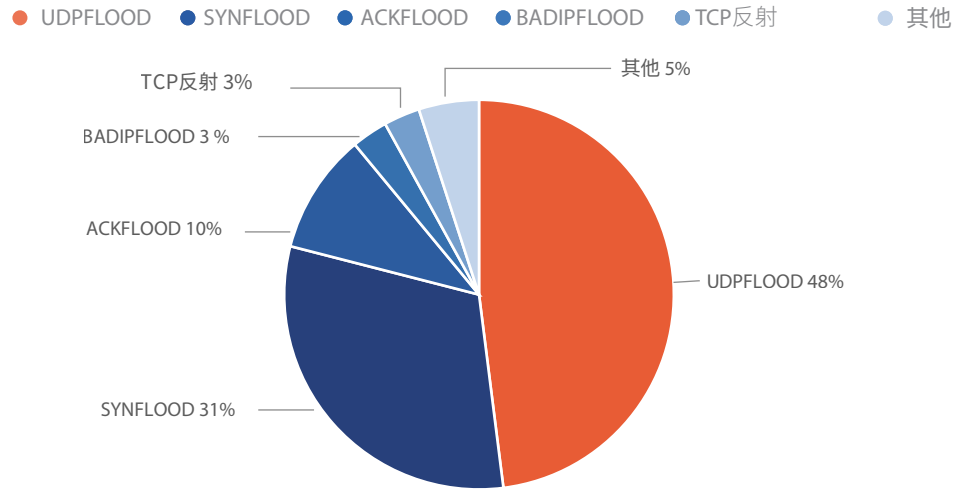


2.5 UDPFLOOD为大流量攻击主流

由于具有可大幅放大初始攻击流量以及攻击资源多、难溯源的特性，UDP反射放大攻击手法为主的UDP-FLOOD深受攻击者喜爱，继续成为DDoS攻击主要威胁场景。

DDoS攻击分布-类型维度

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

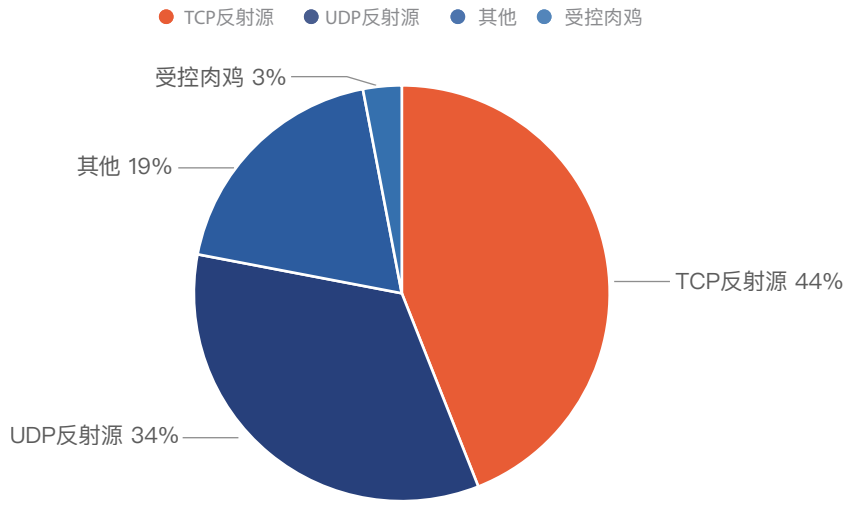


2.6 TCP反射源成数量最大攻击资源

由于互联网上对公众开放TCP80/443/22/21等端口的服务器数以亿计，同时不安全的网络配置导致大量的家庭网络对互联网暴露了TCP7547/1900等端口，TCP反射源因此成为数量最大的攻击资源。

攻击资源分布

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）



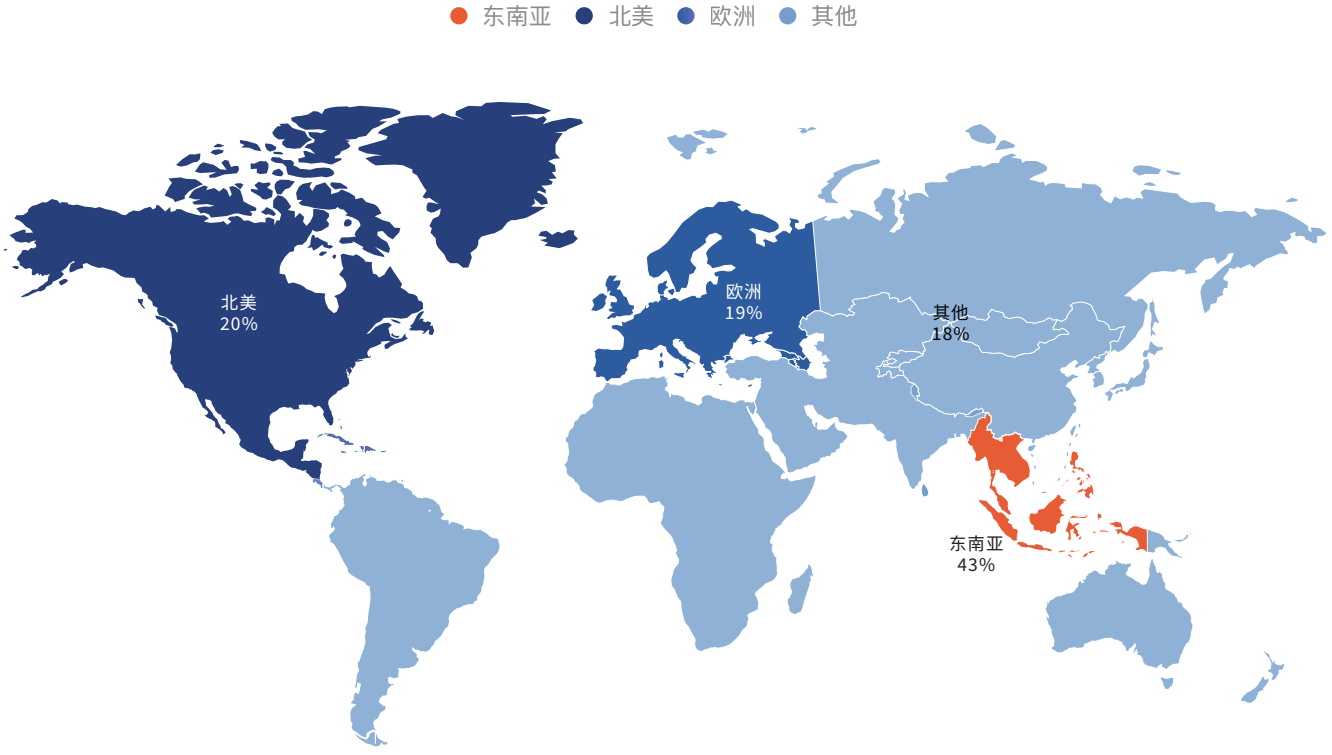
03 海外威胁

3.1 东南亚、北美、欧洲遭受攻击最多

一般而言，DDoS攻击活动与当地的网民数量以及互联网产业的发展程度呈高度相关。因此网民数量巨大且互联网经济较活跃的东南亚、北美、欧洲不仅是游戏、电商等行业海外布局的重点区域，也是国外DDoS攻击活动的主要被攻击区域。

中国以外DDoS攻击地域分布

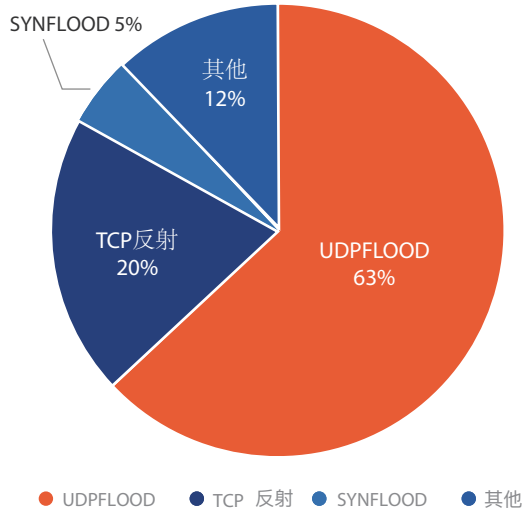
（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）



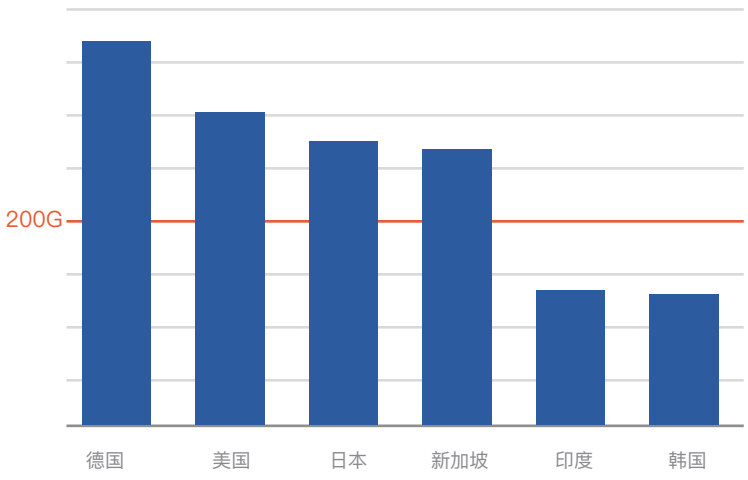
3.2 海外UDP反射放大攻击威胁严峻

与整体威胁中的占比相比，由于国外大量的售卖DDoS攻击的站点都优先支持UDP反射等UDP协议攻击，以UDP反射为代表的UDPFLOOD攻击在国外更为泛滥，占比更高。而且大流量攻击基本都为UDP反射放大攻击，更有多个国家最大攻击流量超过200G。

中国以外DDoS攻击的类型分布
（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁



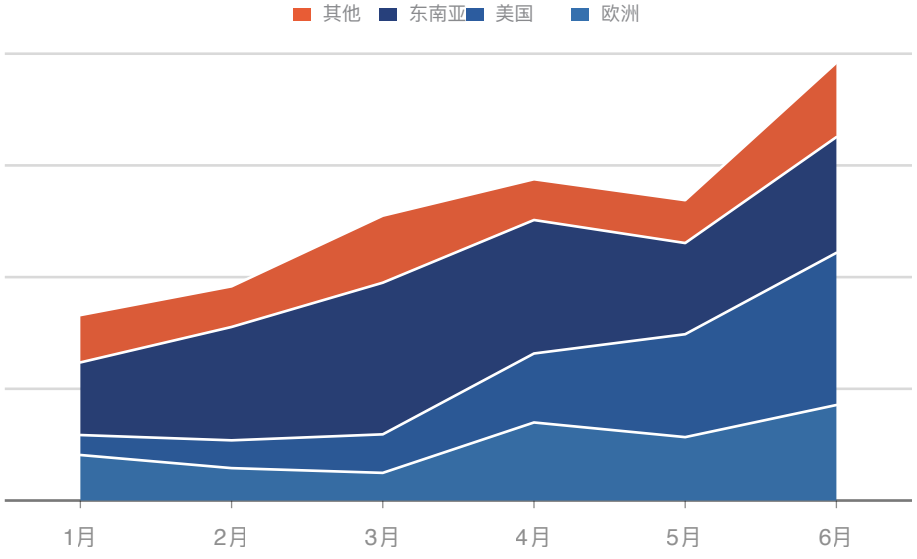
腾讯云业务海外最大攻击流量分布
（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）



3.3 位于欧美的攻击源明显增长

国外DDoS攻击在上半年总体呈现逐月增加趋势，其中欧洲和美国区域的增长较为明显。

国外主要区域的攻击走势
（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

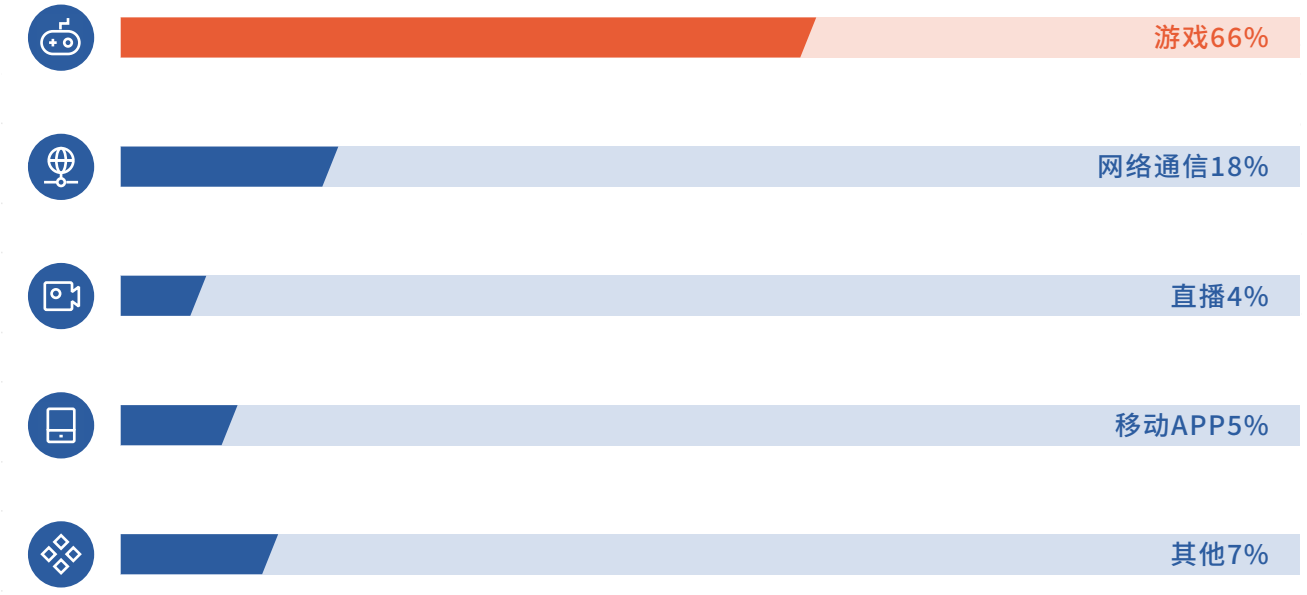


3.4 攻击聚焦游戏行业

由于多个业界知名的敲诈勒索黑产团伙（如Fancy Lazarus/Fancy Bear等）在国外比较活跃，另外像ACCN等团伙也会针对性地对出海的游戏企业进行敲诈勒索，因此针对游戏企业发起敲诈勒索在国外更为普遍，在加上恶意游戏玩家发起攻击等场景，导致国外DDoS攻击在游戏行业更为聚集，占比超过6成。

DDoS攻击行业分布

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

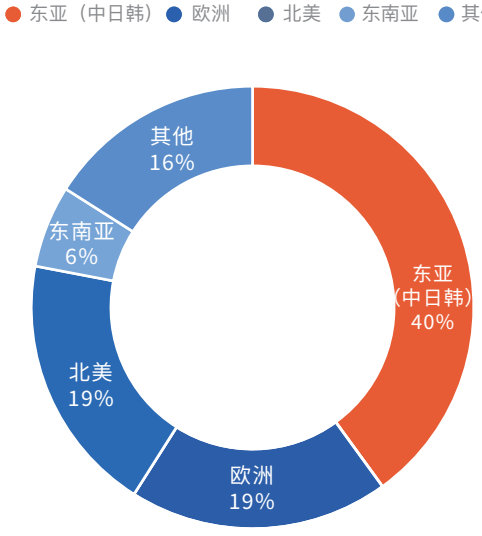


3.5 攻击源来源全球化

国外DDoS攻击的攻击源来源也有明显的全球化趋势，广泛分布在很多国家，其中网民数量多、互联网产业发展程度高的东亚（中日韩），欧洲，北美等区域成为攻击资源的主要贡献地。

海外DDoS攻击行业分布

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）



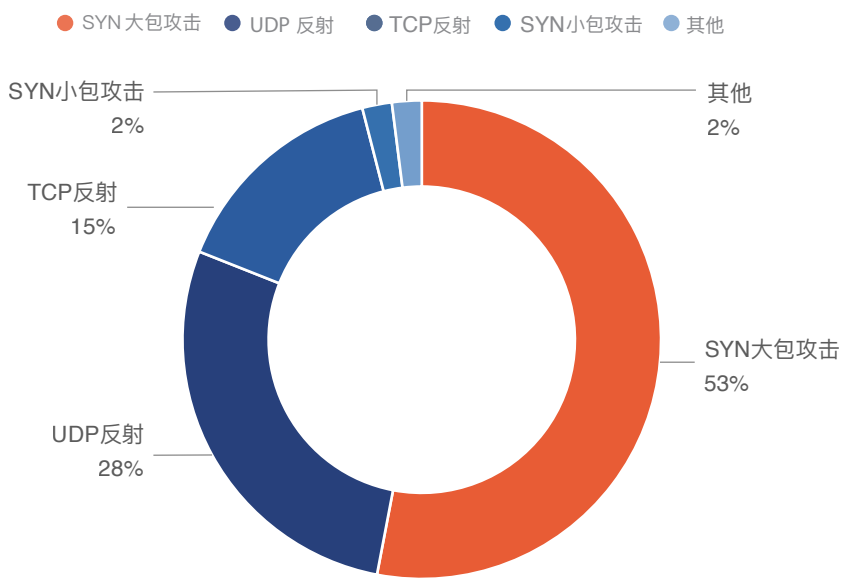
04
黑产视角

4.1 SYN大包攻击和UDP反射是黑客发起大流量攻击的主要手法

和往年百G以上大流量攻击主要以UDP反射和SYN大包主导不同，今年上半年的百G以上大流量攻击呈现三足鼎立的格局，SYN大包超过UDP反射成为最主要的攻击手法。TCP反射手法成功挤进前三，占比达到16%。

百G以上大流量攻击手法分布

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

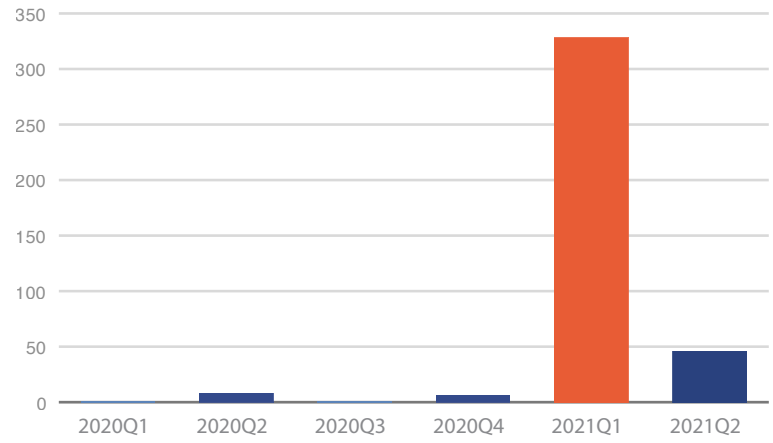


4.2 TCP反射呈明显海量化趋势

由于同时具有危害大（同等带宽下拥有最大的包速率），资源多（互联网上有大量开放TCP端口的服务器和设备）等优势，TCP反射呈现明显的海量化趋势，峰值流量超过百G，包速率数以亿计的大型TCP反射攻击同比增长数十倍。

百G以上的TCP反射攻击次数走势

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

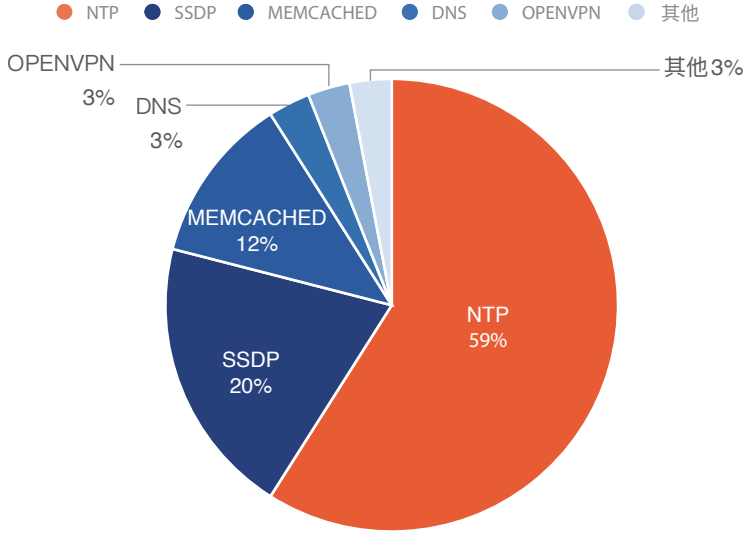


4.3 NTP反射是最常见的UDP反射手法

攻击源数量多且绝大多数为高配服务器，同时拥有较为可观的放大倍数，导致NTP反射成为最常见的反射攻击手法。

UDP反射放大手法攻击次数分布

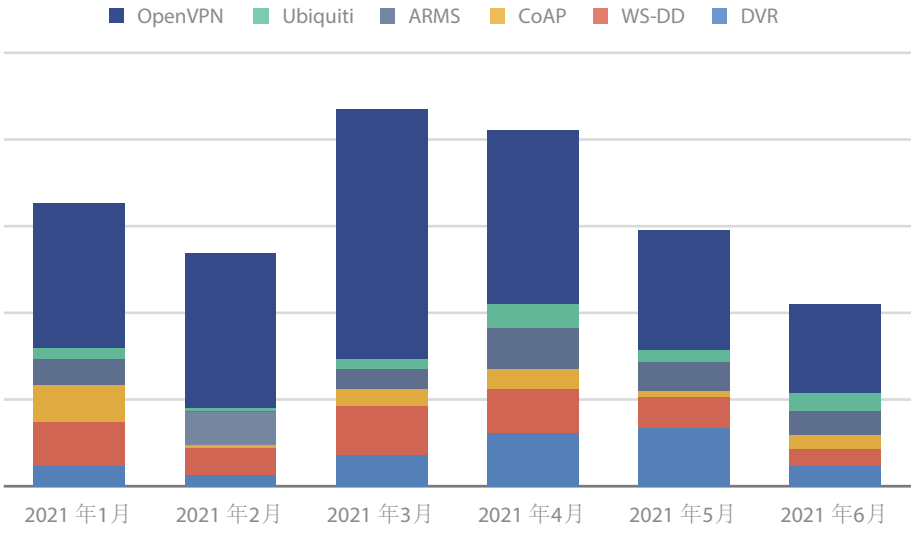
（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）



4.4 OpenVPN反射成为新型UDP反射手法中的黑马

今年上半年，OpenVPN反射，DVR反射，WS-DD反射等新手法在现网也较为活跃，其中OpenVPN反射出现的频率远远领先于其他手法，成为新型UDP反射攻击中的黑马。

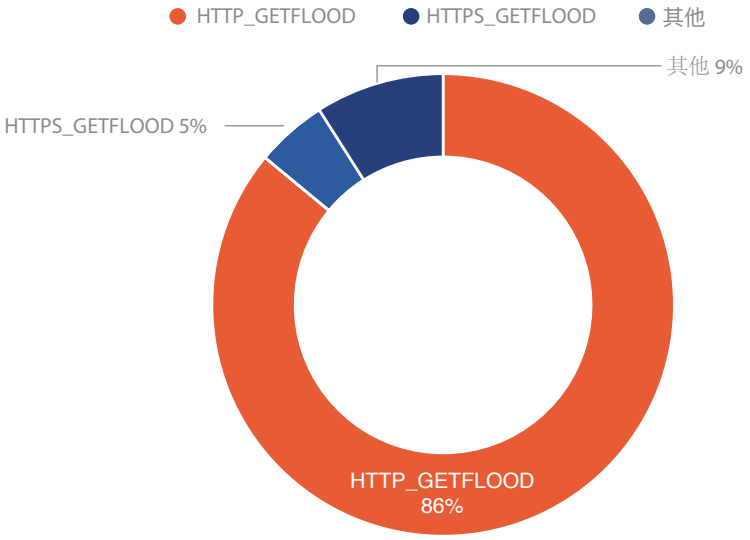
新型UDP反射攻击手法攻击次数走势
（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）



4.5 GETFLOOD仍然是应用层攻击的主要场景

GETFLOOD历来是应用层攻击的主要场景，今年上半年HTTP协议GEFLOOD和HTTPS协议GETFLOOD在应用层攻击中的占比合计达91%。

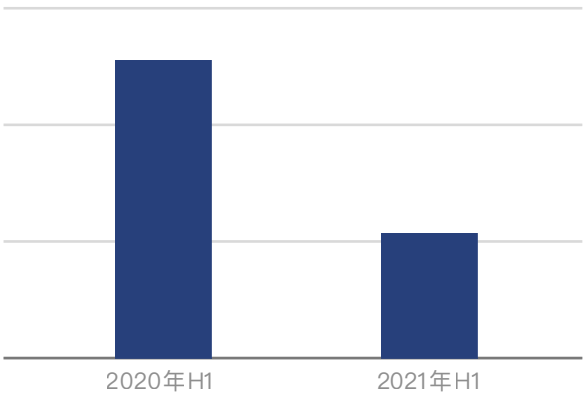
应用层攻击手法分布
（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）



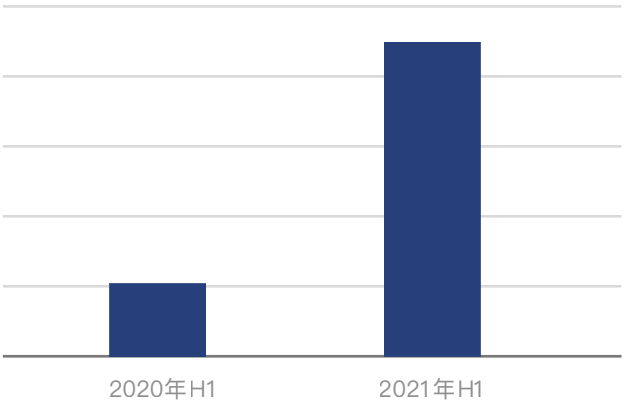
4.6 肉鸡数量同比下降，但攻击活动更为活跃

由于上半年比特币/以太坊等虚拟币的价格处于历史高位，导致大量肉鸡流入挖矿领域，上半年捕获到参与DDoS攻击的肉鸡数量出现明显下降，大约只有去年的一半左右，但是发起的攻击次数却是去年的4倍左右。

肉鸡数量下降



肉鸡发起攻击次数上升

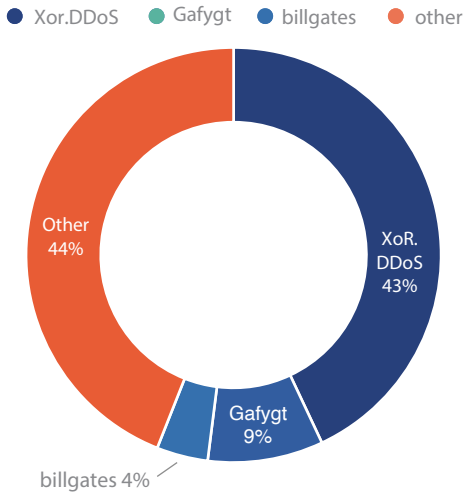


注：数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告

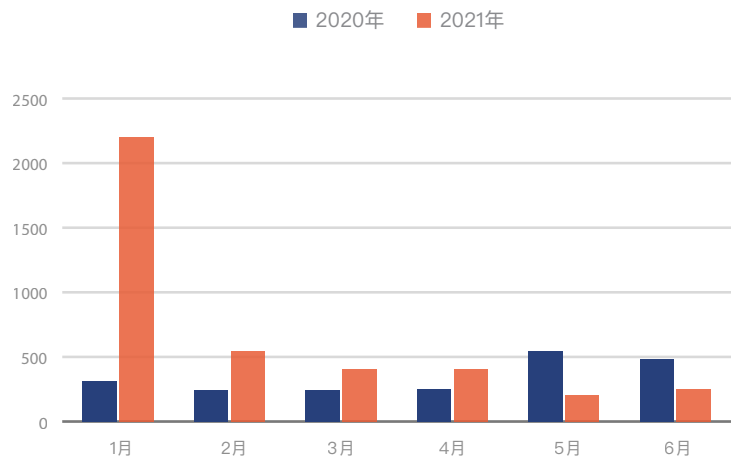
4.7 XoR.DDoS僵尸网络是现网危害最大的僵尸网络

由于利用弱密码获取肉鸡的成本最低，XoR.DDoS僵尸网络仍是危害最大的僵尸网络，在现网的肉鸡数量中占据了4成的份额，此外以物联网设备为主的Gafygt僵尸网络也成为了现网第二活跃的僵尸网络。

肉鸡所属僵尸网络分布



XoR.DDoS僵尸网络发起的攻击走势



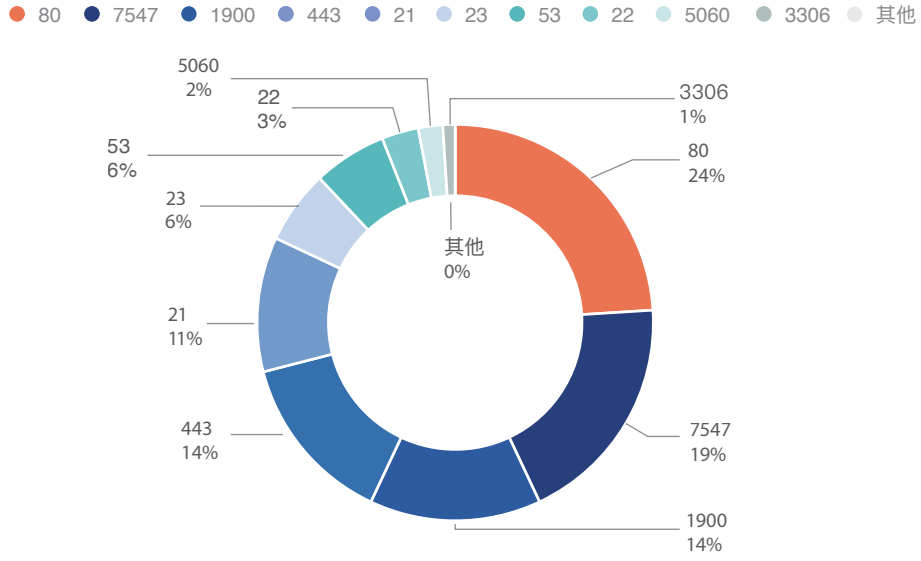
（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁

4.8 家庭网络的部分端口被黑客用于发起TCP反射

TCP反射近年来非常受黑客青睐，为了增加攻击威力，黑客不断挖掘新的反射端口。除了IDC服务器上常见的80/443/21/23/22端口外，3306端口也被黑客利用。黑客还把魔爪伸向了家庭网络，部分家庭网络由于不安全的配置导致对外暴露的TCP 7547/1900/5060等端口也被黑客用于发起TCP反射DDoS攻击。

TCP反射攻击源的端口分布

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

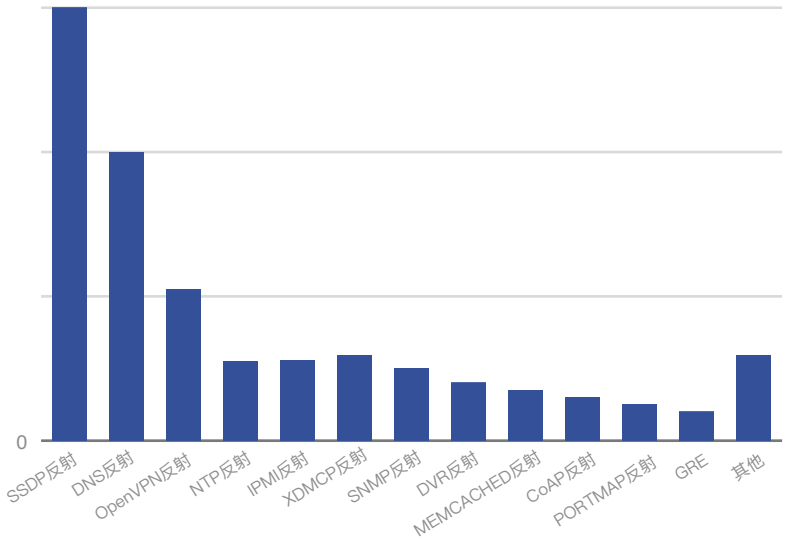


4.9 OpenVPN反射源的数量突破百万

OpenVPN攻击源数量超过NTP反射等传统UDP反射手法，OpenVPN反射源数量进入前三。

各类UDP反射手法攻击源数量

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

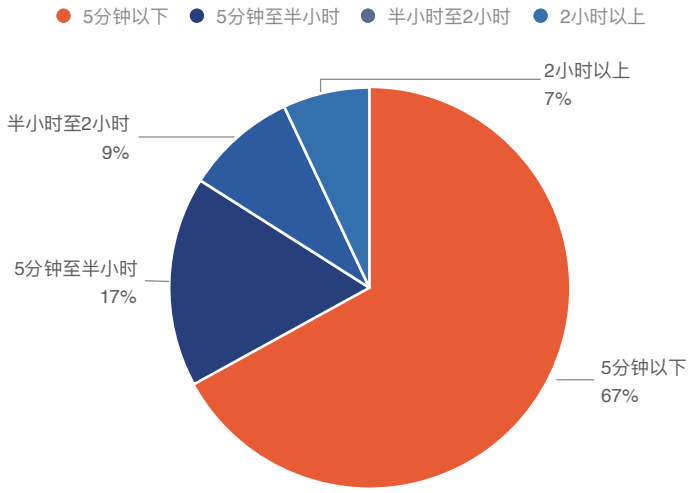


4.10 大多数攻击持续在半小时以内

黑产大量调用DDoS攻击站点发起攻击，导致绝大多数攻击持续在半小时以内。

攻击持续时长分析

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

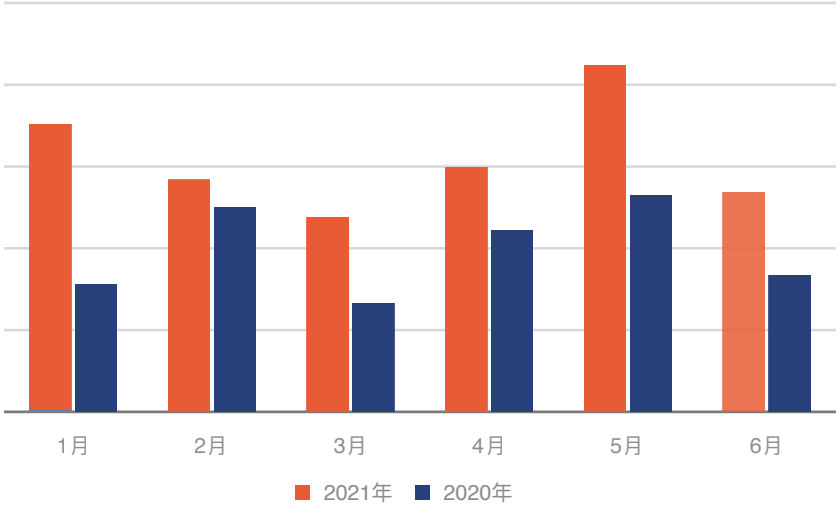


4.11 5月和2月攻击最多

从DDoS攻击的月度分布可以看出，今年的每个月的攻击相比去年都有增长。由于春节前企业放假和员工返乡的原因，往年的1月往往会出现明显回落，成为上半年DDoS攻击次数最少的月份。但是今年春节前后和五一长假期间，DDoS攻击活动较为活跃，导致今年1月的攻击次数不仅没有回落反而高居第二，五月则成为上半年攻击最高峰。

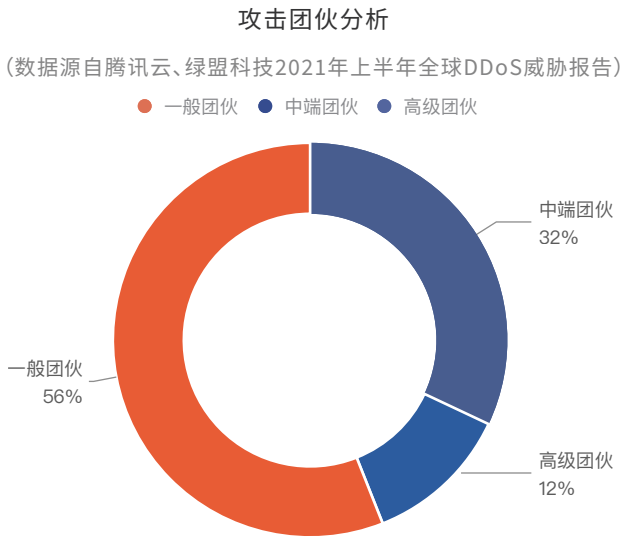
DDoS攻击分布-时间维度

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）



4.12 大部分攻击由一般团伙发起

由于黑产攻击站点不断完善攻击手法的封装，降低DDoS攻击的门槛，只要具备操作电脑的基本技能的人都能发起一场DDoS攻击。因此大部分DDoS攻击主要由一般团伙或者中端团伙发起。拥有自己的攻击资源、能够定制攻击工具，发起超大流量DDoS攻击的高级团伙发起的攻击占比超过1成。



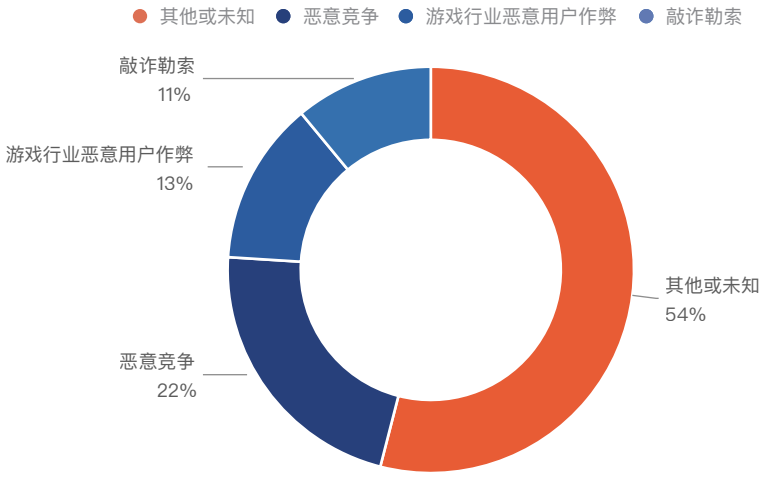
*注：高级团伙可发起数百G甚至上T大流量攻击，中端团伙可发起上百G大流量攻击，一般团伙攻击流量常在100G以内。

4.13 DDoS攻击最主要动因是金钱

对于大部分DDoS攻击团伙来说，发起DDoS攻击的最主要动因是金钱。他们为了巨额佣金对企业发起DDoS攻击，帮企业的竞争对手抢夺市场和用户，单次攻击发起的成本在数百元至上万元不等。另一部分团伙则对企业敲诈勒索，以获得丰厚的赎金，上半年部分团伙单次勒索的赎金甚至高达数个BTC，折合人民币数十万元。此外在游戏行业还存在一种痼疾，部分恶意玩家为了作弊也会对游戏企业发起攻击。综合下来，企业之间恶意竞争、游戏行业恶意玩家作弊、敲诈勒索是DDoS攻击的主要动机。

攻击目的分析

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

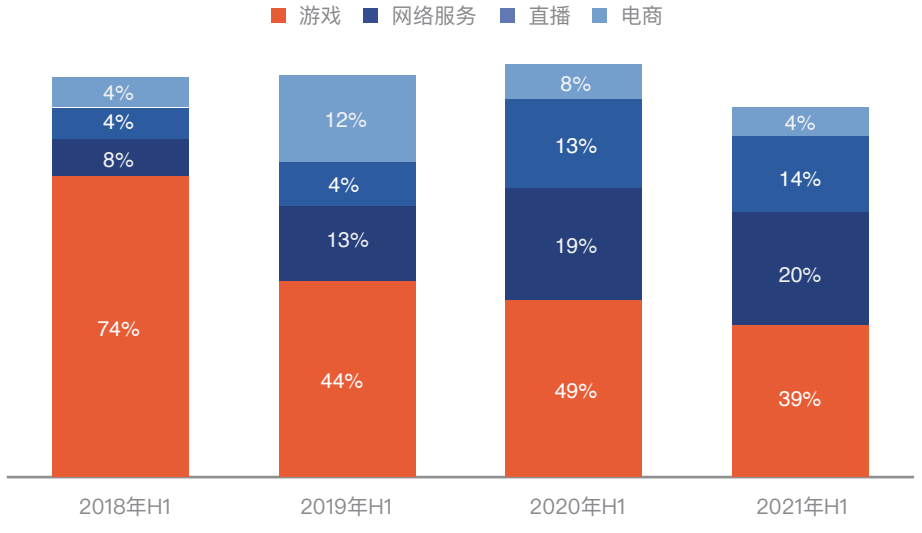


4.14 游戏行业连续多年成DDoS攻击最多行业

由于在线教育、在线医疗、在线会议等新兴产业的兴起，网络服务行业的占比持续增加。而直播行业由于搭上了“卖货”的快车，近年的攻击占比也在持续增加。新兴行业DDoS攻击比例增加，游戏行业攻击占比虽持续多年居首，但比例持续降低。

DDoS攻击的行业分布

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）

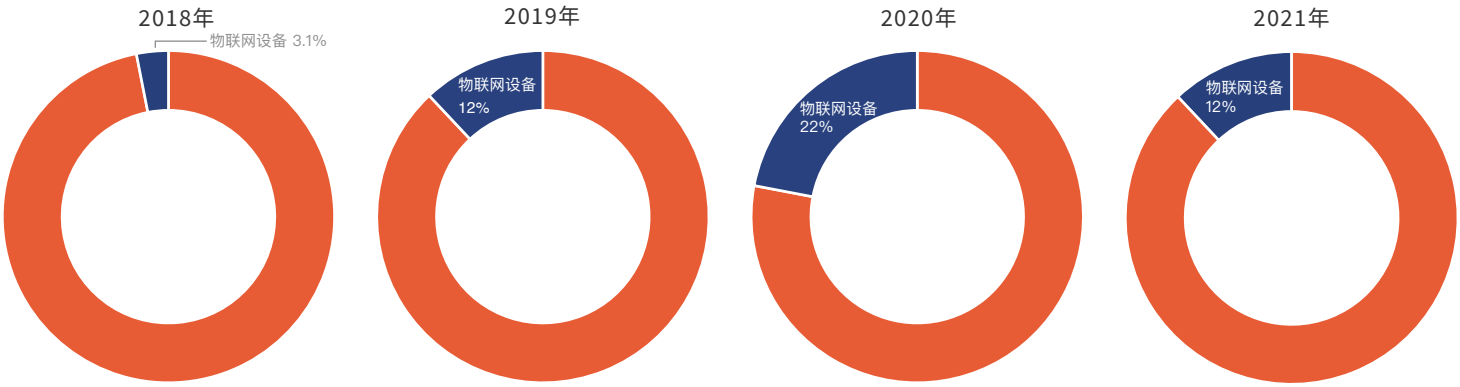


4.15 长期活跃攻击资源中的物联网设备占比

2021年上半年，攻击资源中物联网设备的数量基本平稳。由于攻击资源总量增长，导致物联网设备占比下降，侧面反映物联网设备的相关治理已收到一定成效。

长期活跃攻击源中的物联网设备占比

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁

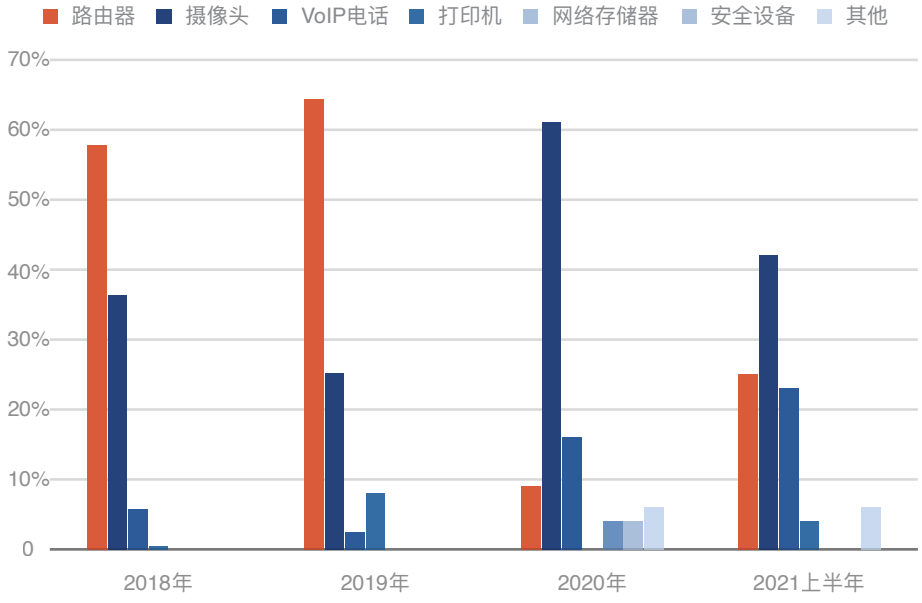


*注：根据攻击源IP 的活跃持续时间分布，活跃时间达十天以上的攻击源，我们视为高活跃度攻击资源。这些资源一般存在明显的安全隐患极易被利用，威胁程度较高。

4.16 参与DDoS攻击的物联网设备类型分布

长期被操控的团伙攻击资源主要是IDC和物联网设备。统计团伙所有攻击资源类型，占比最高的为物联网设备，达 31%。其中，摄像头占比15% ，路由器设备占比12%，网络电话占比 3% 。

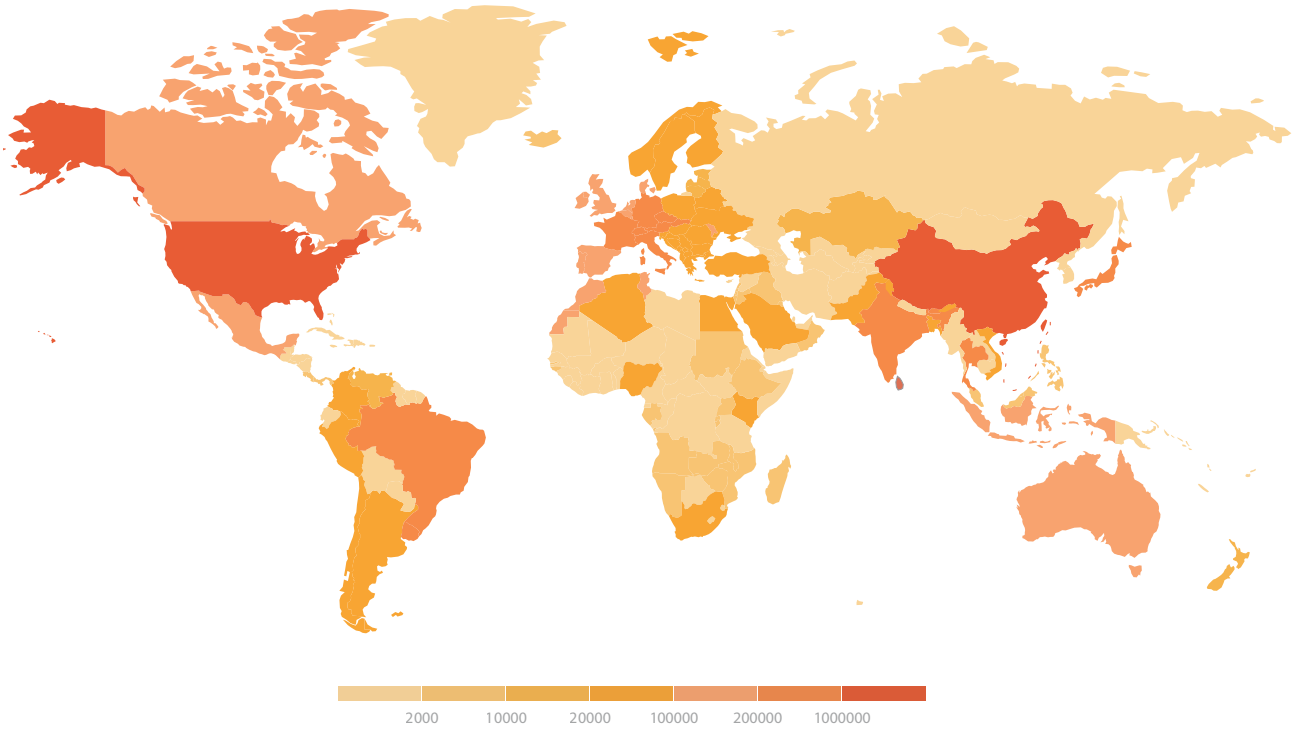
（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报

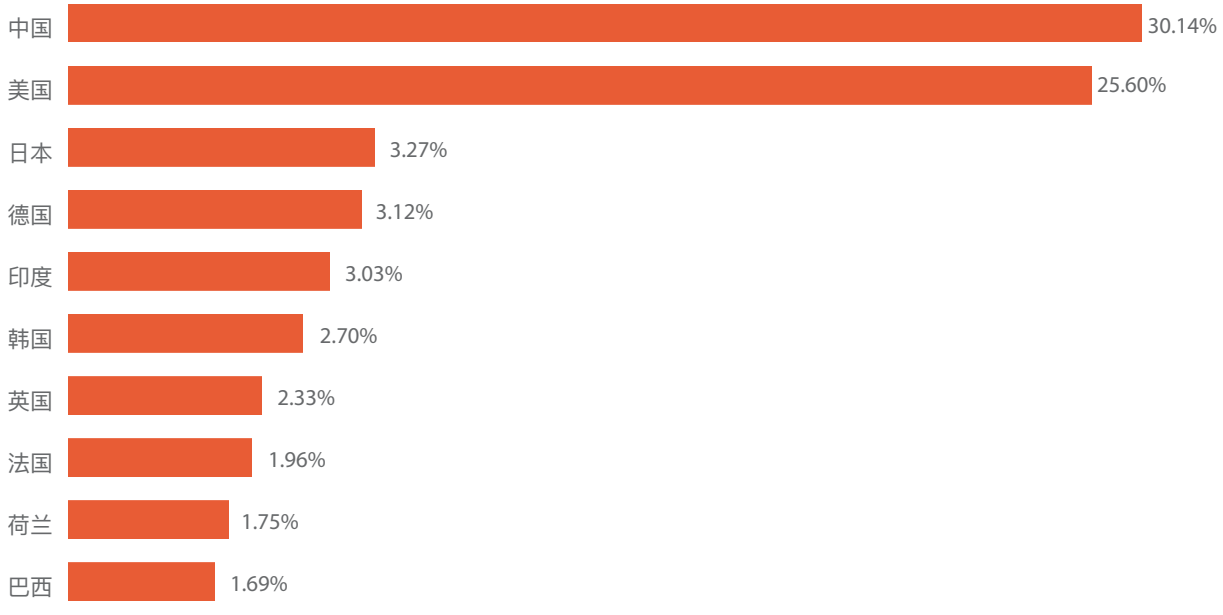


4.17 活跃攻击资源地域分布

从全球分布来看，高活跃度攻击源主要分布在中国、美国和日本。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。

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告





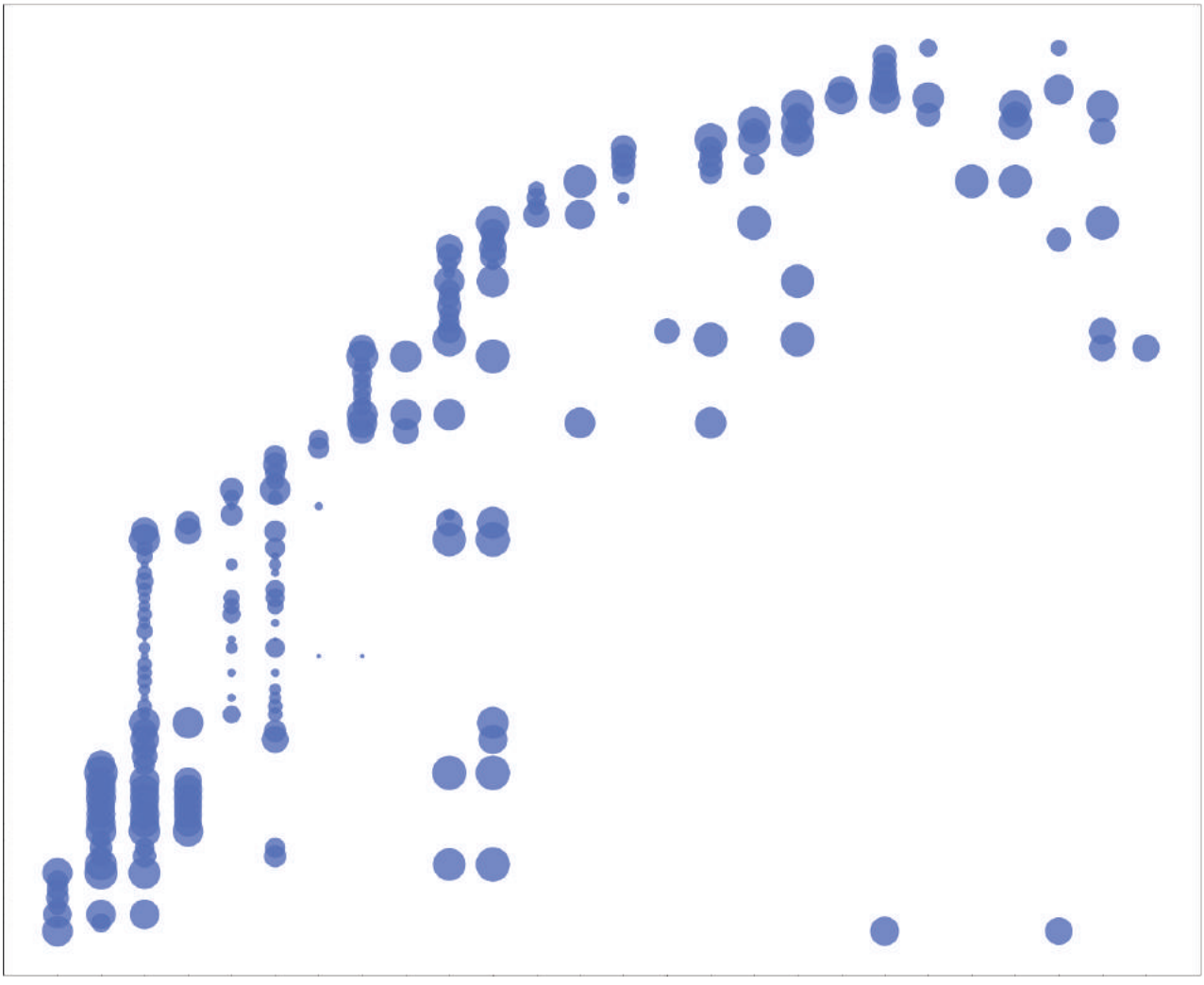
4.18 攻击资源团伙行为分析

团伙攻击是指通过相对独占的攻击资源、基于一定的攻击手法进行规模化攻击的行为。与其他大量由个体发起的普通攻击事件不同，团伙攻击行为往往带有典型的情报、经济等利益目标。因此形成基于网络数据的攻击团伙行为视角，掌握数据中的主要虚拟攻击团伙具有重要意义。

据统计，DG1团伙在5月份最为活跃，活跃惯犯数量为2.7万。

如下图所示，横坐标是日期（以天为粒度），纵坐标是攻击目标IP，蓝点表示该团伙在某天攻击了某IP，蓝点的大小表示攻击源IP数量。蓝点越大越多，则表示该团伙性行为的DDoS攻击越频繁、团伙活跃度越高。5月17日为攻击次数最多一天，同时有1.13万个攻击源对同一目标发起攻击。

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报



DG1团伙1-6月活跃状况

*注：DG1团伙系DDoS团伙，近年持续活跃，主要使用SYN洪水攻击。攻击源主要集合在西欧地区，涉及到荷兰、德国、波兰等，攻击源活跃数量稳定。攻击目标集中在中国香港。攻击事件数量为平均817/天。

4.19 DDoS僵尸网络

在2021年上半年的DDoS僵尸网络活动中，监控到的攻击指令逾63万条，主要来自Xor.DDoS、Dofloo、Mirai和Gafgyt等7个家族，并由Mirai产生了最多的攻击事件，其占比超过了70%。

上半年检测到的DDoS攻击手段以SYNFLOOD、CC、ACKLOOD和UDPFLOOD为主，其中SYNLOOD和CC各自占比约为36%。

上半年检测到的C&C有近40%位于美国。所有的已知云服务商/运营商为169个，其中位列前三的分别是ColorCrossing（占比17%）、OVH和Digital Ocean。

上半年检测到的IoT DDoS木马传播利用的各类漏洞种类为60种。
在使用数量上位居前三的漏洞为：

- CVE-2017-17215（华为HG532路由器）
- CVE-2014-8361（Realtek SDK miniigd SOAP服务远程代码执行）
- CVE-2018-10561（GPON光纤路由器漏洞）。

其中，2021年新增漏洞为：

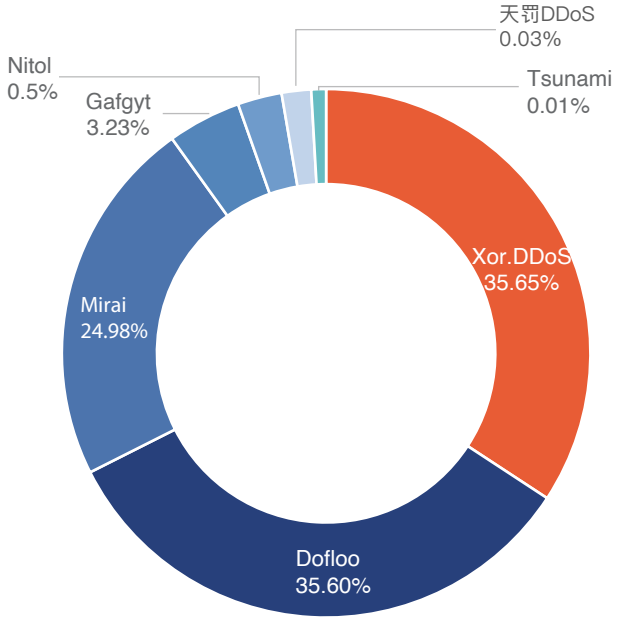
- CVE-2021-27561（Yealink设备管理平台未授权远程代码执行）
- CVE-2021-22502（Micro Focus监控软件远程代码执行）
- CVE-2021-22986（F5 BIG-IP 链路控制器远程代码执行）

1. DDoS攻击事件及家族分布

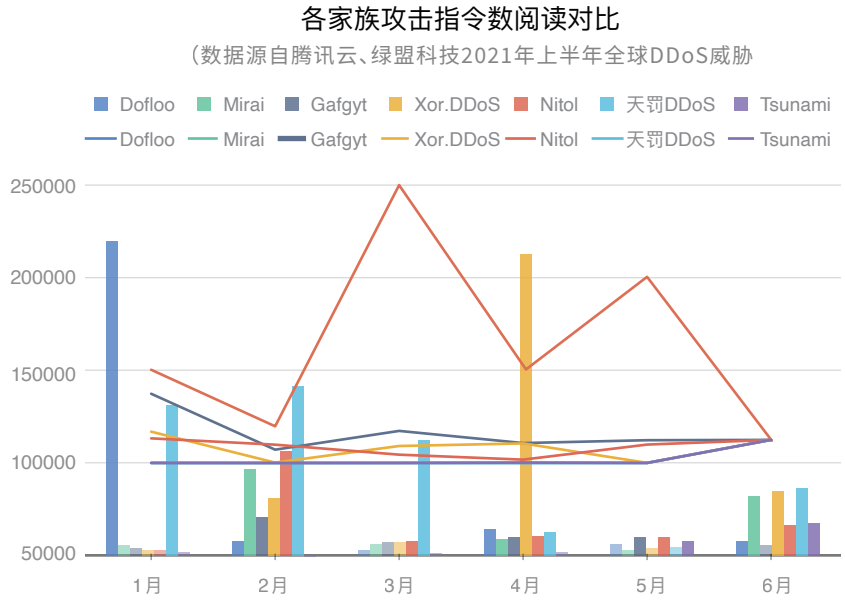
2021上半年检测到DDoS攻击指令逾63万条，其中包含的攻击事件数为75,141，共来自7个家族，其攻击比重如下：

僵尸网络攻击指令与家族分布

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报



1-5月各家族攻击指令和攻击事件数对比如下。



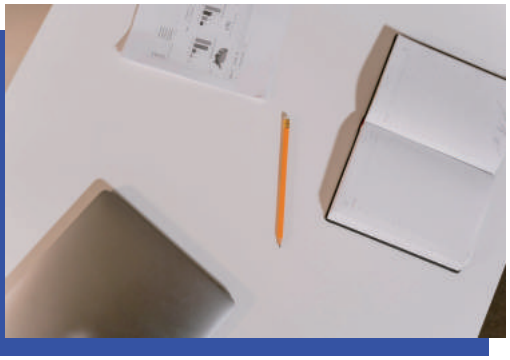
2. DDoS攻击事件及家族变种构成

各家族变种在攻击事件中的比例如下：

家族	变种	比例
Mirai	mirai（各变种流量在此统一）	72.12%
Xor.DDoS	DDOS.XORDDOS.S0P0R0.LV	9.38%
	xorddos	7.78%
Gafgyt	gafgyt_left	9.05%
	gafgyt_demon	0.01%
	gafgyt_rebirth	<0.01%
Nitol	DDOS.NITOL.S0P0R0.WO	0.97%
	DDOS.NITOL.S1P0R3.WV	0.63%
	DDOS.NITOL.S0P0R15.WV	0.01%
	DDOS.NITOL.S0P3R7.WV	<0.00%
	servstart	<0.00%
Tsunami	DDOS.TSUNAMI.S0P0R1.IV	0.02%
天罚DDoS	DDOS.TF.S0P0R0.LO	0.01%
Dofloo	DDOS.DOFLOO.S0P0R0.LO	0.01%

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告

05
攻防对抗案例



案例一

2021年春节前后腾讯云某游戏行业客户旗下的多款热门游戏被黑产团伙发起“打卡式”的针对性攻击，一个月内累计攻击数千次，多次攻击流量峰值接近500G。

攻击特征

1. 攻击原因为游戏行业的痼疾

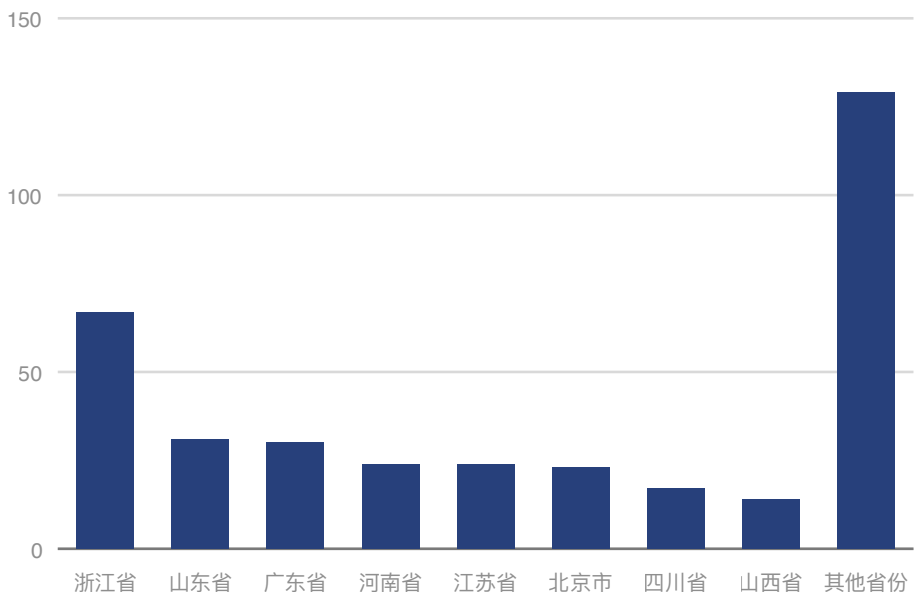
行业内竞争对手出于不正当竞争的目的，雇佣黑产团伙发起攻击。

2. 攻击团伙技术实力强

选择的攻击手法都是现网防护难度大的手法（TCP反射、TCP四层CC攻击、HTTP CC攻击），甚至利用客户的业务瓶颈，通过遍布全国的海量肉鸡发起低频小流量的攻击来绕过防护，引发客户服务器崩溃。肉鸡IP分布全国各地，没有明显集聚，且肉鸡IP不断轮换，使得传统的黑名单或区域封禁等策略无效。

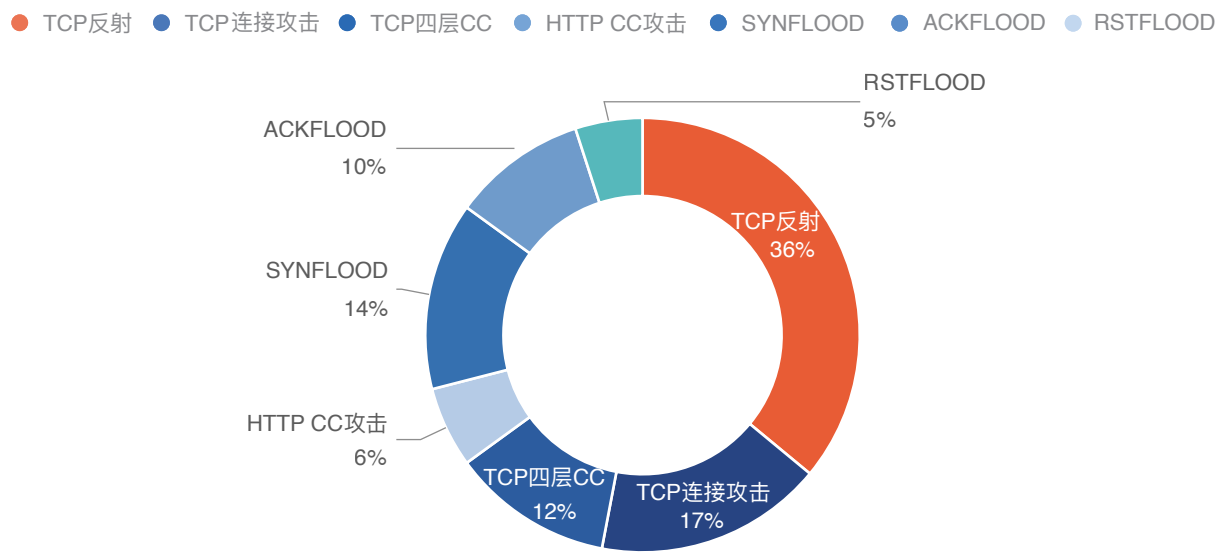
国内攻击源来源省份分布

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）



攻击手法分布

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）



3. 攻击流量大

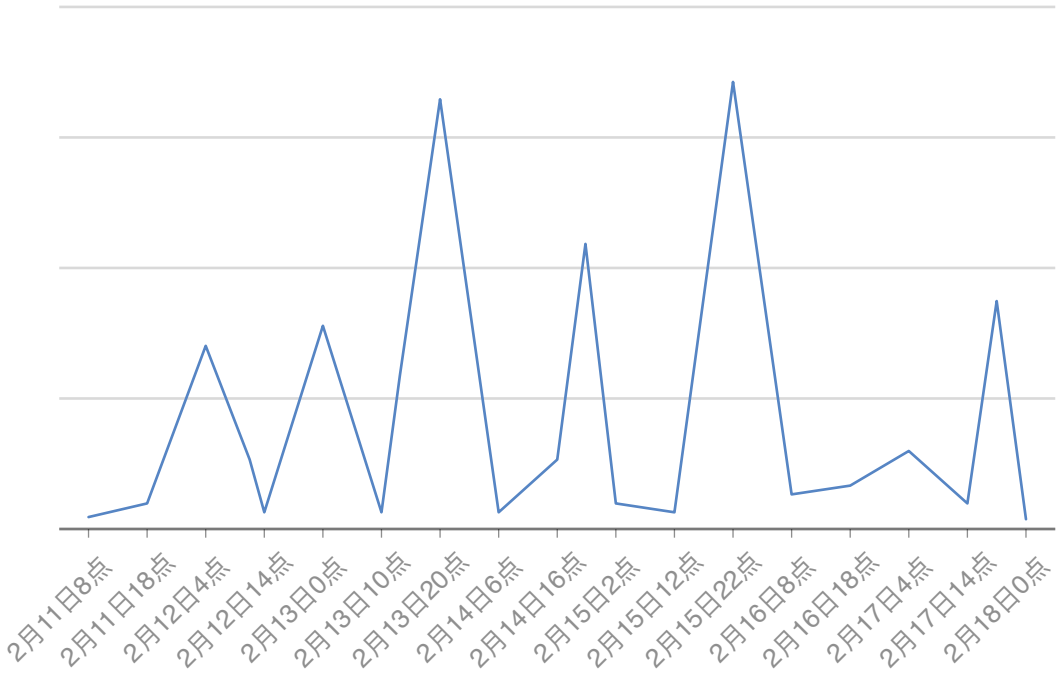
100G以上的大流量攻击占比24%，多日攻击流量峰值均接近500G。

4. 打卡式攻击

春节长假每一天都有数百次攻击，黑产团伙精心选择业务高峰时段（晚19:00-23:30），对客户的热门游戏一个不落地进行“打卡式”攻击。

春节长假期间攻击次数走势

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）



对抗难点

1. 腾讯云T-SecDDoS团队率先监测到TCP反射手法的威胁，并研发出独有的TCP反射防护算法，无需人工干预、在玩家无感知的前提下精确区分攻击流量和正常流量，实现自动化、智能化清洗。

2. 大数据+深度学习AI防护，腾讯云T-Sec DDoS系统根据深度学习模型的判断结果进行统计分析，有效识别识别和清洗TCP四层CC攻击流量和TCP连接攻击流量。

3. 通过先进的流量指纹防护算法，依据流量来源的OS指纹、程序指纹、设备指纹对肉鸡和正常玩家进行精准区分，实现对低频TCP连接攻击的降维打击。

案例二

2021年5月下旬开始，腾讯云某游戏行业客户旗下热门游戏遭受多次攻击，攻防对抗除了常见的SYNFLOOD、UDP反射放大攻击、TCP非法标志位攻击外，TCP、UDP、ICMP之外的其他非常见IP协议也被用于攻击之中。在攻防对抗进一步升级后，黑客针对性分析客户的网络协议，针对性地模拟业务流量构造攻击包发起攻击，甚至对客户的专线网段发起扫段攻击。

攻击特征

1. 攻击手法多变

黑客使用了多达10种以上的攻击手法。除了常规的SYN大包、SYN小包、UDP大包攻击、UDP反射放大攻击、TCP非法标志位攻击、ACK-FLOOD、RST-FLOOD外，TCP、UDP、ICMP之外的其他非常见IP协议也被用于攻击之中，甚至7秒内完成针对客户专线网段250个IP的扫段攻击。

2. 团伙技术实力强

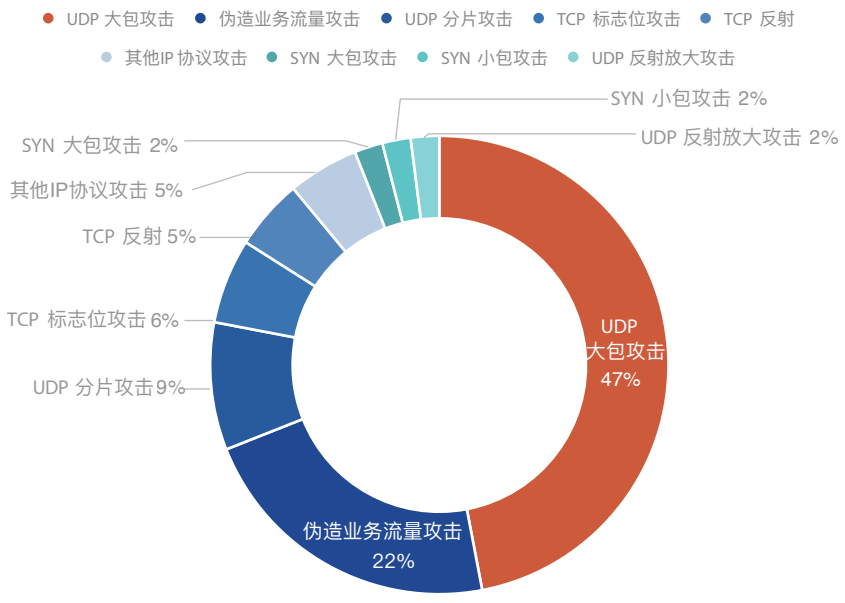
在攻防对抗进一步升级后，黑客针对性分析客户的网络协议，动用大量肉鸡模拟业务流量构造攻击包发起攻击，攻击包可以绕过客户自身的校验算法，出现敌我难分的局面。

3. 攻击团伙的攻击资源非常丰富

攻击团伙控制的肉鸡数量非常庞大，且相当部分肉鸡位于国外，在未使用反射放大攻击的情况下，UDP大包攻击的攻击流量就已近600Gbps。

攻击手法分布

（数据源自腾讯云、绿盟科技2021年上半年全球DDoS威胁报告）



4. 攻击团伙技术能力强大

和大部分攻击团伙租用第三方攻击工具或者调用攻击站点发起攻击流量不同，黑客团伙对攻击资源完全掌控，可以迅速更新攻击手法，可以按需对每一台肉鸡定制攻击载荷，可以针对性分析客户的网络协议，模拟业务流量构造攻击包，构造的攻击包甚至可以绕过客户自身的网络协议包校验算法。

对抗难点

1. 客户专线带宽有限却由多个业务共享，少量透传以及扫段攻击期间在加保护瞬间的少量透传都很容易造成专线不可用，给防护方提出了更高的要求。腾讯云T-Sec团队通过定制化的常态化防护、精细化防护策略，进一步减少上述场景的透传，确保用户专线网络的可用性。

2. 部分UDPFLOOD攻击的攻击载荷复杂多变，静态特征算法很容易被绕过，人工介入处理难以跟上攻击者的节奏。腾讯云T-Sec系统的自适应启发式算法，可以动态提取攻击特征并自动进行防护。

3. 针对模拟业务流量构造攻击包发起攻击，攻击包可以绕过客户自身的校验算法，引导用户接入腾讯云T-Sec侧自主研发且已经在多个客户得到成功应用的安全水印算法。

案例三

2021年3月，绿盟科技某国际运营商客户业务遭受持续攻击，其中TCP反射攻击成为攻击的主要方法。

目前传统的防御方法主要是通过规则封禁源端口为0-1024、目的端口为0-1024的TCP报文，或者根据抓包封禁TCP反射的源端口。但由于互联网上开放的服务端口越来越多，这种通过静态规则的方法往往无法适应攻击的变化，防护效果不够理想。

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。

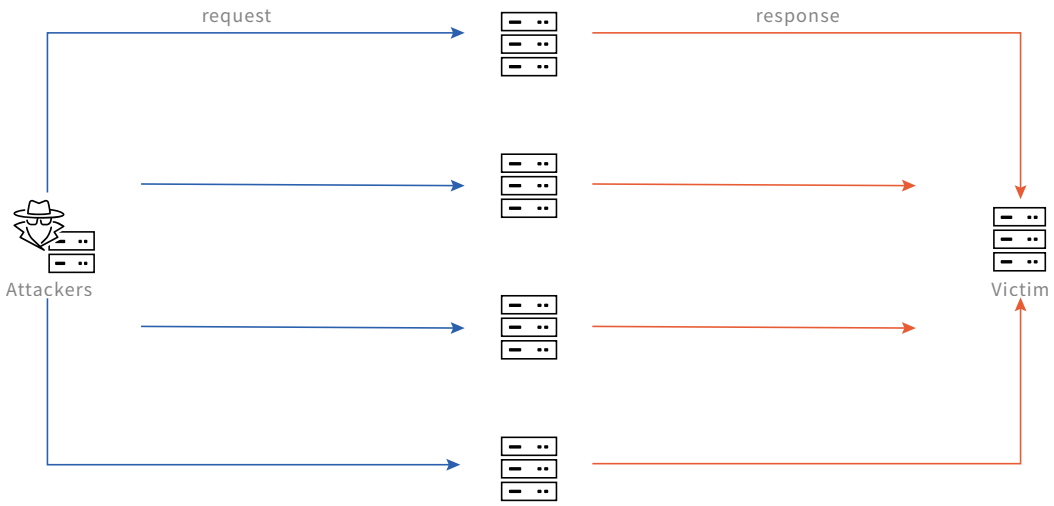
绿盟科技基于对各种反射器的深入研究和不断的攻防实践，提炼了一套融合了动态识别、行为分析等的多维度综合算法，并在客户遭遇攻击期间迅速上线，有效的防御了TCP反射攻击。

攻击特征

1. 攻击者通过伪造源IP地址（设置为受害者IP地址），向大量公网服务器发送请求报文。

2. 公网服务器则会将响应报文回复给伪造的IP地址（受害者IP地址）。

3. 由于公网服务器数量众多，导致大流量集中涌向受害者，造成DDoS攻击。



根据绿盟科技数据，2020 年反射源数量占所有攻击源的14%，其中大部分反射源为IoT 设备。

对抗难点

通常，攻击者会选择UDP协议作为载体发起反射攻击。原因很简单，基于UDP的反射攻击可以达到数倍的放大的效果。Memcache反射攻击的甚至能实现超过5万倍的放大效果。以小博大，简单粗暴。而对于TCP协议来说，尽管很难达到UDP的放大效果，但是却有一项关键“优势”——难防。

1. TCP反射形成的攻击流具有一定的协议栈行为，比传统使用攻击工具无脑发起的攻击迷惑性更强、更难防御。

2. TCP反射攻击的攻击报文有SYNACK、ACK和少量RST几种，与正常通信流程的报文构成类似，难以区分。

3. 由于网络中的服务器种类和配置等多种多样，导致最终形成的反射攻击流情况较多、更加复杂。

06 DDoS大事记

1. 2021年1月，国外黑客团伙利用DDoS攻击大肆发起敲诈勒索活动。全球DDoS攻击活动大幅增加，敲诈勒索金额大幅提升，单次勒索数额甚至高达10枚BTC，折合人民币超过200万元。

2. 2021年1月，由于大幅增加的DDoS攻击活动推升了对攻击资源的需求，包括腾讯云在内的多家厂商观测到黑客将OpenVPN、DTLS、MS-RDP、TeamSpeak 3、PlexMedia等UDP协议应用到DDoS反射放大攻击，腾讯云上观测到基于这些协议的DDoS攻击次数也有大幅增加。

3. 2021年1月13日，马耳他最大的互联网服务供应商Melita经历了公司有史以来规模最为庞大的DDoS攻击，本次攻击属于勒索性质，犯罪分子试图通过DDoS攻击影响其服务的正常运转，以索取巨额的赎金。尽管Melita在 To B业务上提供DDoS的防护服务，但在本次攻击中Melita却依然没有避免大范围服务停运的结果。

4. 同样在2021年1月，某亚太区域大型电信运营商也曾收到过DDoS攻击的勒索信，但从绿盟科技实际监控来看，并未真正实施DDoS攻击，勒索者通过模仿流行的攻击团伙名称进行冒名威胁。从中也可以看出，DDoS攻击给企业带来的损失和影响之大，才能造成假勒索如此猖狂局面。

5. 2021年2月春节期间，包括腾讯云在内的多家厂商监控到DDoS攻击活动同比往年大幅增加。根据腾讯云T-Sec DDoS团队的监控数据，春节长假期间，腾讯云上的DDoS攻击次数约为去年同期的2.5倍。

6. 2021年5月，一场DDoS攻击狂潮席卷比利时，攻击针对比利时的运营商Belnet（该运营商受政府资助，主要为比利时国内的政务站点和教育科研机构服务），超过200个政务部门和教育机构与互联网的连接被迫断开，公众一度无法访问这些站点。

7. 2021年5月，Avaddon勒索软件组织针对墨西哥国家彩票公司和保险巨头安盛（AXA）的攻击表明：DDoS攻击也成为部分数据加密勒索犯罪组织的有力武器，勒索软件攻击目前已经演变为综合了加密、数据窃取和DDoS攻击的三重威胁。

以往这类犯罪组织首先会将受害者的数据进行加密导致数据无法使用。之后这些团伙会威胁将受害者的机密数据公开，以便向受害者施压，让他们及时支付赎金。但是5月底Avaddon勒索软件在对墨西哥国家彩票公司以及安盛（AXA）实施了数据加密/数据窃取之后，声称如果谈判在240小时内没有开始，将公布更多的文件，并将对受害者的网站发起DDoS攻击。

8. 疫情持续蔓延，极大地影响了各国人民的日常生活。很多国家医疗机构始终保持着超负荷运转，以应对疫情的冲击，而很多教育机构则被迫停课，通过互联网进行远程授课和线上学习。但部分医疗和教育机构在对互联网高度依赖的同时，却在安全方面准备不足，从而使DDoS攻击成为这些站点的阿喀琉斯之踵。

2021年2月份Winthrop公立大学遭受了严重的DDoS攻击，尽管负责人公开表示没有任何学生、雇员、以及财务数据遭受损害，但是远程授课服务将在很长一段时间内受影响，校方尝试建立临时的互联网平台以满足学生的需要。在美国加利福尼亚州，一非盈利综合医疗机构Scripps Health自2021年5月1日起，开始遭受勒索者长达两周的DDoS攻击。此次攻击导致该机构的电子病历系统遭受损害，用户也无法进行正常的预约、咨询和查询处方等操作。

Scripps Health是美国加利福尼亚州的一个非盈利综合医疗机构，排名全国第十五名，雇员超过15000人。自2021年5月1日起，该机构开始遭受勒索者长达两周的DDoS攻击。在此期间，官方网站页面仅能显示“Scripps.org will be back soon.”及紧急联系电话等信息。此次攻击导致该机构的电子病历系统遭受损害，并且攻击者还关闭了旗下的“My Scripps”智能手机APP，使用户无法进行正常的预约、咨询和查询处方等操作。

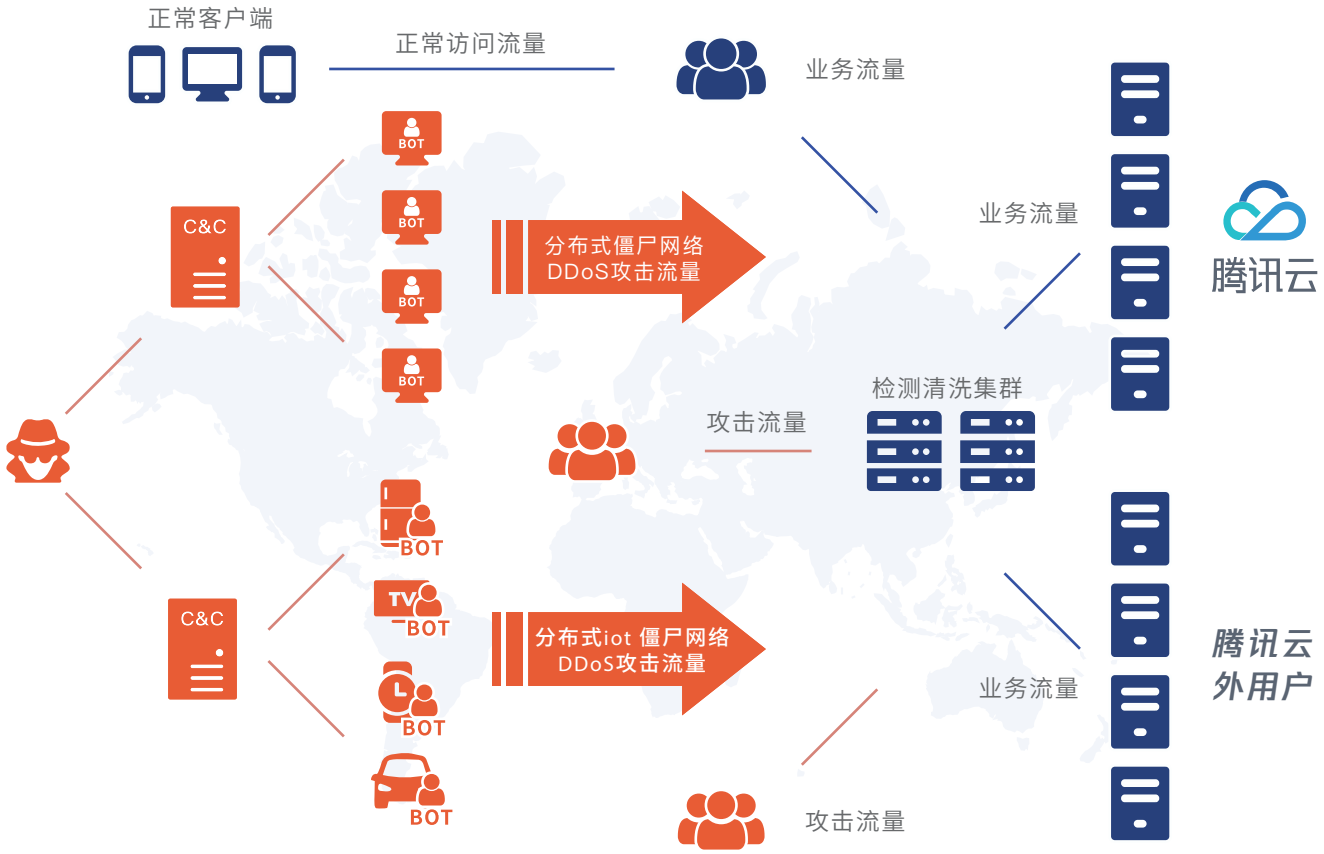
07 产品介绍

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。



腾讯安全
Tencent Security

腾讯云DDoS防护

绿盟科技国际业务