腾讯安全 | NSFOCUS

2021年全球DDoS威胁报告

腾讯云T-Sec DDoS防护团队、绿盟科技威胁情报团队

目录
Contents

目录
Contents

第一章
专家观点

Expert Opinions

1 游戏仍然是攻击热点，出海游戏更易遭受 DDoS 攻击

根据腾讯云 T-Sec DDoS 防护团队数据显示，互联网多元化发展迅速，云计算、视频直播等新兴行业倍受用户青睐，DDoS 黑产攻击目标也紧随热点业务产生变化，整体来看，今年游戏仍是受 DDoS 攻击最多的行业，但攻击占比为历年新低。

相比于国内发行的游戏，出海游戏更易遭受 DDoS 攻击：一方面，出海企业大多复制国内已验证的成功商业模式，推出的游戏往往颇具竞争力，容易成为海外 DDoS 攻击的目标；另一方面，国外环境比较复杂，以 ACCN 为代表的黑产团伙肆无忌惮，出于敲诈勒索目的的 DDoS 攻击层出不穷。

防护建议：
出海游戏企业在业务拓展到海外的同时，务必需要将安全能力，尤其是 DDoS 防护能力的短板补齐，避免长期的研发成果在黑客攻击面前化为灰烬。

2 虚拟货币监管加码，大量肉鸡流入 DDoS 攻击黑产

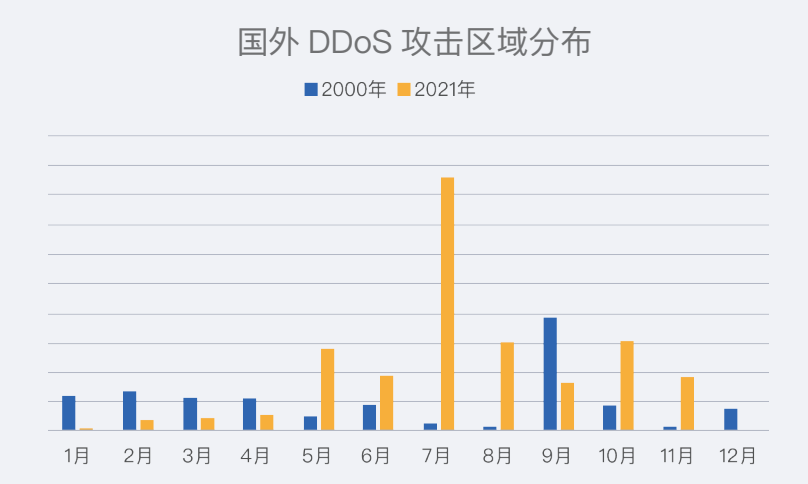
对黑产来说，考虑到动辄数十倍甚至数百倍的放大比，UDP 放大攻击是发起 UDP 类大流量攻击最经济有效的方式。但是腾讯云 T-Sec DDoS 防护团队通过分析数据发现，今年 5 月份以来，未使用 UDP 反射的大流量 UDP flood 攻击比去年明显增多。出现这一现象的原因可能是国家针对虚拟货币挖矿行业进行了持续整治，大量肉鸡从挖矿领域回流进入 DDoS 攻击黑产。

根据历史数据分析，比特币等虚拟货币的价格与肉鸡发起 DDoS 攻击呈现明显负相关。因为挖矿僵尸网络会引起操作系统 CPU 负载消耗过高，往往被安全人员发现并清理。所以挖矿僵尸网络数量需要不断“补量”才能持续达到同等收益，当虚拟货币价格下跌时，黑产团伙选择投放僵尸网络 DDoS 攻击模块，虚拟货币价格上涨时，则选择投放挖矿模块，以实现团伙利益最大化的核心诉求。

2021 年下半年以来，国家持续加强整治虚拟货币“挖矿”活动，以改善能源利用效率，维护社会稳定和国家安全。大量基于矿机挖矿的企业迁移海外，利用肉鸡进行挖矿的黑产也受到较大冲击。大量肉鸡从虚拟货币挖矿行业流出，进入 DDoS 攻击领域。

黑客手里的肉鸡资源较为富余，在 5 月份之后的几个月，不通过反射放大而是利用肉鸡直接发起的 UDP flood 攻击大幅高于去年同期水平，甚至 2021 年 7 月一个月的攻击数量都高于 2020 年上半年或下半年的总和。同时，今年此类攻击的最大攻击流量相比去年增长了 2 倍多，高达 787G。

防护建议：
预计在未来几年里，DDoS 攻击的峰值及大流量攻击发生的次数都会持续增长，企业须评估在遭遇 Tb 级超大流量攻击的极端场景下，现有防护方案和防护资源是否还能保障业务不受 DDoS 攻击影响。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

3 僵尸网络成扫段攻击重要推手

扫段攻击是近年兴起的一种攻击方式，会对一大段 IP 同时或顺序发起 DDoS 攻击，针对同一 IP 的攻击流量较小、时间持续较短，一般控制在 3–30 秒内，并且组合多种 DDoS 攻击类型发起攻击。腾讯云 T–Sec DDoS 防护团队也多次防御发生在现网的扫段攻击。在最密集的攻击期间，单天被攻击的 IP 数以万计，从单个 IP 的攻击流量来看，单次扫段攻击的最大攻击流量超过 700G。

无论从攻击涉及的 IP 数还是单个 IP 的最大攻击流量来看，扫段攻击对企业都是极其严峻的挑战，攻击表象背后的逻辑是黑产团伙和攻击防御者之间的心理、智力、技术、体力的对抗与博弈。看似是零星攻击，但黑产团伙会对受害者的 IP 地址、攻击间隔、攻击时长，攻击频度进行不断变化。这类攻击是对现有 DDoS 监测和防御中的单 IP 流量人工阈值、单 IP 流量牵引、牵引消耗等防御策略的针对性对抗。

据腾讯云 T–Sec DDoS 防护团队监测数据，扫段攻击大体分为两种：带宽型扫段攻击和扫描型攻击。这两种扫段攻击方式在单个 IP 的攻击时长、攻击流量及攻击手法方面存在差异。通过持续监测和研究发现，部分扫段攻击的幕后黑手竟是一些业界知名的 DDoS 僵尸网络。

DDoS 僵尸网络控制的资源众多，攻击目标变换迅速，溯源非常困难。目前监测到的扫段攻击都是一些常见手法，但由于大量 IP 被同时攻击，很容易出现少量透传导致机房网络异常、大量攻击流量与业务流量叠加，导致防护设备性能紧张等问题，应对方案和普通的 DDoS 攻击有较大区别。

防护建议：
企业在日常安全防护中应制定必要的预案，进行适当的演练，提升扫段类攻击的监测和响应的灵敏度 。

4 漏洞修复不及时，僵尸网络利用时差攻击

绿盟科技观察，DDoS 攻击是僵尸网络第一个有明确收益的攻击方式，在国家和安全人员不断治理打击僵尸网络的形式下，黑产团伙往往打时间差，抢在漏洞修复前利用漏洞投放僵尸网络程序，并持续寻找新型反射漏洞。

以 CVE-2021-22205 漏洞为例，虽早在 2021 年 4 月，GitLab 就已对该漏洞发发布补丁，但 11 月，负责谷歌 DDoS 防御的云安全可靠性工程师 Damian Menscher 披露，DDoS 攻击团伙利用该漏洞批量攻陷了数以万计的服务器，将这些服务器加入僵尸网络，发动大规模 DDoS 攻击。

据腾讯云 T-Sec DDoS 防护团队监测数据，10 月 31 日起，Mirai 僵尸网络团伙控制的肉鸡数量开始快速增长。该僵尸网络以大量入侵 IoT 设备著称，但新增的肉鸡中，超过 60% 是存在漏洞且运行着 GitLab 服务的服务器。说明在 GitLab 漏洞的影响下，Mirai 僵尸网络不再局限在 IoT 设备领域，而是将触手伸向了存在漏洞的 IDC 服务器。

不仅 Mirai 僵尸网络从 GitLab 漏洞乘虚而入，其他僵尸网络（如 BillGates 僵尸网络）也有运行着 GitLab 服务的服务器加入，数量不等。尽管在最初几天里，随着 GitLab 服务器上的漏洞修复，僵尸网络控制的肉鸡数量也在不断减少，但从监控数据看，仍有不少机器因漏洞未修复，成为僵尸网络持续活跃的肉鸡。

防护建议：
企业发现服务器存在高危安全漏洞时，务必及时修复。否则，不仅导致存在漏洞的机器被黑客攻陷，还会波及内部其他服务器，导致大量服务器被部署僵尸网络的攻击程序，持续对外发起 DDoS 攻击。

5 DDoS 威胁或成为犯罪团伙首选勒索手段

勒索软件攻击事件在 2021 年闹得沸沸扬扬，绿盟科技观察，2021 年勒索软件和 DDoS 攻击曾多次同时勒索受害者。犯罪团伙利用勒索软件实施勒索，若受害者不支付赎金，便威胁将数据公之于众。此时，如果受害者报案，犯罪团伙就发起 DDoS 攻击，试图报复。勒索 DDoS（Ransomware DDoS） 事件前几年已经出现，2020 年和 2021 年勒索团伙赚得“盆满钵满”，进一步刺激了 DDoS 攻击团伙的贪欲。而 DDoS 攻击溯源难度较大，勒索实施成本低、收益丰厚，预计未来一段时间内，DDoS 勒索依然对企业安全构成较大威胁。

防护建议：
企业在遭受 DDoS 勒索时，建议不要支付赎金。支付赎金虽能获得短暂的喘息，但带来的将是永无休止的勒索攻击。改头换面，专打弱点是 DDoS 攻击团伙的惯用手段。寻求专业正规 DDoS 防护厂商，一起协同对抗 DDoS 攻击团伙才是抵御 DDoS 勒索的长久之道。

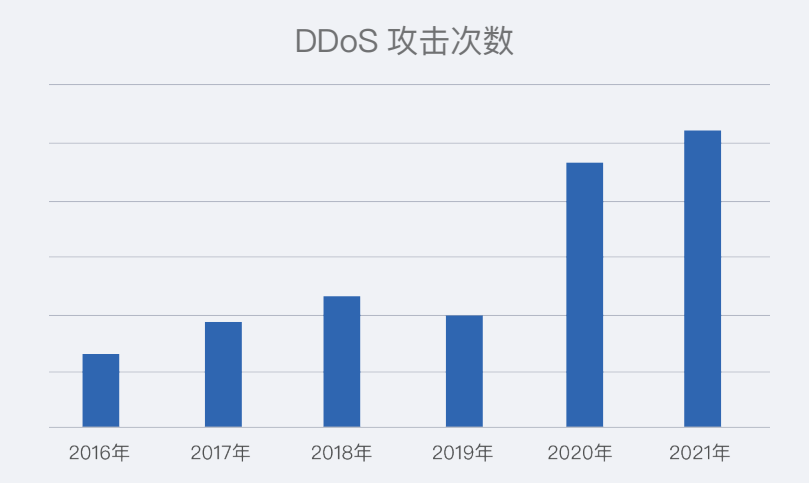
第二章
整体威胁

Overall Threats

1 DDoS 攻击连增 2 年，Tb 级攻击时代已逾 5 年

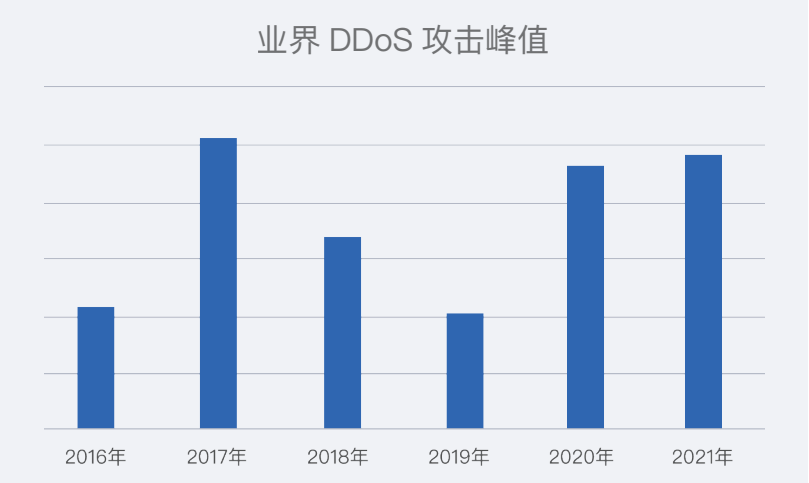
疫情之下，传统的旅游、社交、差旅、文体娱乐、线下零售等活动受到较大冲击，线上直播、社交、游戏、视频、办公等活动越来越多地融入人们生活，互联网行业成为近两年难得的持续高速增长的行业。

线上业务繁荣，DDoS 攻击黑产也早已适应了网上交易的模式，攻击活动更为频繁。从整体看，近两年的攻击次数均高于疫情爆发前。继去年攻击次数大幅增加后，今年攻击次数依旧呈增长态势，实现了 2 连增。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

除了攻击次数持续增长，2021 年业界最大的 DDoS 攻击流量达到 2.4Tb，腾讯云 T-Sec DDoS 防护团队也多次成功防护 Tb 级别的 DDoS 攻击，最大攻击流量达 1.26Tb。这意味着 DDoS 攻击峰值在 2016 年迈入 Tb 级攻击时代后，连续 5 年超过 1Tb，Tb 级别攻击已成为企业的现实威胁。



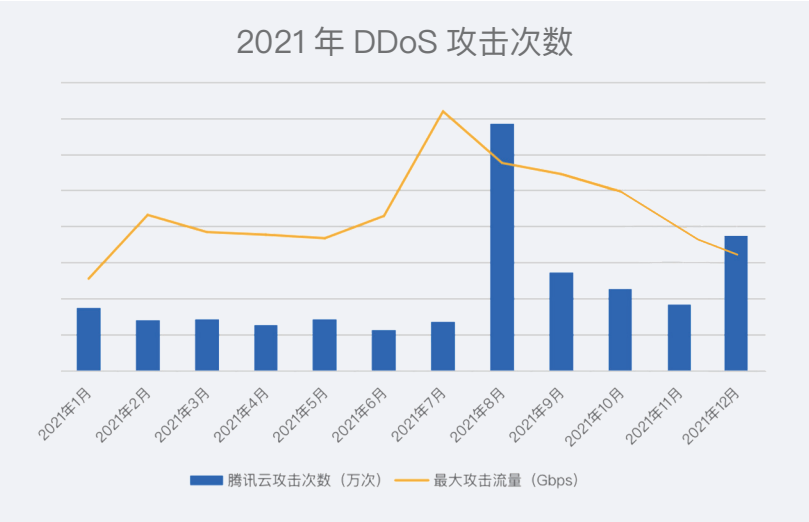
腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

2 下半年攻击又多又猛，8 月成攻击高峰

通常来说，人们下半年的消费活动较为旺盛，企业往往迎来业务高峰，这也会导致互联网企业在下半年遭受更多的 DDoS 攻击。今年下半年的 DDoS 攻击威胁远远大于上半年，不仅 8 月份的攻击次数遥遥领先，接近上半年的攻击总次数，而且下半年每个月的攻击次数均大于上半年单月次数。

一方面，虚拟货币挖矿行业受到强大的监管，大量肉鸡从挖矿流入 DDoS 攻击黑产；另一方面，部分广泛使用的基础软件存在漏洞，大量 IoT 设备或 IDC 服务器受漏洞影响成为肉鸡。上述两个因素使攻击者攻击资源大幅增加，导致下半年 DDoS 攻击峰值水涨船高，7 月份多次攻击突破 Tb 级，最大攻击流量为 1.26Tb。

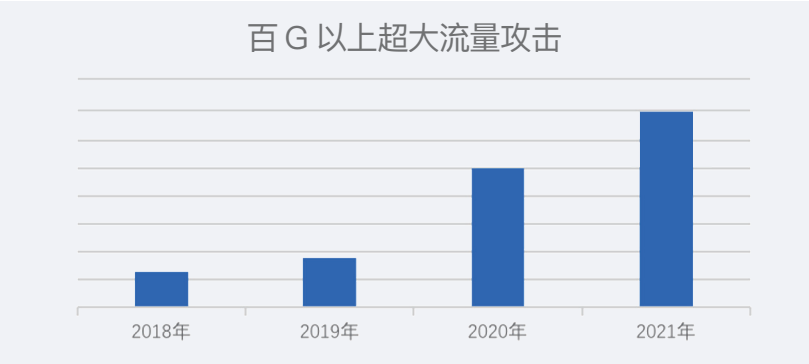
黑产团伙常利用攻击次数、攻击流量、攻击类型、攻击时间点等组合因素制定攻击策略，尝试产生最大化打击效果。因此，平衡多种因素制定防御方案也是一项高难度的挑战。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

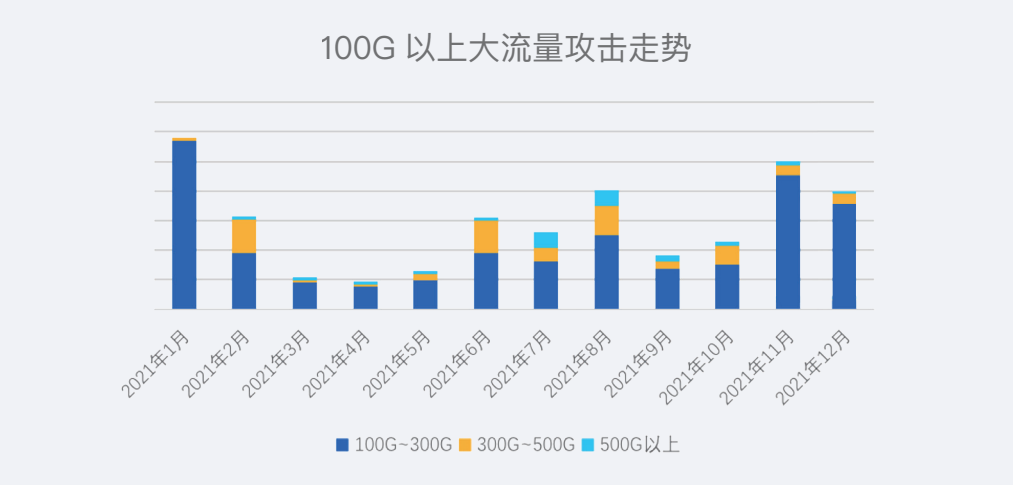
3 大流量攻击呈现多元化趋势

整体来看，5G 快速覆盖，家庭网络带宽大幅提升，大量设备接入网络，导致黑客攻击资源不断增加。这一趋势不仅推升了 DDoS 攻击次数，也导致超百 G 大流量攻击持续增长，对企业带来重大危害。



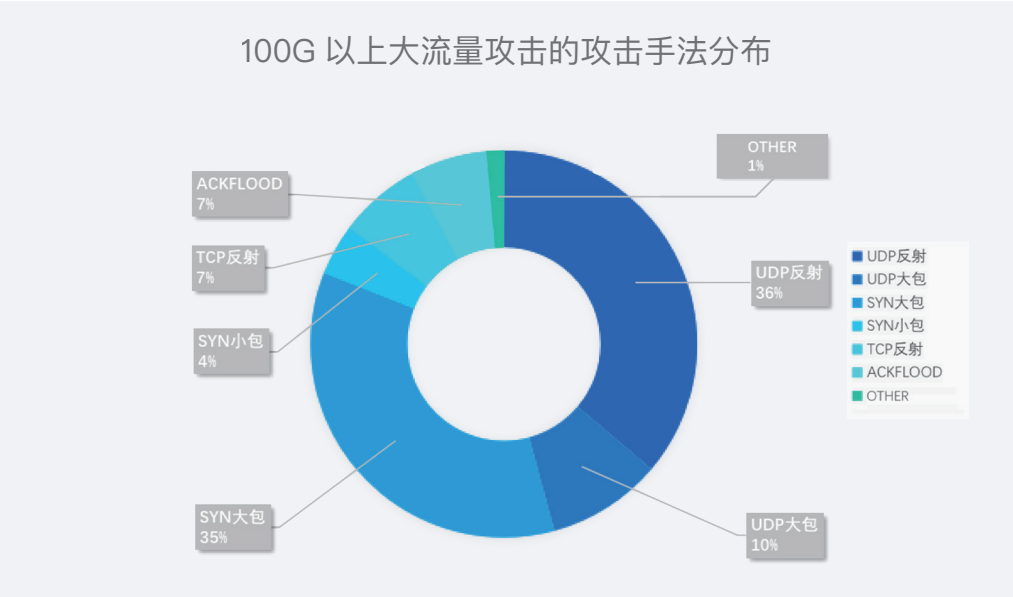
腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

在上述因素的影响下， 300G 以上更大规模的 DDoS 攻击在超百 G 的大流量攻击中的占比也明显提升，2021 年有 5 个月（2 月、6 月、7 月、8 月、10 月）占比超过 30%。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

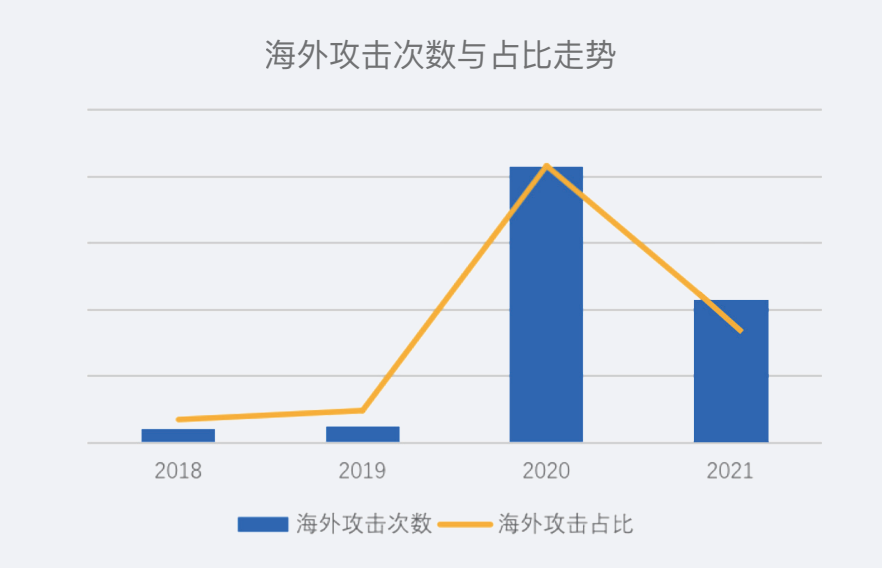
黑客拥有数以千万计的各类 UDP 反射源，挖矿活动整治及漏洞利用促使大量肉鸡流入 DDoS 攻击黑产。此外，近两年兴起的 ACK 反射格外受黑客重视，挖掘出的反射源也数以千万计。这些变化不仅抬高了大流量攻击的次数，也影响到了黑客发起大流量攻击的方式。前几年的大流量攻击手法基本都是 SYN 大包和 UDP 反射的天下，但今年统计数据显示，相当比例的超百 G 大流量 DDoS 攻击是由 SYN 大包或 UDP 反射之外的手法发起的（包括 TCP 反射、SYN 小包、ACKFLOOD 等），说明超百 G 大流量 DDoS 攻击手法呈明显多元化趋势。



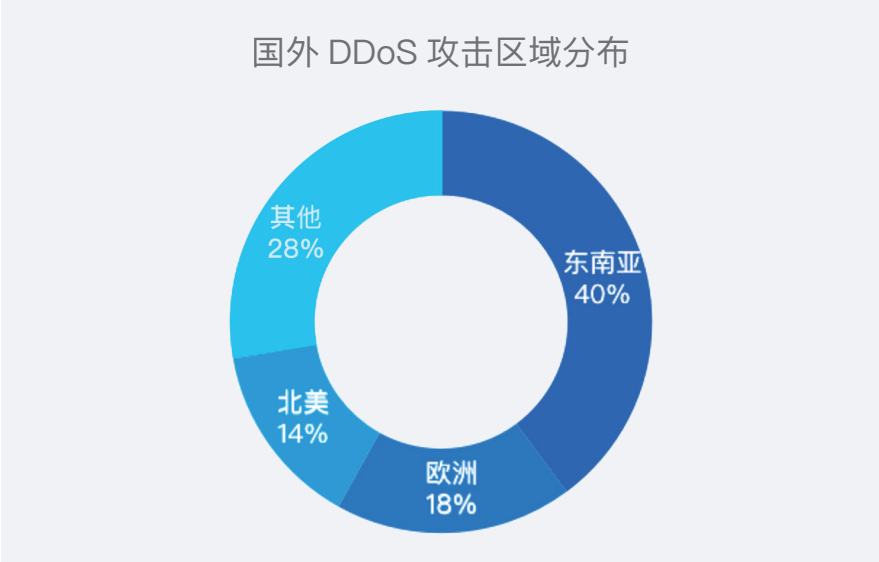
腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

4 海外攻击数据占比 20%，东南亚成主要攻击战场

中国的游戏、直播、社交和电子商务等互联网企业在海外持续拓展，目前已取得相当不错的成绩，海外 DDoS 攻击威胁也较为突出。从 DDoS 攻击数据上看，2021 年海外攻击次数在整体中的比例比 2020 年有所回落，但仍然远远高于 2018 年和 2019 年。地域上看，东南亚地区 DDoS 攻击占比最高，占海外总攻击次数的 40%。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

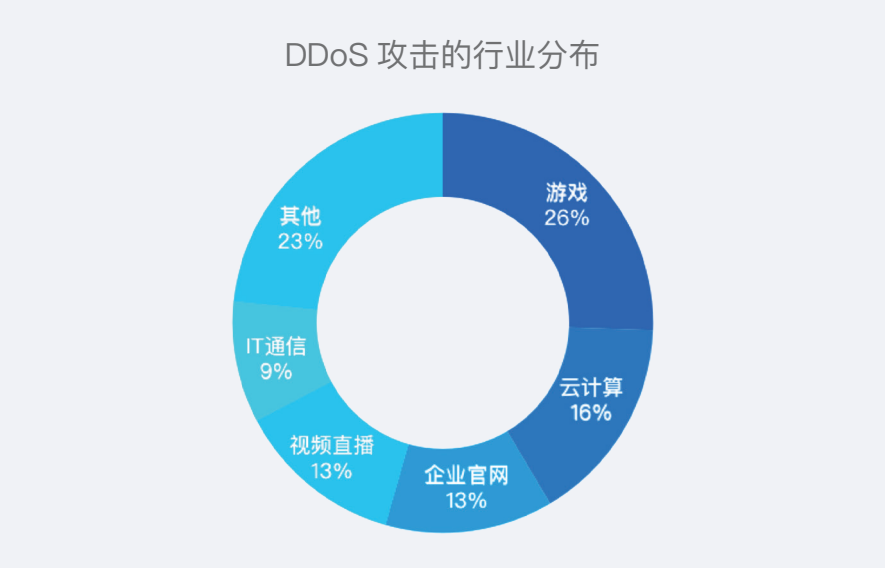


腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

5 攻击行业分布多元化，游戏行业占比仍居第一

根据腾讯云 T-Sec DDoS 防护团队监测数据，2021 年 DDoS 攻击行业分布呈现多元化趋势。游戏行业 DDoS 攻击占比继续保持第一，但是相比往年比率偏低，不再是一家独大的局面。除游戏行业外，云计算、企业官网、视频直播、IT 通信等行业成为 2021 年攻击占比较高的行业。

腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

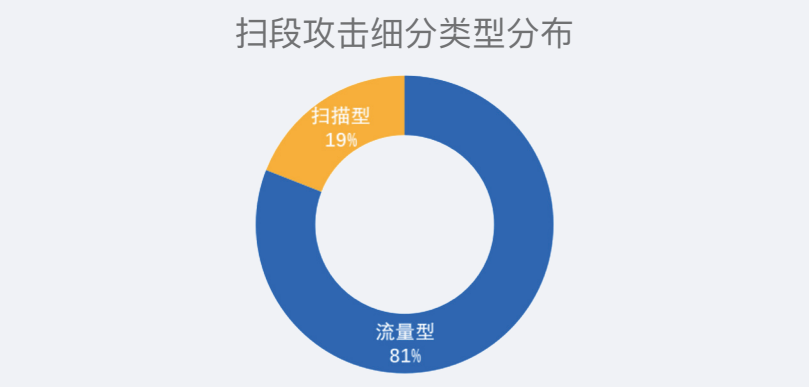


腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

6 扫段攻击成网络公害，脉冲攻击防不胜防

扫段攻击是近年来兴起的一种攻击方式，和以往攻击者只盯着单个目标 IP 不断变换攻击手法、寻求突破防护策略短板的攻击方式不同，扫段攻击多使用已知的通用攻击手法，攻击期间基本不会变换，但攻击者会在短时间内对大量 IP 进行无差别攻击，令大量攻击流量涌入机房，而防护设备也需要承载大量 IP 上的业务流量，防护系统性能压力大，易造成整个机房业务瘫痪。

根据腾讯云 T-Sec DDoS 监测数据，扫段攻击大体分为 2 种：带宽型扫段攻击和扫描型攻击。带宽型扫段攻击在整体扫段攻击中占比 81%，主要以 UDP 反射为主，部分攻击为混合手法攻击。此类攻击单个 IP 上的攻击流量较大，典型的攻击中，单个 IP 攻击流量可达数十 G 至上百 G，单个 IP 的攻击时间大约在几十秒至数分钟不等。扫描型攻击则是以 SYN 小包为主，相对而言单个 IP 攻击流量较小（几十 M 至数百 M 不等），单个 IP 持续的攻击时间较短（数秒至十几秒不等），各个 IP 上的攻击流量比较均匀，但是多个 IP 同时期的瞬时攻击流量仍然高达数十 G，带来的危害同样不容小觑。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

除了扫段攻击外，脉冲攻击也成为现网比较典型的攻击手法。黑产团伙通过定制攻击工具，以固定时间为间隔，短期内对目标发起高达业务流量上千倍大小的攻击流量，随后很短时间内，攻击又消失于无形。这种攻击流量增长快、消失快，攻击密集，不仅让企业的安全运维人员不堪其扰，对防护系统的性能和灵敏度也提出了更高的要求。

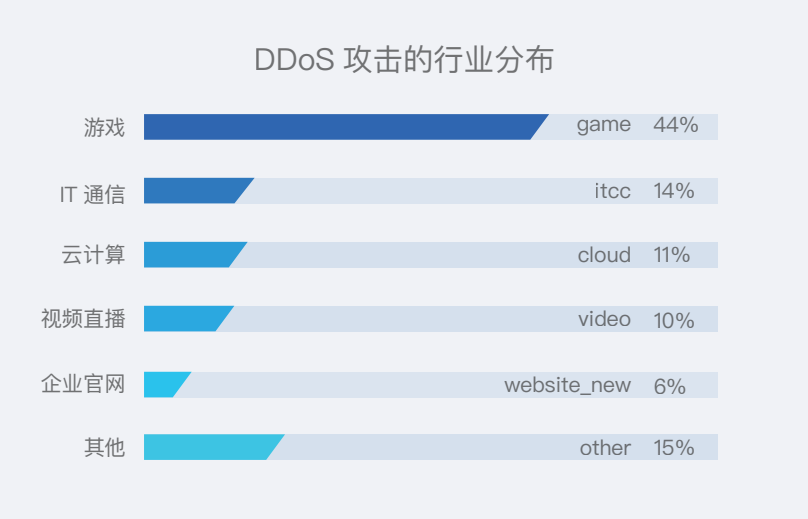
腾讯云、绿盟科技2021年全球DDoS威胁报告

第三章
海外威胁

Overseas Threats

1 海外与国内攻击热点行业重合

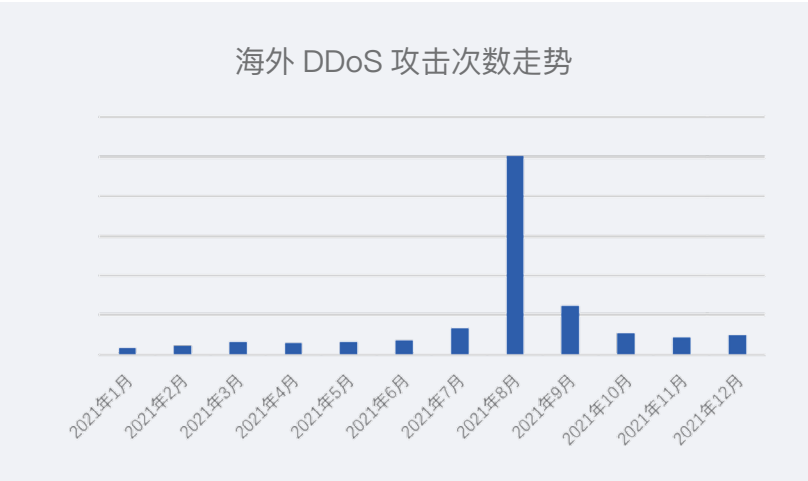
出海企业大多复制国内已验证的成功商业模式，推出的业务往往颇具竞争力，因此容易成为海外 DDoS 攻击的目标。与国内相似，海外攻击排名第一的行业也是游戏行业，但海外的攻击占比高于游戏行业在国内的攻击占比，游戏在海外攻击中占比近一半。此外，和国内一样，海外 IT 通信攻击占比位居第二，略多于一成。云计算、视频直播等行业的占比也较多，大约在一成左右。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

2 扫段攻击使 8 月成攻击最多月份

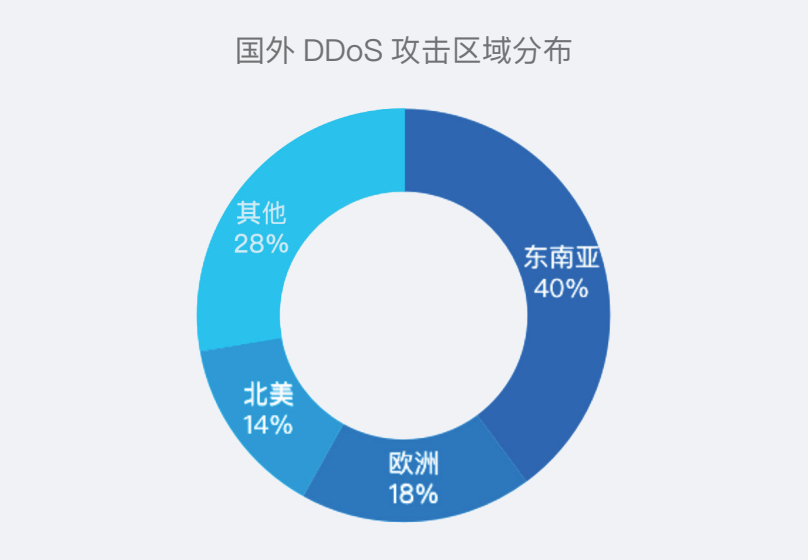
海外攻击整体呈现下半年多于上半年的趋势，8 月由于多个区域出现大规模扫段攻击，导致 8 月攻击次数约为其他月份的总和。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

3 东南亚成海外攻击热点区域

一般来说，DDoS 攻击的地域分布和当地经济发展水平以及人口数量呈正相关趋势。此外，中国一些游戏、直播、网络通信等出海企业比较集中的区域，企业间竞争更激烈，也会成为海外 DDoS 攻击的主战场。其中，东南亚区域人口众多，经济发展水平高，是中国出海企业集中的地区，因此成为海外 DDoS 攻击最集中的区域。除东南亚之外，整体来看， 2021 年海外的 DDoS 攻击总体分布比较均衡。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

4 海外多次攻击超过 1Tb

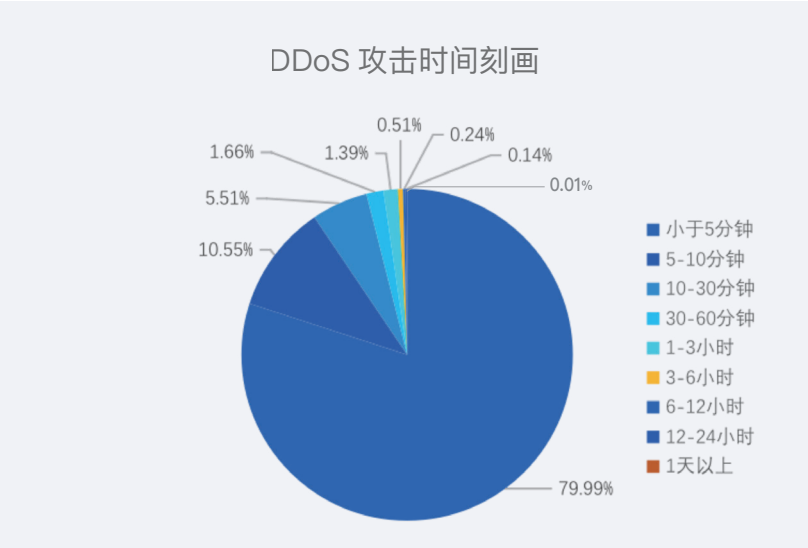
2021 年 7 月，业界厂商披露了 2 次超过 1Tb 的大型 DDoS 攻击，其中 Imperva 防护了一次峰值流量达 1.02Tb 的大型 DDoS 攻击。NETSCOUT 也在其威胁报告中披露，一次针对德国某运营商的大型 DDoS 攻击峰值流量高达 1.5Tb。

2021 年 8 月，微软云服务 Azure 的某欧洲客户遭遇了一次 2.4Tb 的超大流量 DDoS 攻击。尽管本次攻击未打破 2.54Tb 的历史最大 DDoS 攻击记录，但 2.4Tb 的攻击峰值距离 2.54Tb 仅一步之遥。

此外，根据业界厂商 Cloudflare 的报告，2021 年 Cloudflare 为其客户防护了数十次超过 1Tb 的大型 DDoS 攻击，其中 11 月份的一次攻击峰值流量接近 2Tb。

5 高频瞬时攻击成对抗博弈的重要手段

根据绿盟 Bothunter 监测数据来看，2021 年，80% 的 DDoS 攻击时长在 5 分钟以内。瞬时攻击占比高，说明攻击者越来越重视攻击成本、效率和技术对抗，倾向于在短时间内，以极大的流量导致目标服务用户掉线、延时和抖动。长远来看，多次瞬时攻击能够严重影响目标的服务质量，有效控制攻击成本，尽快耗尽 DDoS 防御服务人员的精力。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

第四章
黑产视角

Black Market Perspective

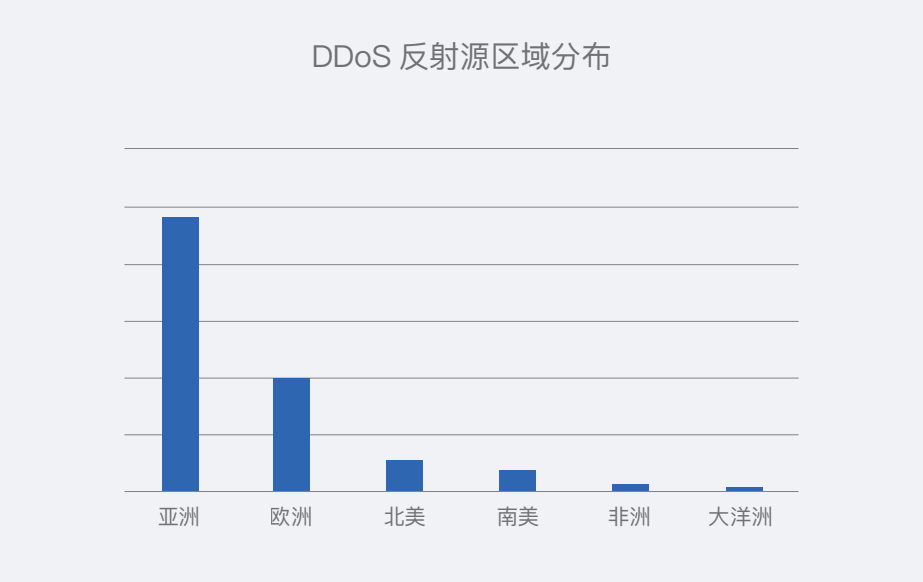
DDoS 攻击背后是完整复杂的黑色利益链，和不择手段、规模庞大的捞金团伙。与之对抗，既要在防御上推陈出新，不断引入新型技术，也要知己知彼，对黑客团伙的战术持续研究。

1 中国是主要攻击源来源国之一

中国经济体量大、人口多，互联网产业较发达，一直位居最主要攻击源来源国家的前 2 位，来自中国的攻击源超过 50%。日本、德国、韩国、英国等发达国家，以及越南、印度尼西亚、巴西、印度等发展中国家也是主要的攻击源分布国家。

2 DDoS 反射源分布与 IoT 发展速度及其基数相关

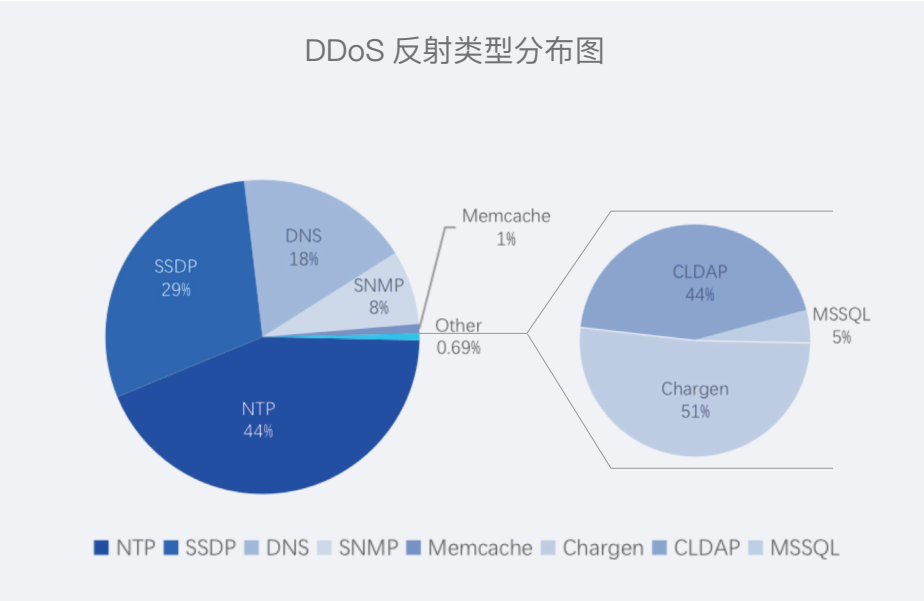
根据绿盟科技 Bothunter 监测数据显示，全球 DDoS 反射源与区域互联网发达程度高低呈明显相关性。全球物联网行业迅速发展，家用路由器、摄像机、门禁等设备纷纷接入网络。快速发展的同时，安全措施还未跟上，即使发现 IoT 设备漏洞，也很难在短期内快速修复。一旦被黑产团伙盯上，大量 IoT 设备会迅速被恶意利用。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

3 UDP 反射攻击类型利用喜好与反射放大倍数成正比

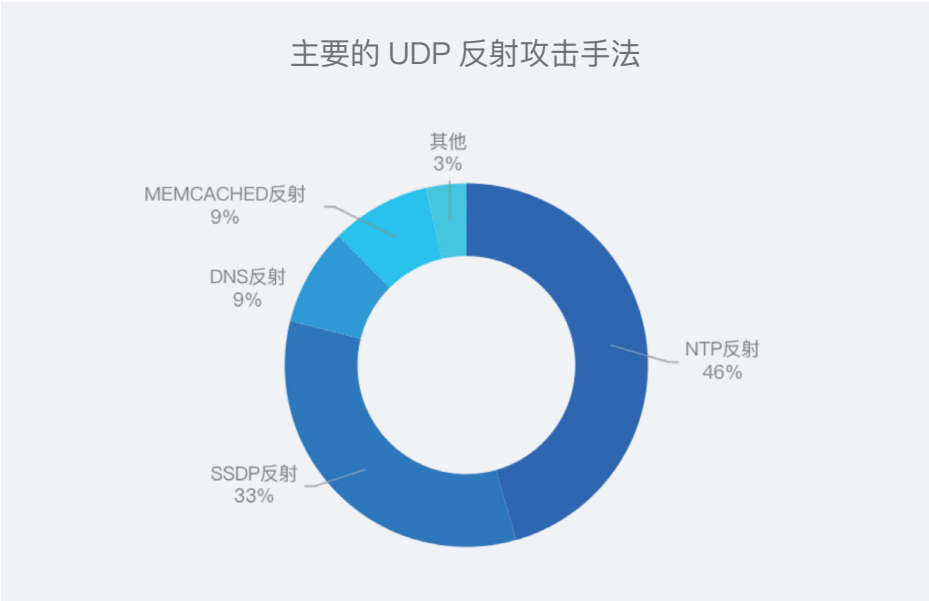
根据绿盟科技 Bothunter 监测数据来看，NTP 反射放大 400–500 倍、SSDP 反射放大 30 倍、DNS 反射放大 40–50 倍、SNMP 反射放大 4–6 倍。结合下图可以看出，UDP 反射放大类型分布与协议的反射放大比直接相关，但也同它们在互联网上的数量相关。以上放大类型常出现在超过 100G 以上的大流量攻击中，是大流量攻击的主要贡献者。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

4 UDP 反射仍是最主要攻击手法

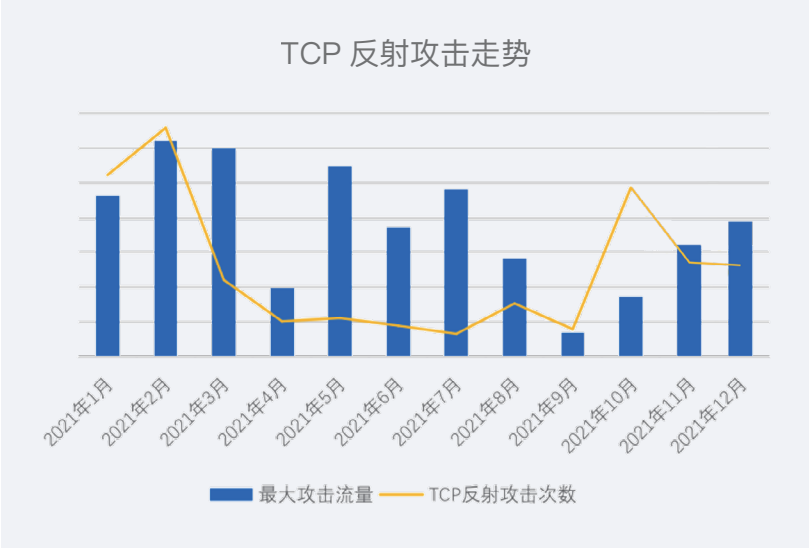
UDP 反射由于其可观的放大比和可以隐藏攻击者行踪的特性，历来被攻击者利用。从现网看，当前最常见的 UDP 反射方法为 NTP 反射和 SSDP 反射。此外在超过 100G 以上的大流量攻击中，SSDP 反射和 DNS 反射则最为常见。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

5 TCP 反射手法呈“U 型”走势

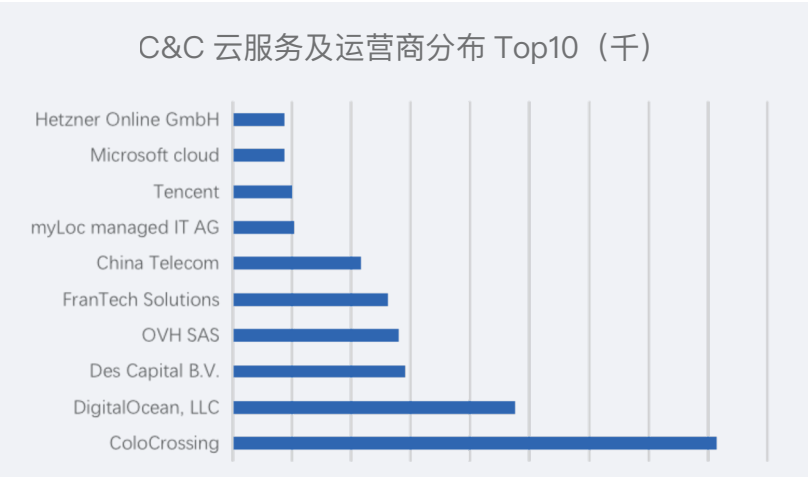
根据腾讯云 T-Sec DDoS 防护团队的监测数据，TCP 反射攻击在第一季度达到顶峰之后，出现明显回落。攻击次数在 4 月至 9 月期间处于近一年的低位。不过从 10 月份开始，TCP 反射的攻击手法开始增加，全年呈现 U 型走势。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

6 僵尸网络控制端（C&C）绝大多数位于国外

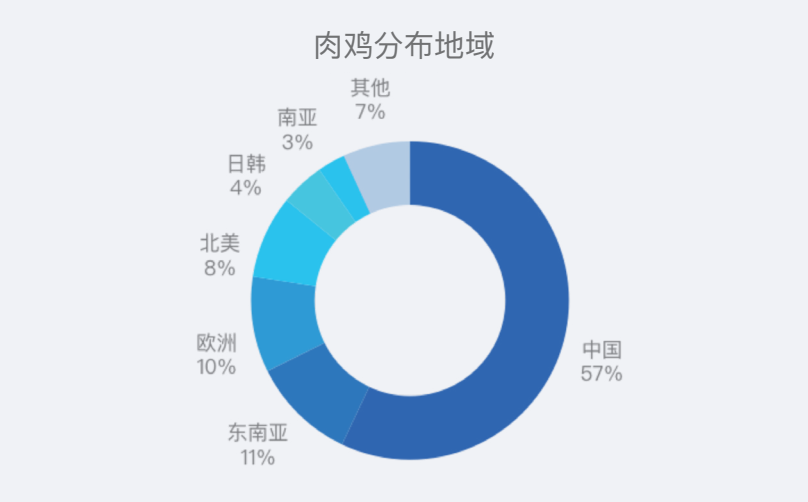
从绿盟科技 Bothunter 监测数据来看，大部分控制端来源于国外，其中北美、欧洲是僵尸网络控制端的主要分布地区，来自中国国内的控制端在整体中占比不足 10%。C&C 托管服务是黑产团伙关注的重点，每一个 C&C 控制着数以千计肉鸡，一旦肉鸡失联，相关付出将损失殆尽。因此黑产团伙会选择持续服务有保障、网络品质高、运营自主的服务商。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

7 肉鸡主要来自中国、东南亚、欧美

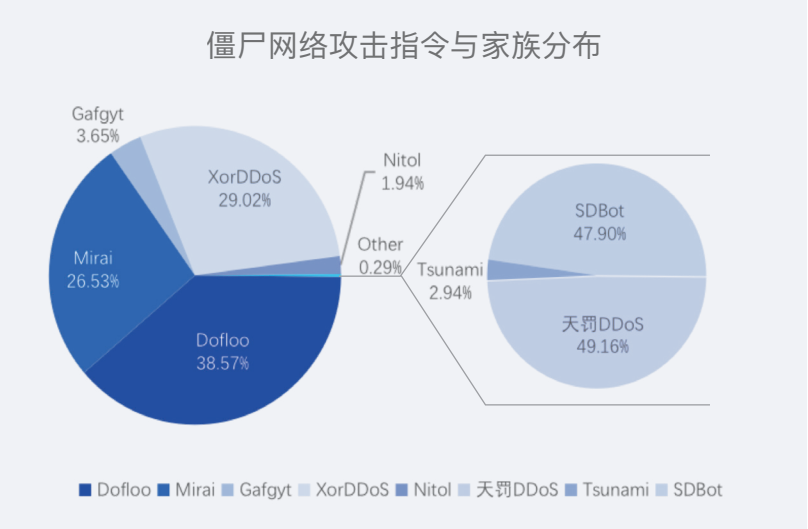
肉鸡分布的地域与经济发展水平以及互联网普及程度高度相关，全球几个经济较为发达的区域的肉鸡数都位居前列，具体来说，中国的肉鸡数占比超过 50%，东南亚、欧洲和北美的肉鸡数也在 10% 左右。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

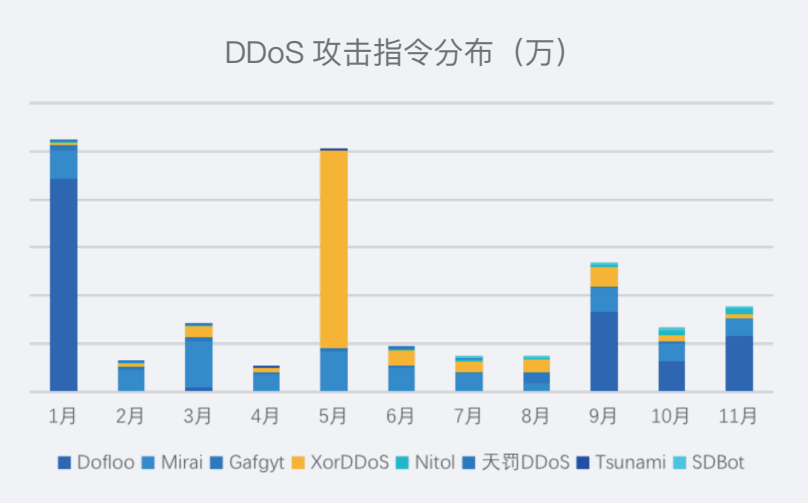
8 DDoS 僵尸网络四大家族各有特色，“一统江湖”局面不再

绿盟科技 Bothunter 在 2021 年对僵尸网络家族中 15 个 DDoS 僵尸网络家族进行跟踪，从中发现 Dofloo、XOR DDoS、Mirai、Gafgyt 家族攻击活动活跃度位列前四，攻击指令主要来自 8 个家族。到 11 月份共跟踪到 DDoS 攻击指令百万量级，其中攻击事件数量数大约是攻击指令的六分之一。主要的 8 个家族攻击比重如下：



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

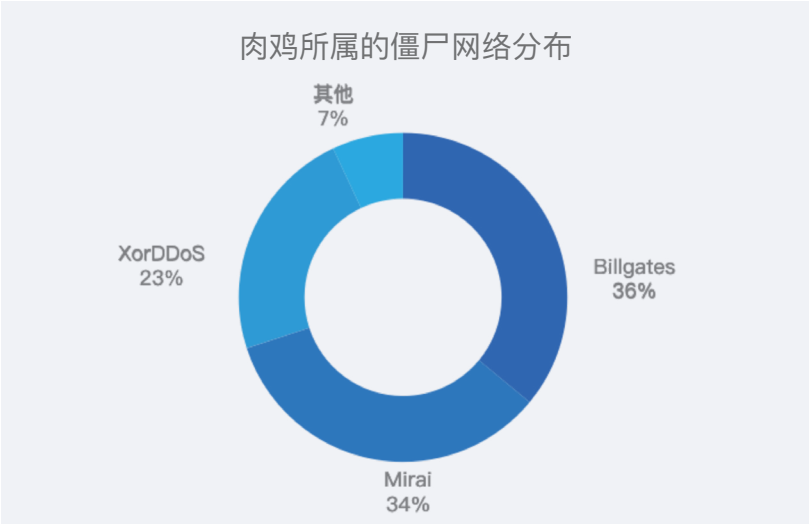
Mirai 家族在全年的整体活跃度较平稳，但其变种和感染速度最快。Dofloo 在 1 月份达到活跃高峰，在 9 月至 11 月活跃也较频繁。XOR DDOS 在 5 月份达到活跃高峰。其余家族活跃度相对更低，尚且无法与 Mirai、Dofloo、XOR DDOS 相提并论，但常一起参入攻击，可能是加入了 BaaS 组织。



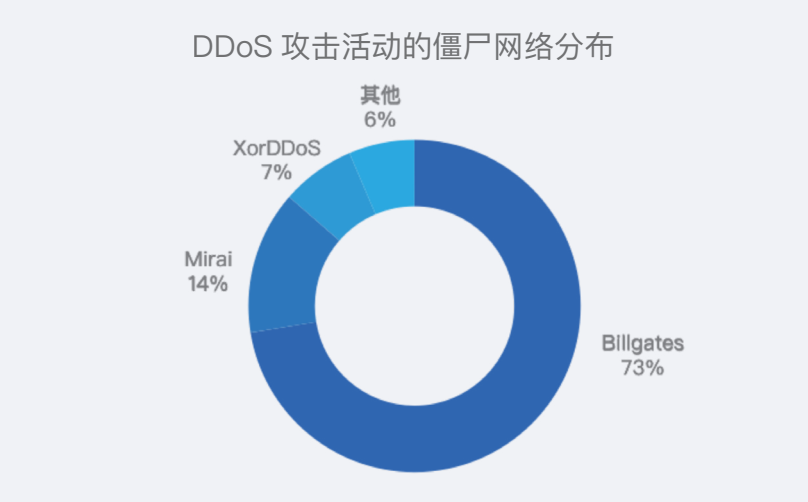
腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

9 XOR DDoS 逐渐没落，BillGates 最为活跃

根据腾讯云 T-Sec DDoS 防护团队研究，2021 年较为活跃的 XOR DDoS 僵尸网络在下半年变得萎靡不振，被 BillGates 僵尸网络和 Mirai 僵尸网络甩到了身后。其中 BillGates 僵尸网络控制的肉鸡数位居第一，发起的 DDoS 攻击活动（以单个 IP 当天被攻击计为 1 次攻击）是其余僵尸网络攻击活动的接近 3 倍。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

10 扩大僵尸网络规模是黑产团伙提升 DDoS 打击能力的重要手段

根据绿盟科技 Bothunter 监测数据，DDoS 僵尸网络利用漏洞和弱口令扩张控制范围的势头愈演愈烈。分析发现，当前被僵尸网络利用的在野漏洞已达 72 种，最快在 1 天内集成最新漏洞，抢在设备漏洞修复前，感染并控制设备。利用最频繁的漏洞是路由器设备 Web 管理端的命令执行漏洞，漏洞被各家族利用的分布情况如图所示：

DDoS 僵尸网络家族利用 Top 20

攻击事件使用Linux/IoT 漏洞TOP2N 对应家族分布表	Gafgyt	hybrid MQ	Mirai	Mozi	Persirai_ shiina	tsunami	vbot	ZHtrap
CVE-2NY7-Y72Y5	Y	Y	Y	Y	Y	N	Y	N
CVE-2NY8-YN56Y	Y	Y	Y	Y	Y	Y	N	N
CVE-2NY4-836Y	Y	Y	Y	Y	Y	Y	N	Y
Netgear_DGNYNNN_Y_Y_NN_48_Setup_cgi_Remote_ Code_Execution	Y	Y	Y	Y	Y	N	N	Y
Eir_DYNNN_Wireless_Router_WAN_Side_Remote_ Command_Injection	Y	Y	Y	Y	Y	N	N	N
JAWS_Webserver_unauthenticated_shell_command_ execution	Y	Y	Y	Y	Y	N	N	N
CVE-2NY5-2N5Y	Y	Y	Y	Y	Y	Y	N	N

攻击事件使用Linux/IoT 漏洞TOP2N 对应家族分布表	Gafgyt	hybrid MQ	Mirai	Mozi	Persirai_shiina	tsunami	vbot	ZHtrap
CCTV-DVR Remote Code Execution	Y	Y	Y	Y	Y	N	N	Y
ThinkPHP_5_X_Remote_Command_Execution	Y	Y	Y	N	N	Y	N	N
ZyXEL_P66NHN_T_vY_ViewLog_asp_privilege_escalation	Y	Y	Y	N	N	N	N	N
D_Link_OS_Command_Injection_via_UPnP_Interface	Y	Y	Y	Y	Y	N	N	N
CVE-2NY6-6277	Y	Y	Y	Y	Y	N	N	N
Vacron_NVR_RCE	Y	Y	Y	Y	Y	N	N	N
Seagate_BlackArmor_NAS_sg2NNN_2NNN_Y33Y_Command_Injection	N	N	Y	N	N	N	N	N
CVE_2N2Y_2NN9N	N	N	Y	N	N	N	N	N
SAPIDO_RB_Y732_Remote_Command_Execution	N	N	Y	N	N	N	N	N
CVE_2N2Y_35395	N	N	Y	N	N	N	N	N
Linksys_E_series_Unauthenticated_Remote_Code_Execution	Y	Y	Y	N	N	N	N	N
Common_Shell_Command_Abuse	Y	Y	Y	Y	Y	N	N	Y
D_Link_DSL_Devices_login_cgi_Remote_Command_Execution	Y	Y	Y	Y	Y	Y	N	N

腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

第五章：攻防对抗案例

Attack Defense Cases

1 攻防对抗案例

案例一：热门游戏遭多轮攻击，防护团队见招拆招

2021 年 5 月下旬开始，腾讯云某游戏行业客户旗下主要面向国内用户的热门游戏遭受多次攻击，攻防对抗除了常见的 SYN flood、 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，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。8 月开始，客户的海外业务逐渐遭到黑产团伙的持续攻击，经过腾讯云 T-Sec DDoS 防护团队客户安全运维团队的通力合作，该游戏客户的 DDoS 威胁得到有效遏制。

攻击对抗过程：

5 月初开始 SYN 大包、SYN 小包、UDP 大包攻击、UDP 反射放大攻击，针对客户的国内非重点业务进行试探。	**对抗策略：** 非核心业务按需开通高防，核心业务开通弹性高防。
5 月中旬开始 以 TCP 非法标志位攻击、ACKFLOOD、RST flood 手法攻击客户国内核心业务。	**对抗策略：** 高防开启针对 TCP 协议的 AI 算法。
5 月下旬 TCP、UDP、ICMP 之外的其他非常见 IP 协议也被用于攻击客户国内核心业务。	**对抗策略：** 启用非常用协议丢弃。
6 月中旬 针对性地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协议校验算法。	**对抗策略：** 引导客户接入安全水印算法。
6 月下旬 针对客户国内专线业务发起扫段攻击，单个 IP 最大攻击流量接近 600G。	**对抗策略：** 采用“海外流量压制 + 专线 IP 限速”的策略，确保专线业务不受影响，同时与业务侧进行联动，依据攻防对抗情况由用户对业务流量进行调度和重新负载。
7 月下旬 开始利用 UDP 大包攻击手法对海外业务进行初步的试探。	**对抗策略：** 海外非核心业务按需开通高防，核心业务开通弹性高防。

8 月中旬 动用 Mirai 僵尸网络对客户的海外业务进行大规模流量型攻击。	**对抗策略：** 联动腾讯云 T-Sec DDoS 防护威胁情报数据，针对提供了定制化的动态包长算法，依据自学习策略对 IP 下发动态包长拦截策略。

对抗难点及解决方案：

1. 客户面对的攻击团伙非常专业，攻击工具开发能力强，并且熟悉客户业务的分布情况、业务峰谷情况，对客户业务的协议也非常清楚，开发的攻击工具甚至可以完全伪装客户的业务协议。腾讯云 T-Sec DDoS 防护团队与客户运维团队及架构师团队一起，基于业务特性定制个性化检测和防护策略，对高危业务进行常态化防护，确保攻击流量 0 延迟，防护 0 透传。

2. 部分 UDP flood 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 系统利用自适应启发式算法，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 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。

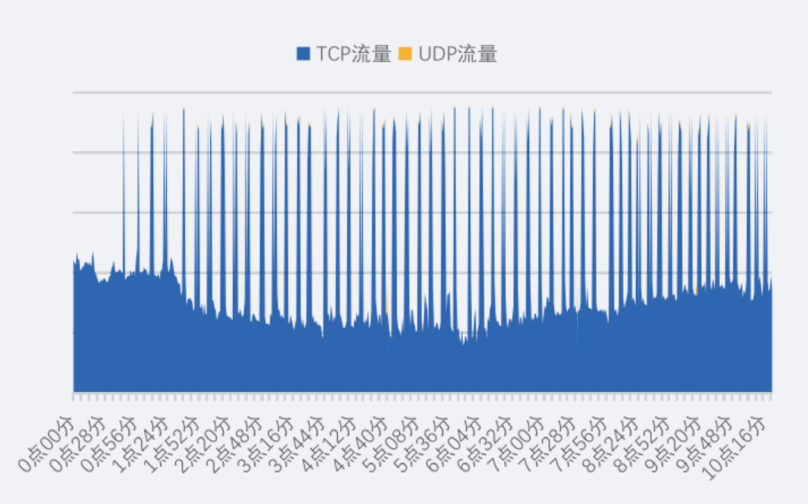
4. 攻防对抗极端激烈，除了腾讯云 T-Sec DDoS 防护安全专家全程支持，7×24 小时随时支援外，腾讯云 T-Sec DDoS 防护团队和客户安全运维团队通力合作，及时响应客户的防护需求，定制与客户业务方案高度融合的防护方案，让攻击者无计可施。

案例二：脉冲攻击并非无解，智能对抗升级策略

2021 年 10 月下旬，某腾讯云 CDN 业务客户在香港的业务 IP 遭受专业黑客发起的脉冲式 DDoS 攻击，攻击持续时间接近 10 小时。

对抗难点及解决方案：

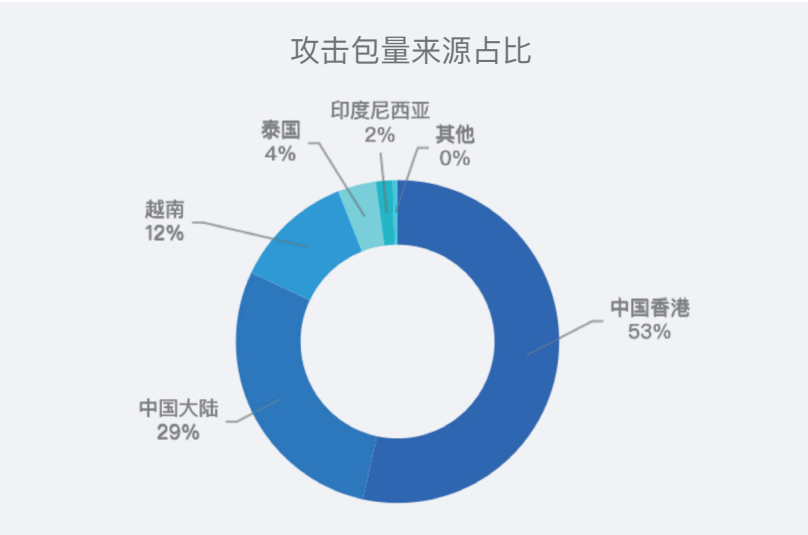
1. 流量蹿升极快，在基于秒级的检测告警中，大多数攻击第一波告警就达到攻击峰值。攻击流量超过接近 100G，由于攻击包均为小包攻击，攻击包量峰值达到 8168 万 pps。	**对抗策略：** 基于高性能计算平台开发打造检测和防护系统，持续不断优化硬件性能和算法效率。同时，在多台设备实现动态负载均衡和冗余备份，分散防护系统的压力。
2. 攻击手法为混合型攻击，攻击流量以 SYN flood 为主和 RST flood 为主，伴随少量的 UDP flood 攻击。但是在不同的攻击波次，攻击手法也会有变化。	**对抗策略：** 引入自学习自适应的启发式算法，实时动态提取攻击特征，调取相应的防护策略进行自动防护。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

3. 攻击流量来源与客户的业务流量来源重合。据分析，本次攻击的攻击来源有中国香港、中国大陆以及东南亚的越南、泰国、印度尼西亚等区域，与客户的主要业务流量来源重合，无法通过地域封禁或丢弃等策略进行防护。

对抗策略：
对于基于 IP 的传统策略无法覆盖的场景，需要引入基于 IP 画像、行为模式分析的 AI 防护算法，以及依据海量数据训练的模型，实现智能对抗。



腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

案例三：僵尸网络扫段攻击，监测防护实时联动

根据腾讯云 T-Sec DDoS 防护团队的监测数据，9 月 27 日 BillGates 僵尸网络活动异常活跃。通过分析发现，该僵尸网络发起了一系列大规模扫段攻击，共涉及 4 个运营商，超过 100 个 C 段，也就是短短 1 天之内，僵尸网络对超过 3 万个 IP 发起了攻击，手法为 UDP flood 攻击。

腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

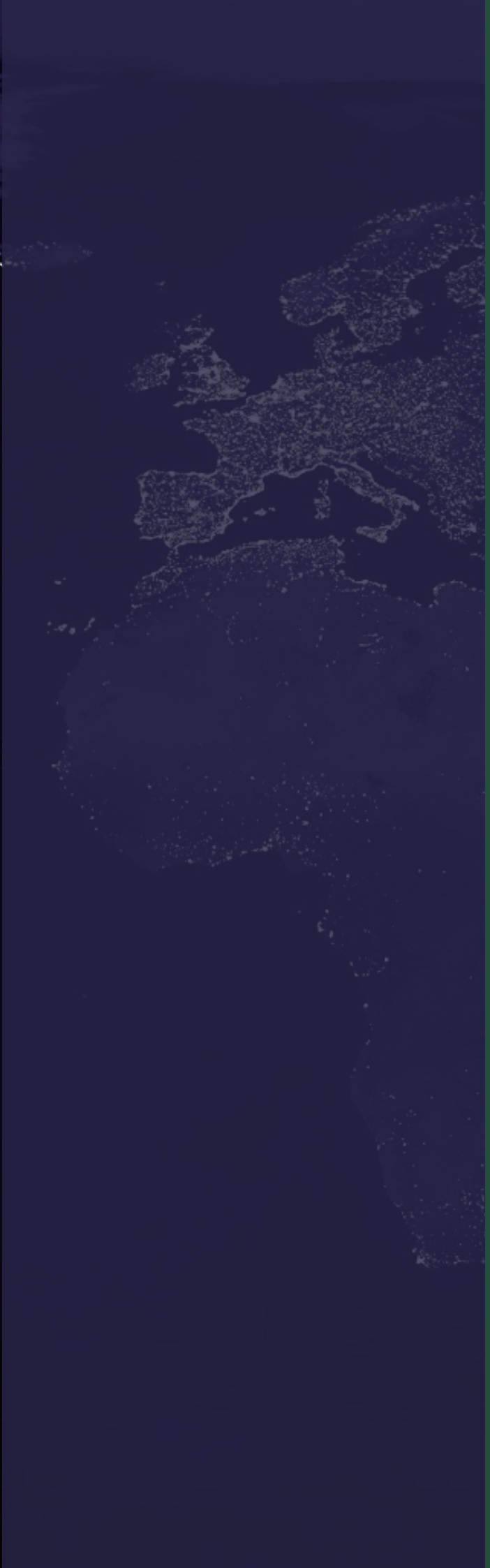
而在 11 月份，腾讯云 T-Sec DDoS 防护团队也监测到多起扫段攻击与 Mirai 等僵尸网络有关：为了获取到存在 GitLab 漏洞的主机，这些僵尸网络的肉鸡频频发起网段扫描：单个 IP 的扫描流量达到数十 M 乃至上百 M，同时扫描数个乃至十几个 C 段，同一时刻并发扫描的流量超过 10G。由于扫描过于暴力，这类扫描演变成了针对网络的扫段攻击。

腾讯云、绿盟科技 2021 年全球 DDoS 威胁报告

腾讯云 T-Sec DDoS 防护团队监测到一次典型的扫描型扫段攻击，一个来自欧洲的 IP，在短短 5 分钟内，对超过 800 个 IP 发起了扫描性扫段攻击。攻击由欧洲的一个 IP 发起，每个 IP 的攻击时间持续很短，仅有不到 10 秒的时间，攻击类型为 SYN flood 攻击，尽管单个 IP 的攻击流量不足 50M，但是由于同时扫描的 IP 都在数百个甚至上千个，因此攻击的总流量最高超过 20G。

防护难点及解决方案：

1. 扫段攻击发生时被攻击 IP 变化迅速，部分 IP 上的攻击持续时间仅有数秒，但是流量却迅速增长到上百 G，如果检测系统和防护系统的延迟较大，就会导致大量攻击流量透传到后端网络，危及整个机房的业务可用性。部分攻击持续时间短至数秒，DDoS 防护系统需要做到实现秒级检测和秒级清洗，否则很容易出现攻击实际已经结束、系统仍未检测到攻击的情况，导致攻击漏检以及防护透传。	**对抗方案：** 基于高性能计算平台开发打监测和防护系统，持续不断优化硬件性能和算法效率，实现秒级检测，秒级防护，监测防护系统实时联动。
2. 虽然部分扫段式攻击整体流量高达数十 G，对机房网络危害极大，但单个 IP 流量很小，容易绕过检测系统阈值，造成漏检漏防。	**对抗方案：** 检测系统需要针对扫段式攻击进行精细化检测，需要覆盖单个 IP 低至数 M 的扫段攻击，避免漏检漏防。
3. 短期内大量 IP 被密集攻击，导致大量业务 IP 触发清洗，不仅防护设备在攻击流量和业务双重重压下易引发高负载问题，业务流量也会增加额外的访问延迟。	**对抗方案：** 检测和防护系统需要有多台设备实现动态负载均衡和冗余备份，避免在扫段攻击场景下出现防护设备性能问题影响业务。同时针对扫段攻击场景，对扫段攻击场景中的防护逻辑进行了优化，提升加保护和去保护的效率。优化防护算法，让算法对用户正常业务更友好，避免给攻击期间或者攻击结束后的给业务 IP 带来额外的延迟。



第六章：全球 DDoS 大事记

Global DDoS Events

1 全球 DDoS 大事记

2021 年 1 月

- 由于比特币价格飙涨，国外黑客团伙大肆发起以 DDoS 攻击为手段的敲诈勒索活动，造成全球 DDoS 攻击活动大幅增加，也大幅提高了敲诈勒索金额，单次勒索的数额甚至高达 10 枚 BTC，折合人民币超过 300 万元。

- 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 依然没有避免大范围服务停运的结果。

- 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，但从实际监控来看，并未真正实施 DDoS 攻击，勒索者模仿流行攻击团伙名称，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，才让虚假勒索有可乘之机。

- 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 放射放大攻击，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。

2021 年 2 月

- 春节期间，包括腾讯云在内的多家厂商检测到 DDoS 攻击活动同比往年大幅增加。据腾讯云 T-Sec DDoS 防护团队数据表明，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。

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。

- Avaddon 勒索软件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 攻击已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。

2021 年 7 月

- 腾讯云 T-Sec DDoS 防护团队为腾讯云客户成功防护一次最大攻击流量为 1.26Tbps 的 DDoS 攻击，这也是今年腾讯云防护的最大的一次 DDoS 攻击。

2021 年 8 月

- 微软云服务 Azure 的某欧洲客户遭遇了峰值 2.4Tbps 的 DDoS 攻击，攻击者调动了分布在马来西亚，越南，中国台湾，日本，中国大陆，美国等地区的约 7 万个攻击源，攻击持续约 10 分钟。

2021 年 11 月

- 11 月 4 日负责谷歌 DDoS 防御的云安全可靠性工程师 Damian Menscher 最近披露，有攻击者正在利用 GitLab 托管服务器上的安全漏洞来构建僵尸网络，并发起规模惊人的分布式拒绝服务攻击（DDoS）。其中一些攻击的峰值流量，甚至超过了 1 Tbps。

- 11 月 13 日，Cloudflare 宣布防护了一次峰值攻击流量接近 2Tbps 的超大流量 DDoS 攻击。

腾讯安全 | NSFOCUS

腾讯云DDoS防护

绿盟科技国际业务