腾讯云·DDoS防护T-Sec
DDoS威胁报告

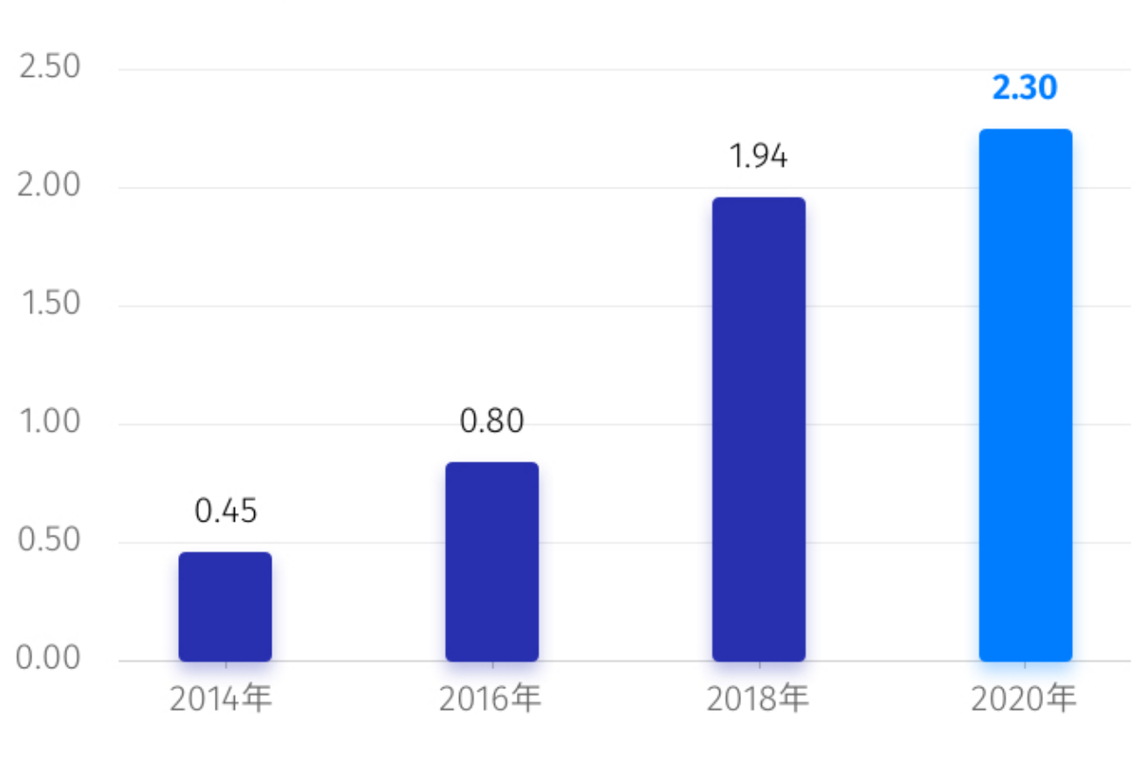
2020年上半年

2020年，新冠疫情在全球肆虐，越来越多的生产活动和社交娱乐从线下转移到线上。很早就习惯网赚的黑客，不仅把最大DDoS攻击记录推升到2.3T，还创造了45%的DDoS攻击次数增幅，其中100G以上的超大流量攻击数量甚至翻番。黑客们的攻击资源从何而来，攻击手法是否有新增？游戏行业是否还是黑客最钟情的目标？黑客的活动因疫情影响而产生了什么变化？腾讯安全DDoS防护T-Sec团队为您一一揭晓。

DDoS威胁态势

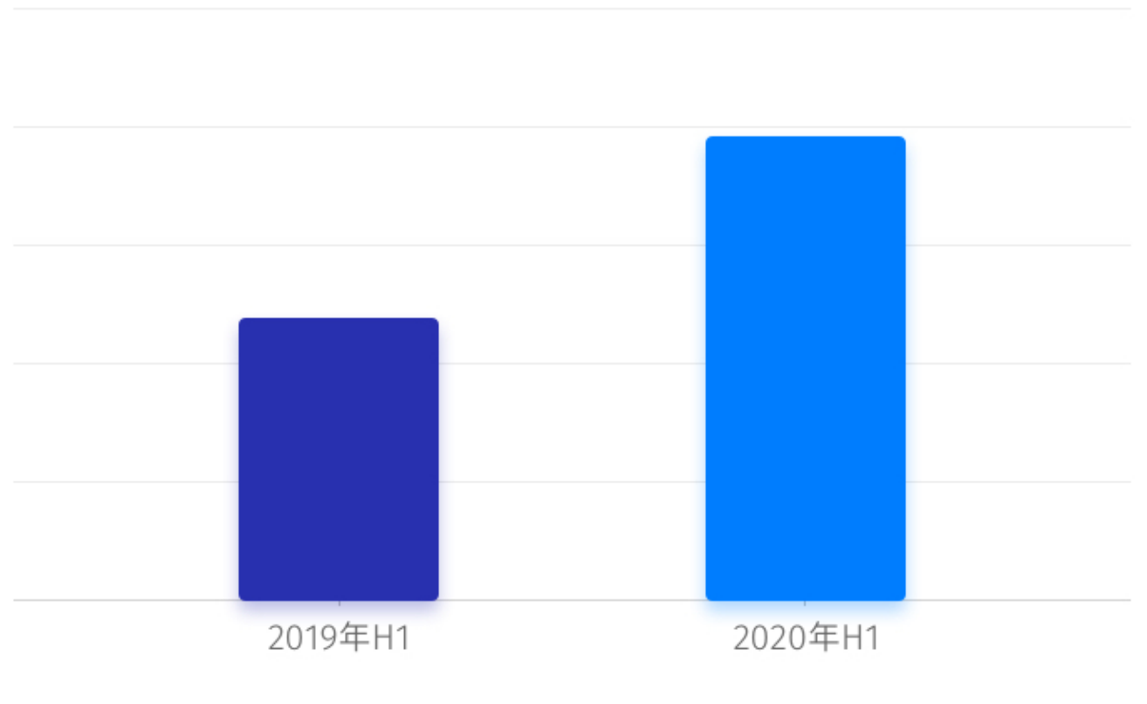
业界最大DDoS攻击峰值流量达到 2.3T

业界最大DDoS攻击流量走势



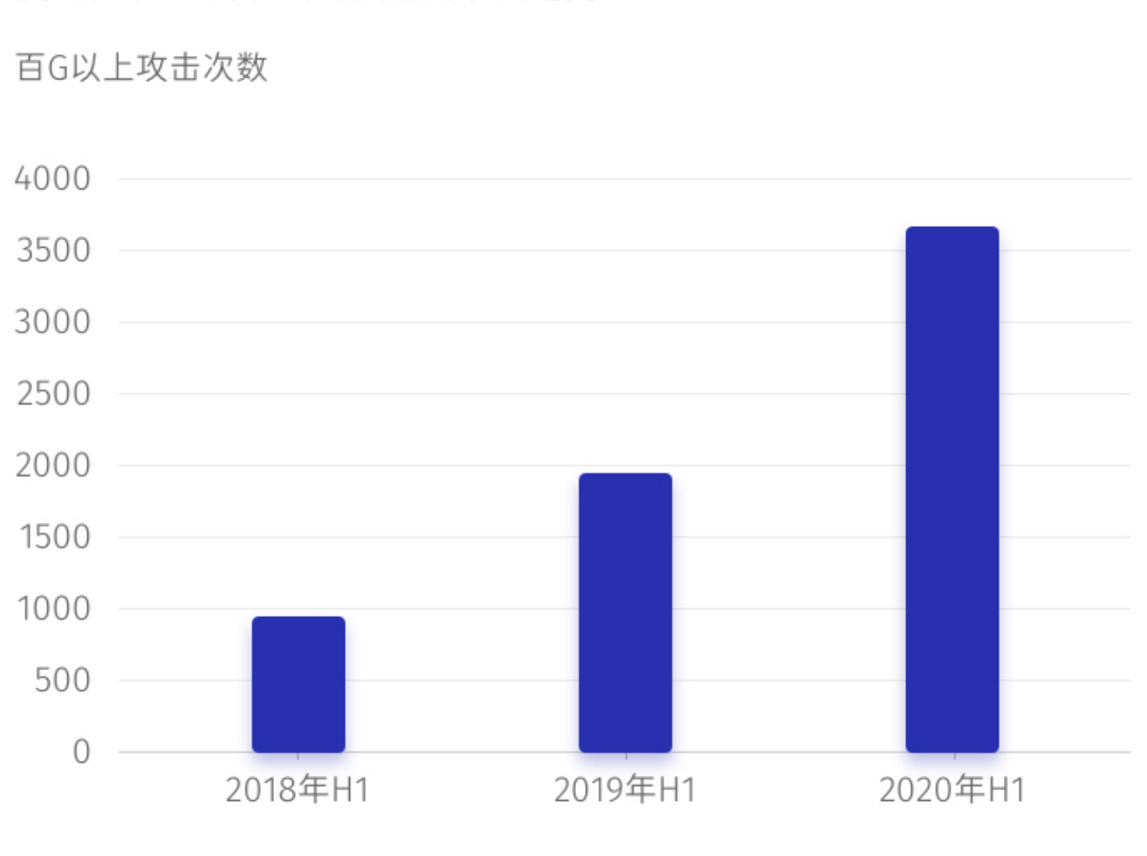
云上DDoS攻击次数大幅增长 45%

攻击次数



百G以上攻击次数同比 翻番

腾讯云百G以上大流量攻击走势



应用层攻击异军突起

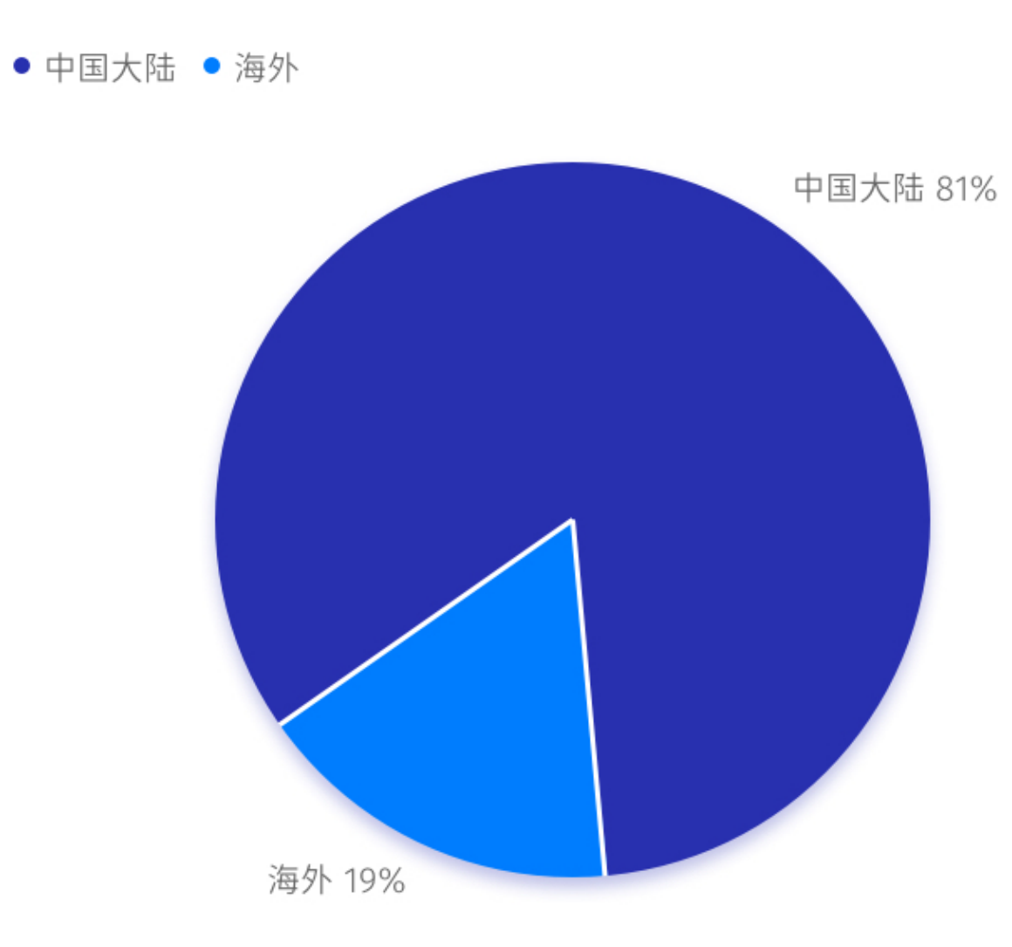
27天 持续时间最长达到	**831亿次** 单次攻击最大累计攻击请求
260万qps 峰值HTTPS请求量	**45万** 单次攻击最大肉鸡数量

游戏、网络服务、直播成黑客最爱

DDoS攻击次数的行业分布

出海企业占DDoS攻击次数的近2成

20年上半年海外攻击占比

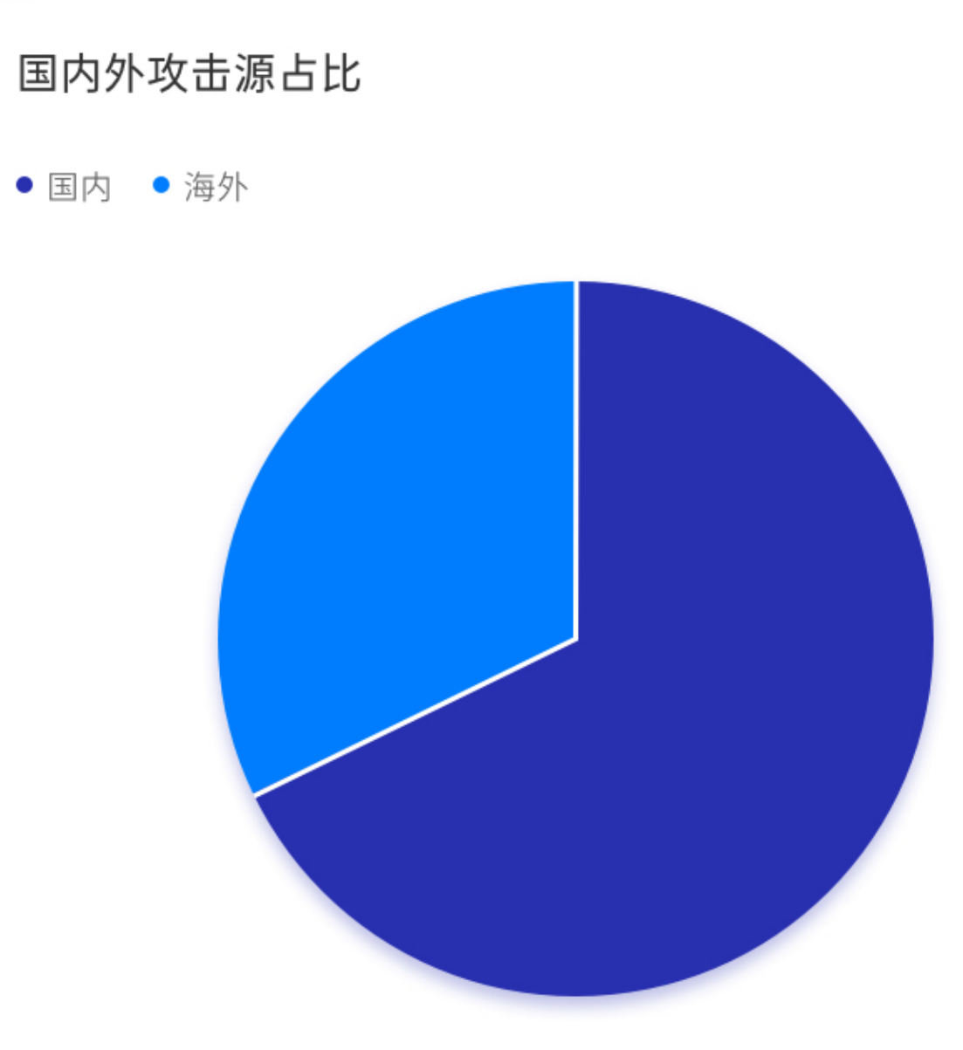


黑客攻击态势

黑客·攻击资源篇

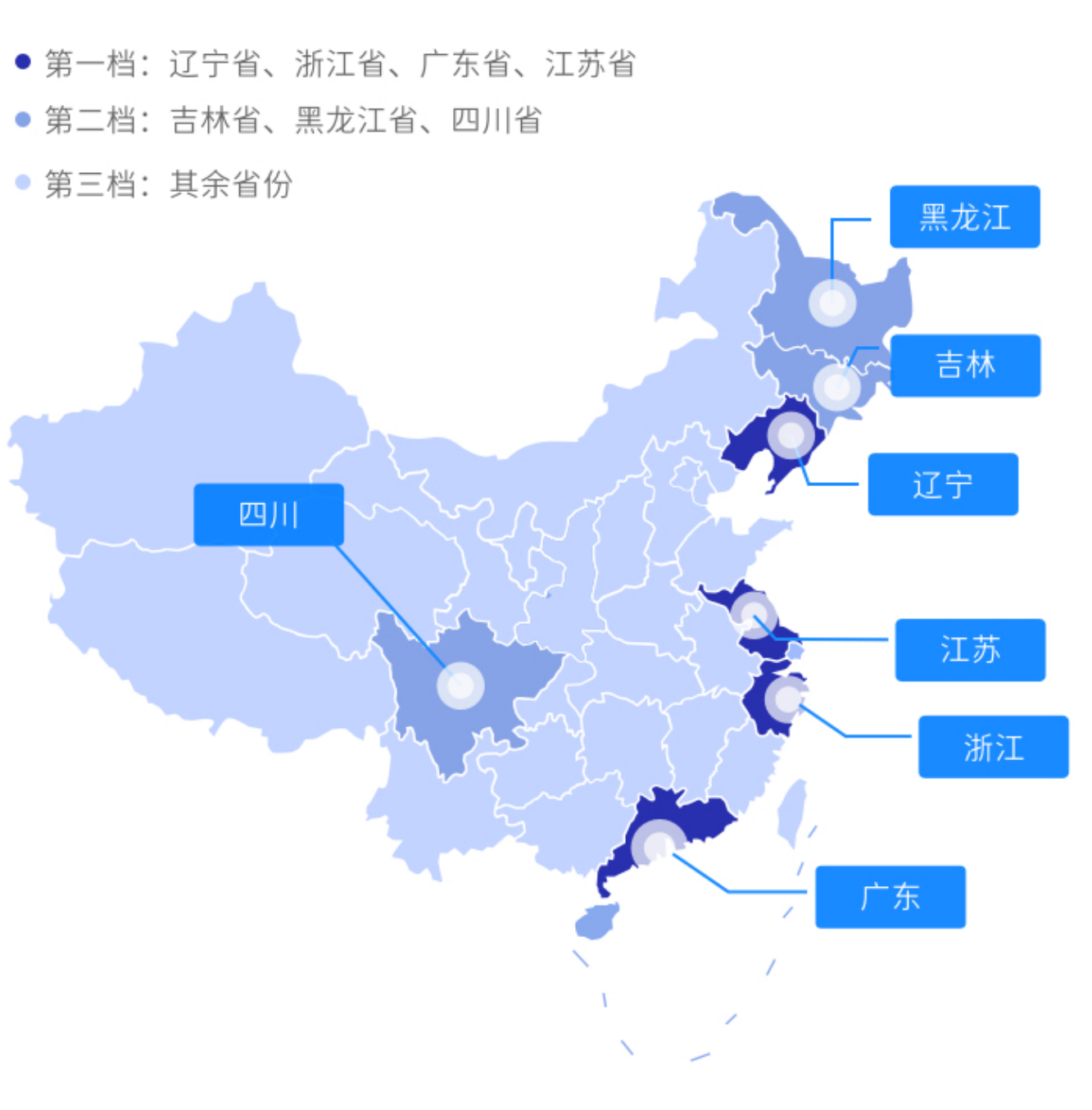
攻击资源主要来自国内

国内外攻击源占比



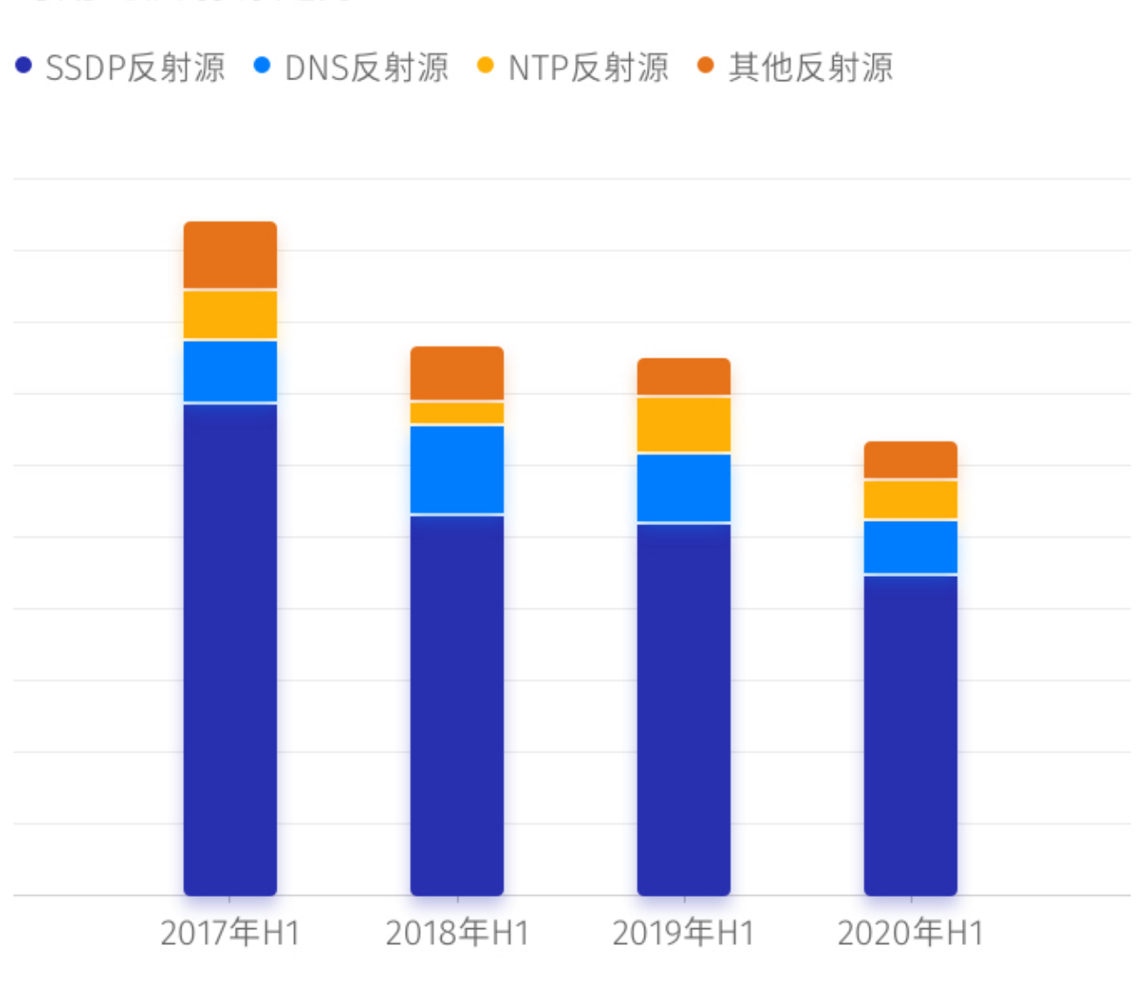
沿海发达省份和东北三省是主要来源地

国内DDoS攻击源的地域分布



可用的反射源数量呈下降趋势

可用的反射源走势



秒拨IP加入黑产大军对应用层防护带来挑战

1、传统的基于IP的策略难以防护

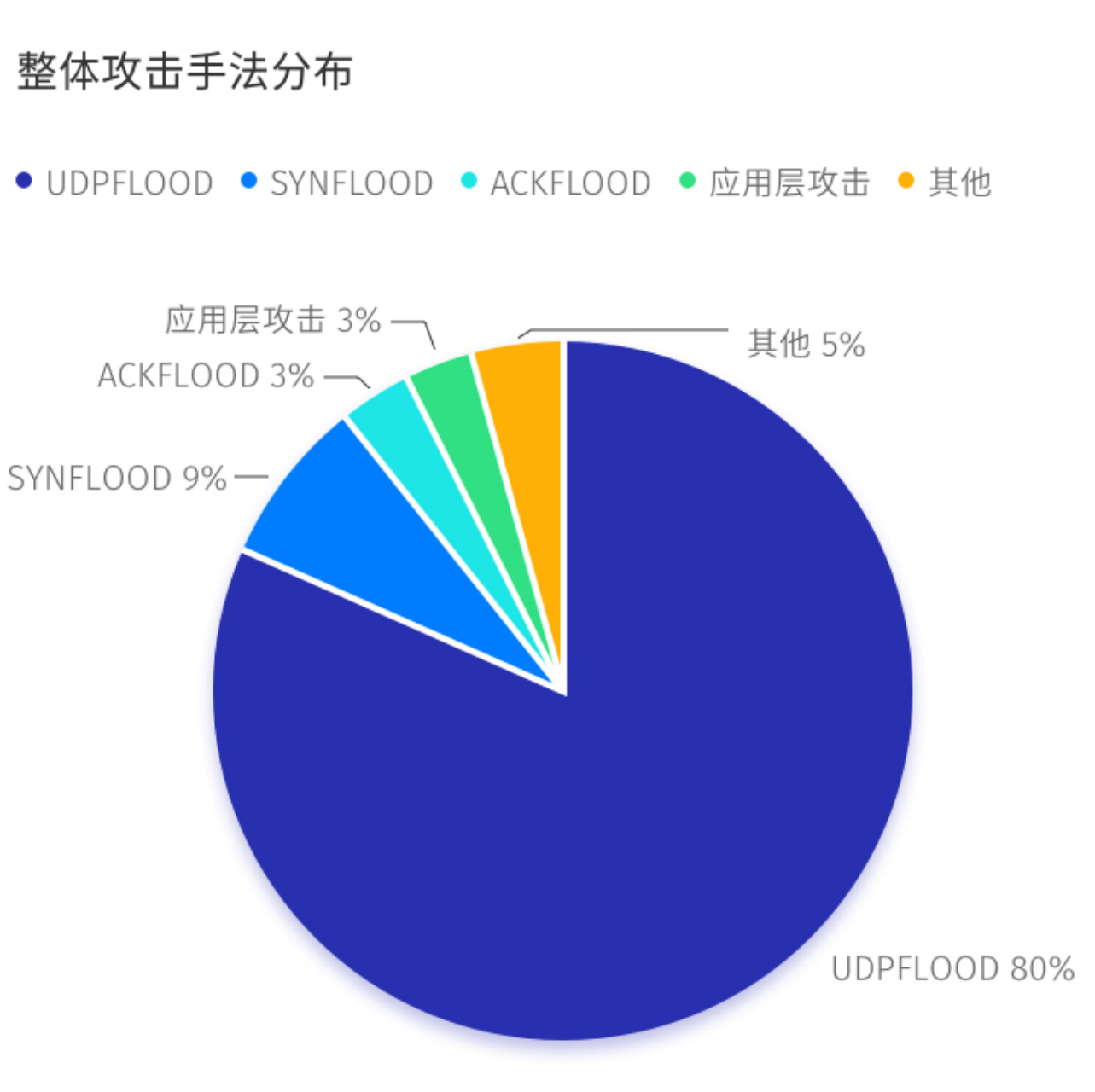
2、容易误伤正常用户

3、溯源更为艰难

黑客·攻击手法篇

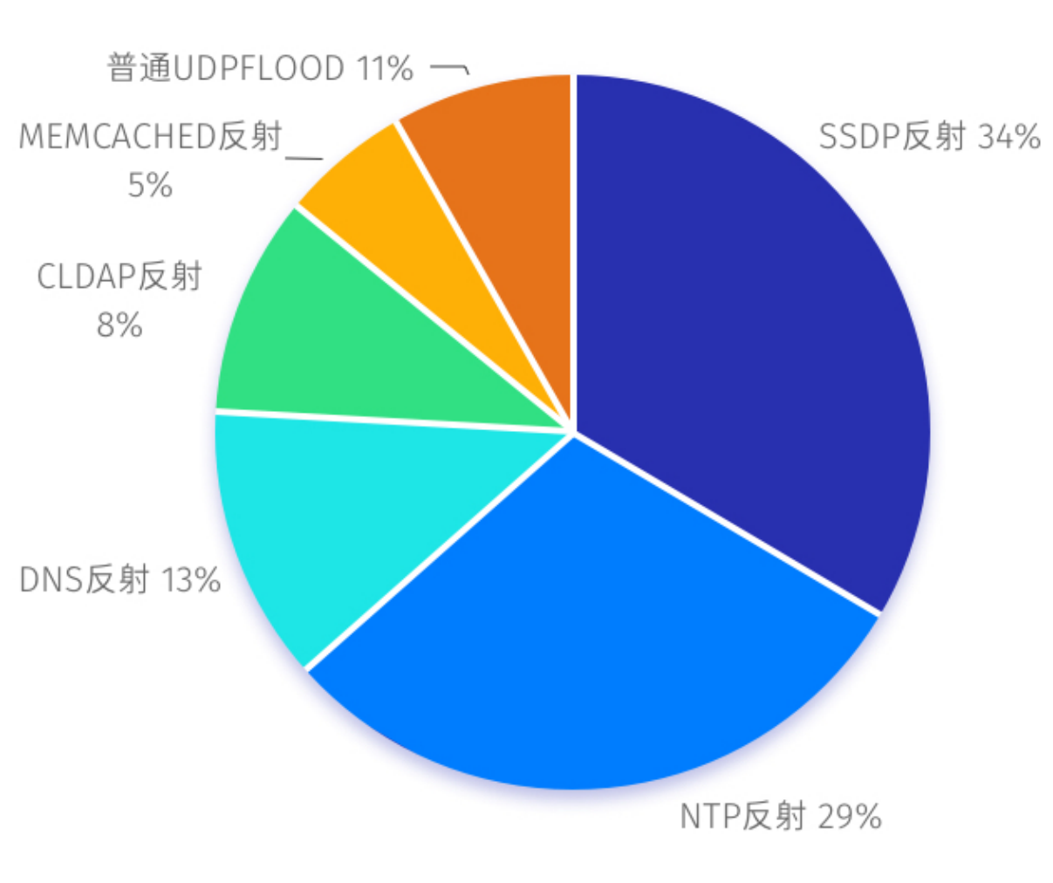
UDPFLOOD仍是主要手法，占比超过8成

整体攻击手法分布



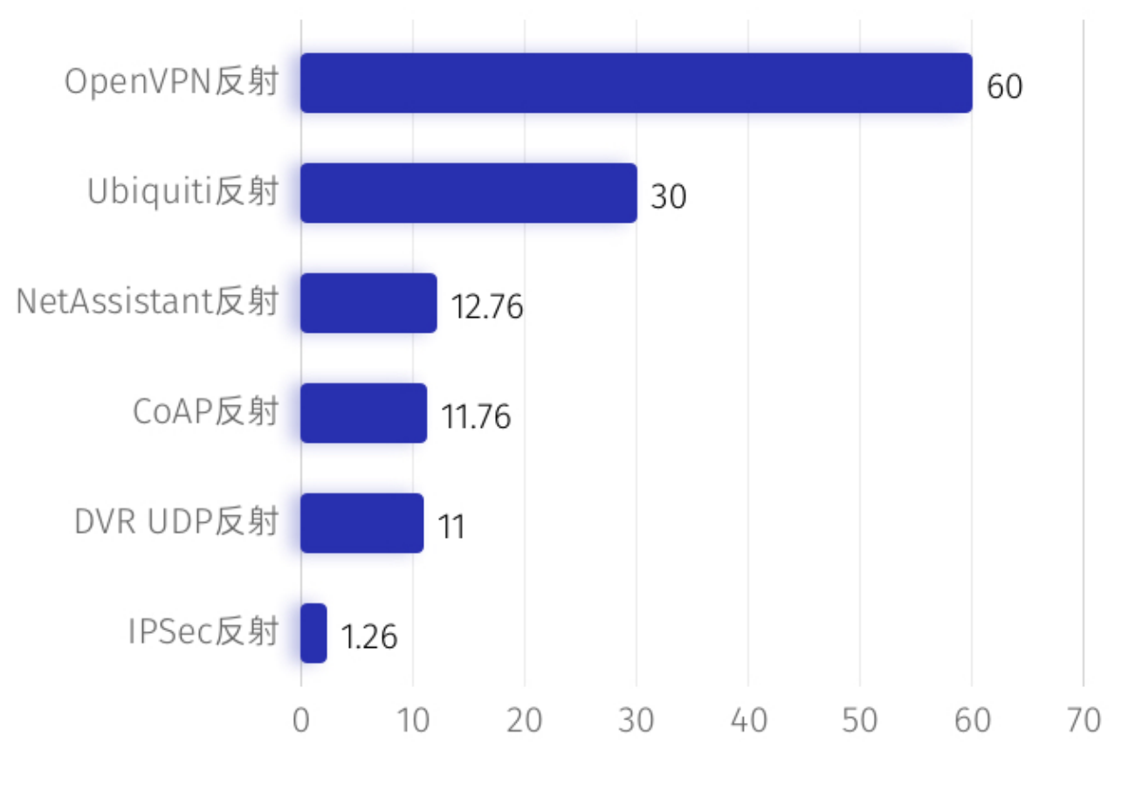
SSDP反射和NTP反射最受攻击者欢迎

UDPFLOOD的类型细分



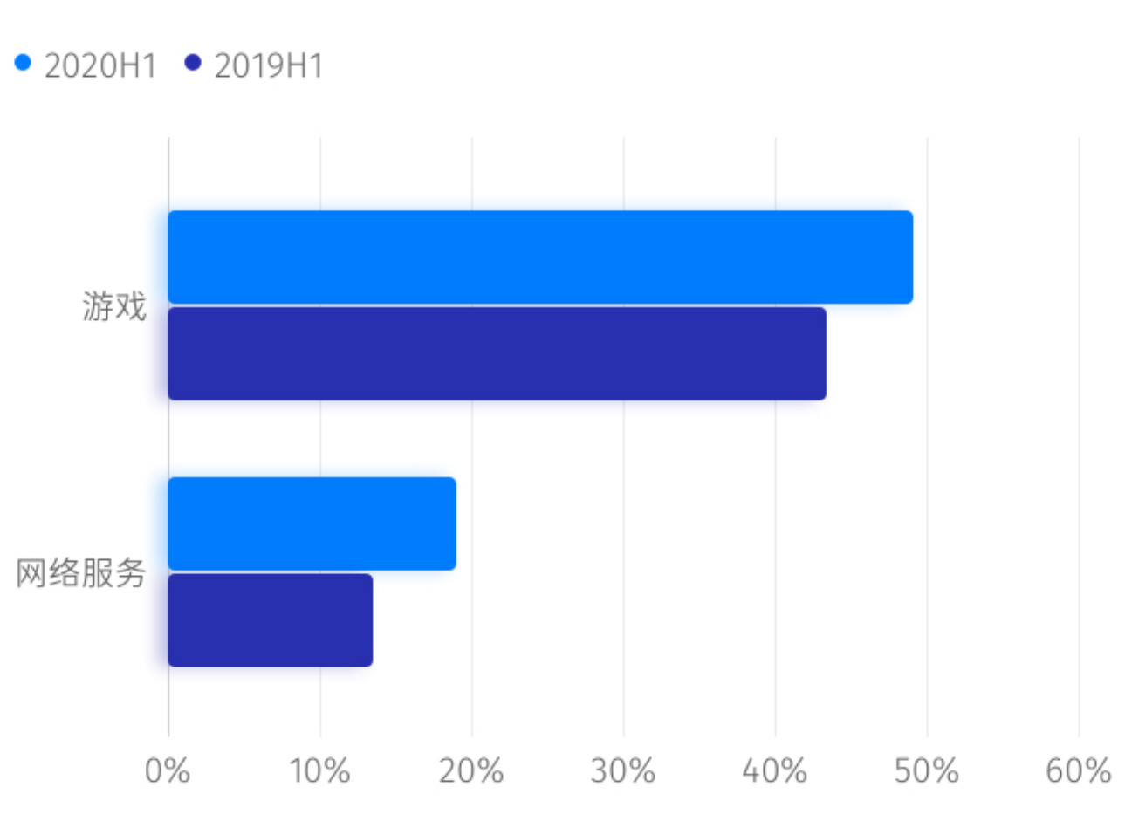
新手法层出不穷

新反射手法以及放大倍数

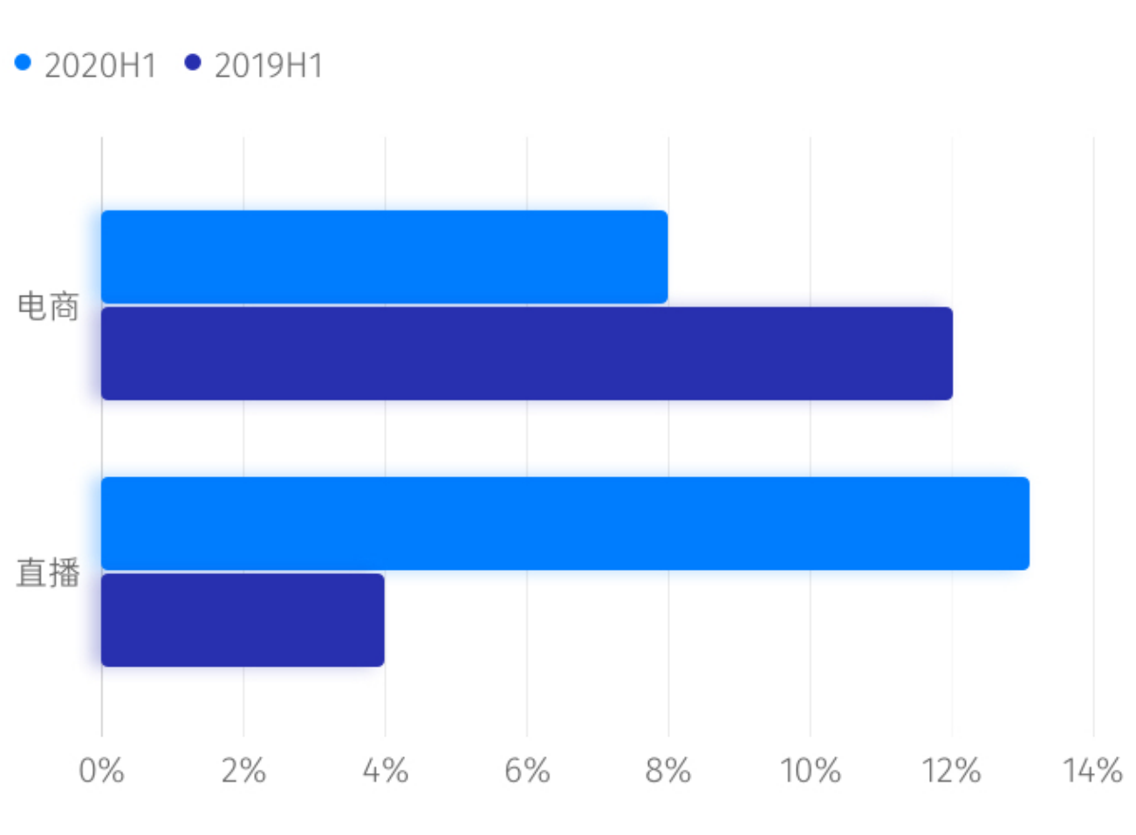


黑客·攻击趋势篇

游戏行业和网络服务行业占比最多

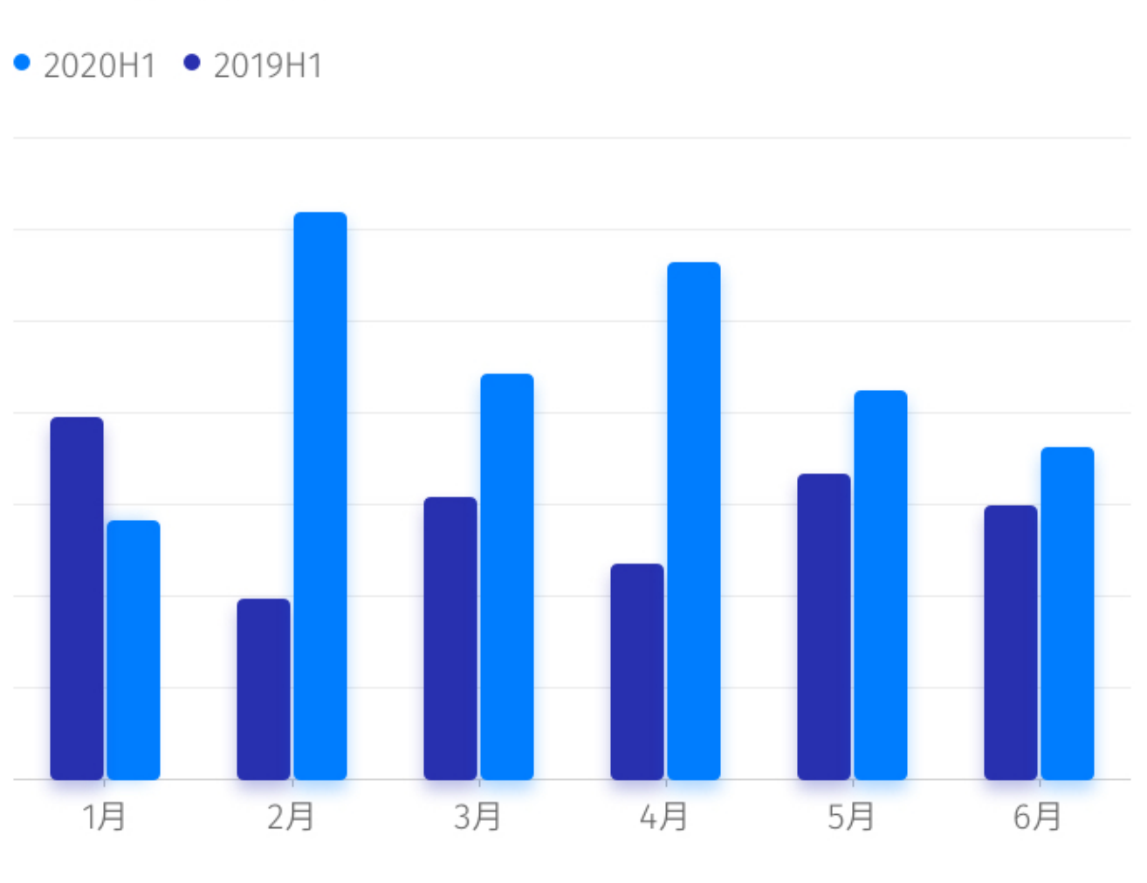


直播和卖货变化趋势相反



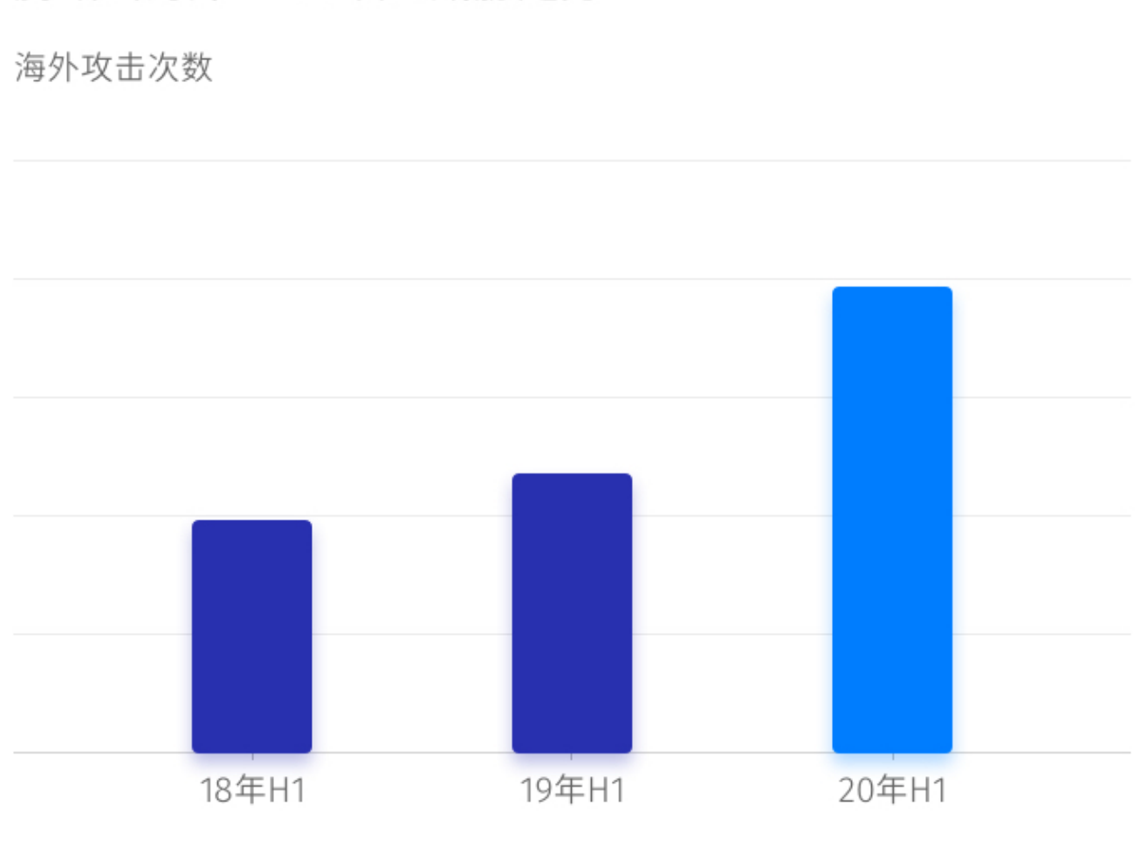
2月成黑客攻击最高峰

DDoS攻击次数走势



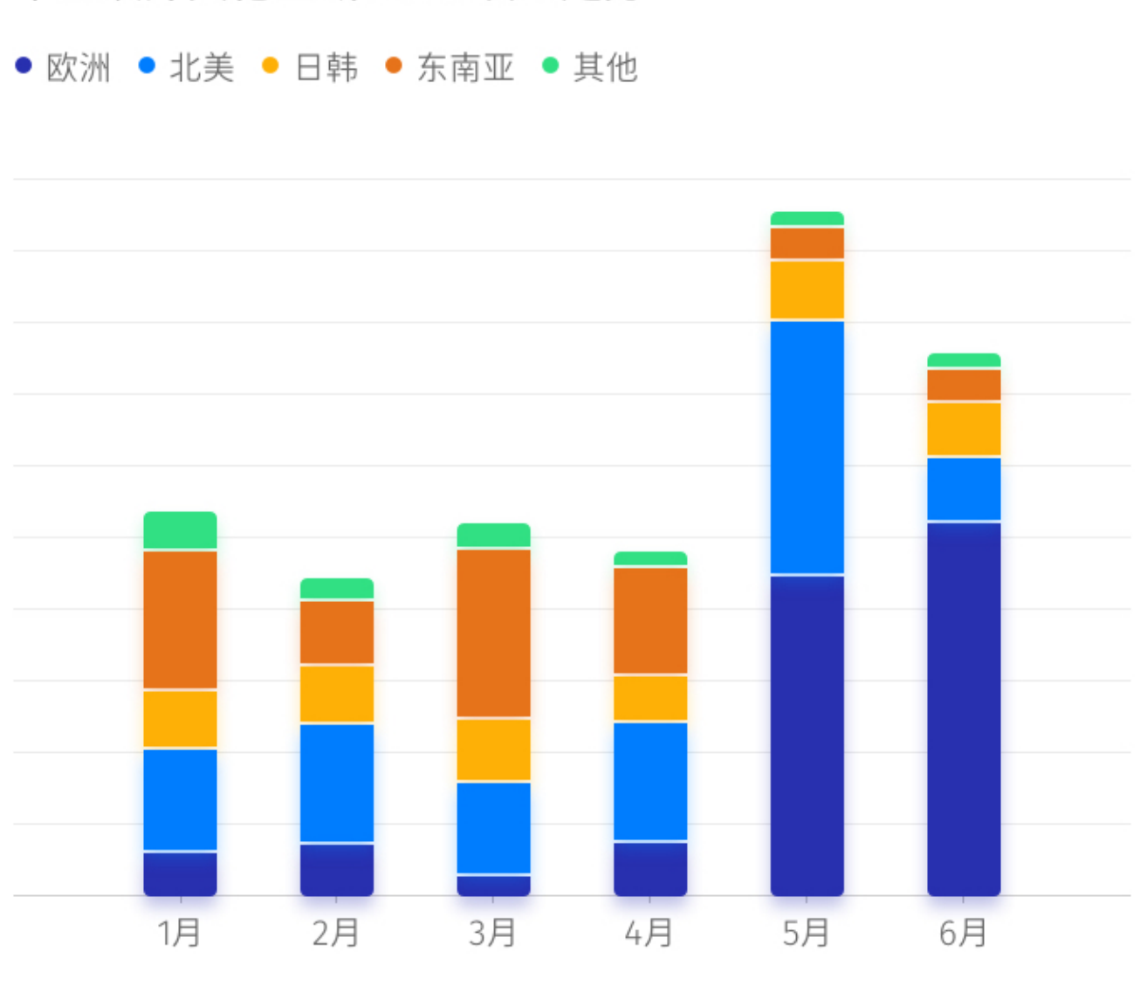
海外攻击持续增长

腾讯云海外DDoS攻击威胁走势



东南亚3月攻击最猛，欧美5月攻击最猛

中国以外其他区域DDoS攻击走势



大事记

1、2020年2月份，亚马逊AWS 观察迄今为止最大的DDoS攻击，最大攻击流量达到2.3Tbps，攻击手法为CLDAP 反射。

2、2020年4月20日，全球知名独立的技术和市场调研公司Forrester发布了最新的Now Tech ：DDoS Mitigation Services, Q2 2020，腾讯云入选云服务商类别推荐名单。

3、5月27日，腾讯安全DDoS防护T-Sec团队为腾讯云用户成功防御腾讯云上攻击流量最大的CC攻击，峰值时刻每秒HTTPS攻击请求超过260万。

4、受疫情影响，全国两会、广交会等会议的多个重要环节移步线上。为此，腾讯安全联合安全平台部宙斯盾团队等多个团队的安全专家，为业务提供了7*24小时全方位网络安全防护，保障期间业务安全稳定运营。优质安全的服务获全国人大实名点赞！

腾讯云·DDoS防护T-Sec
DDoS威胁报告

2020年上半年