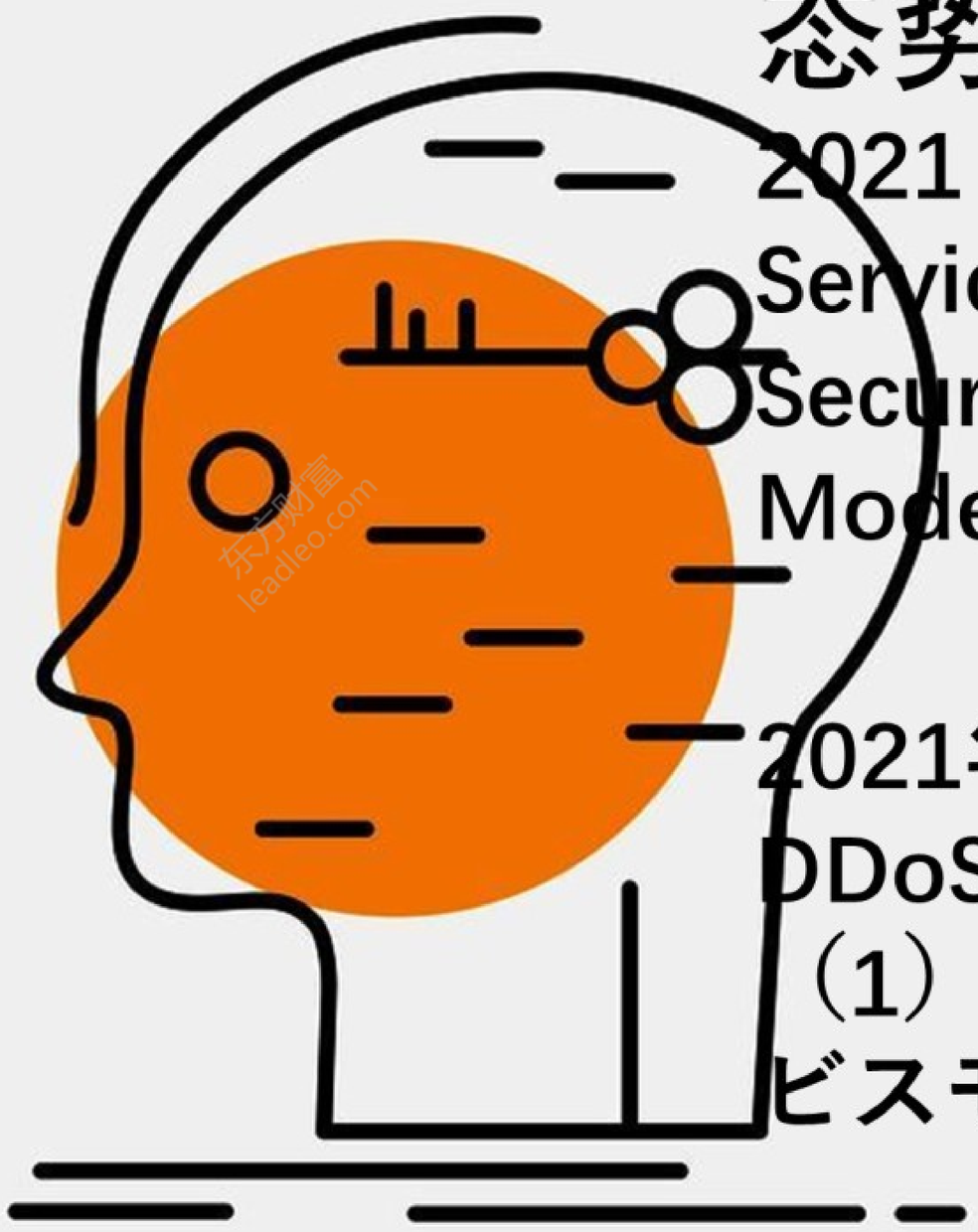
2021年 中国云抗DDoS服务系列报告（一）：DDoS安全态势与服务模式

2021 China Cloud Anti-DDoS Service Report Series (1): DDoS Security Situation and Service Model

2021年の中国のクラウドアンチDDoS攻撃サービス報告書シリーズ（1）：DDoS攻撃治安状況やサービスモデル



报告标签：IPV6、云抗Ddos服务、云安全

头豹研究院简介

- 头豹研究院是中国大陆地区首家**B2B模式人工智能技术的互联网商业咨询平台**，已形成集**行业研究**、**政企咨询**、**产业规划**、**会展会议**行业服务等业务为一体的一站式行业服务体系，整合多方资源，致力于为用户提供最专业、最完整、最省时的行业和企业数据库服务，帮助用户实现知识共建，产权共享
- 公司致力于以优质商业资源共享为基础，利用**大数据**、**区块链**和**人工智能**等技术，围绕**产业焦点**、**热点**问题，基于**丰富案例**和**海量数据**，通过开放合作的研究平台，汇集各界智慧，推动产业健康、有序、可持续发展

300+
资深分析师和研究员

2,500+
细分行业进行深入研究

1万+
注册机构用户
公司目标客户群体覆盖率高，PE/VC、投行覆盖率达80%

25万+
数据元素

50万+
行业专家库

四大核心服务

企业服务

为企业提供**定制化报告**服务、**管理咨询**、**战略**调整等服务

云研究院服务

提供行业分析师**外派驻场**服务，平台数据库、报告库及内部研究团队提供技术支持服务

行业排名、展会宣传

行业峰会策划、**奖项**评选、行业**白皮书**等服务

园区规划、产业规划

地方**产业规划**，**园区**企业孵化服务

报告阅读渠道

- 1、头豹科技创新网 —— www.leadleo.com PC端阅读全行业、千本研报

- 2、头豹小程序 —— 微信小程序搜索“头豹”、手机扫上方二维码阅读研报

- 3、添加右侧头豹研究院分析师微信，邀您进入行研报告分享交流微信群

图说

表说

专家说

数说

扫一扫

实名认证行业专家身份

详情咨询

客服电话

400-072-5588

南京

杨先生： 13120628075

唐先生： 18014813521

上海

王先生： 13611634866

李女士： 13061967127

深圳

李先生： 18916233114

李女士： 18049912451

概览摘要

中国DDoS攻击态势严峻，云端抗D如何发展？

DDoS攻击(分布式拒绝服务攻击）是指依靠客户与服务器技术将多台计算机（又称“肉鸡”）联合操控以形成规模化的攻击平台，进而对单或多攻击目标发起成倍杀伤力的网络攻击。

从威胁态势看，2019年后国家网络安全监管趋严，“净网2020”等专项整治和打击下，相较于2017与2018年，2019年后DDoS攻击次数及攻击流量均呈现双回落。但宏观来看，中国网络态势仍然严峻。2020年，中国受攻击目标占全球的72.8%，其中3-4成攻击源至海外。同时，IPV4地址耗尽、物联网设备的爆发性增长，DDoS防护难度随之增长，未来有望全面利好中国云抗DDoS服务发展。

01 中国云抗DDoS行业挑战与机遇并存

2019年后国家网络安全监管趋严， “净网2020”等专项整治和打击下，2019年后DDoS攻击次数及攻击流量均呈现双回落。随着5G商用进程的加速，DDoS攻击的可用宽带大幅增长，防护难度随之增长。未来，随着IPV4地址耗尽、物联网设备的爆发性增长，DDoS防护门槛及可用肉鸡规模预计将大幅提升。中国云抗DDoS行业挑战与机遇并存

02 DDoS攻击平台化与产业化带动攻击形态多样化

由于DDoS攻击成本低、并发量大、连续性高、致死率高、针对性强、损失巨大且影响深远等特点。同时，随着DDoS攻击的平台化、工具化与产业化，DDoS攻击种类也随之层出不穷。根据TCP/IP协议类型分类，自下至上，DDoS攻击可分为网络层攻击、传输层攻击、应用层攻击及混合型攻击四种

03 一线攻防团队，同时缩减攻击检测与攻击响应周期

云抗D服务可免去前期硬件设备采买投入与技术人员培训费用，直接与云平台共享硬件设备、网络带宽、技术专家运维等高成本资源，弹性按需收费、防御性价比可观。此外，云抗D服务提供一线攻防团队，实战经验丰富，大幅缩减攻击检测与攻击响应周期。同时，服务团队提供针对企业的持续安全策略调整，降低企业DDoS防御体系中的木桶效应。

目录

Contents

名词解释

- **DDoS：**denial-of-service attack，一种网络攻击手法，其目的在于使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问。
- **IPV4：**Internet Protocol version 4，一种无连接的协议，操作在使用分组交换的链路层（如以太网）上。此协议会尽最大努力交付数据包，意即它不保证任何数据包均能送达目的地，也不保证所有数据包均按照正确的顺序无重复地到达。这些方面是由上层的传输协议（如传输控制协议）处理的。
- **IPV6：**Internet Protocol version 6，网际协议的最新版本，用作互联网的协议。用它来取代IPv4主要是为了解决IPv4地址枯竭问题，同时它也在其他方面对于IPv4有许多改进。
- **骨干网：**计算机网络的一部分，它将各个网络相互连接起来，使得不同的局域网或子网之间能进行信息交换[1]。骨干网可以将同一建筑物内、校园环境中不同建筑物内或广大区域内的不同网络连接在一起。通常情况下，骨干网的容量要大于与其相连的网络容量。
- **肉鸡：**接入互联网受恶意软件感染后，受控于黑客的电脑。其可以随时按照黑客的命令与控制（C&C, command and control）指令展开拒绝服务（DoS）攻击或发送垃圾信息。通常，一部被侵占的电脑只是僵尸网络里面众多中的一个，会被用来去运行一连串的或远程控制的恶意程序。
- **物联网：**计算设备、机械、数字机器相互关系的系统，具备通用唯一识别码（UID），并具有通过网络传输数据的能力，无需人与人、或是人与设备的交互。

Chapter 1
宏观DDoS态势

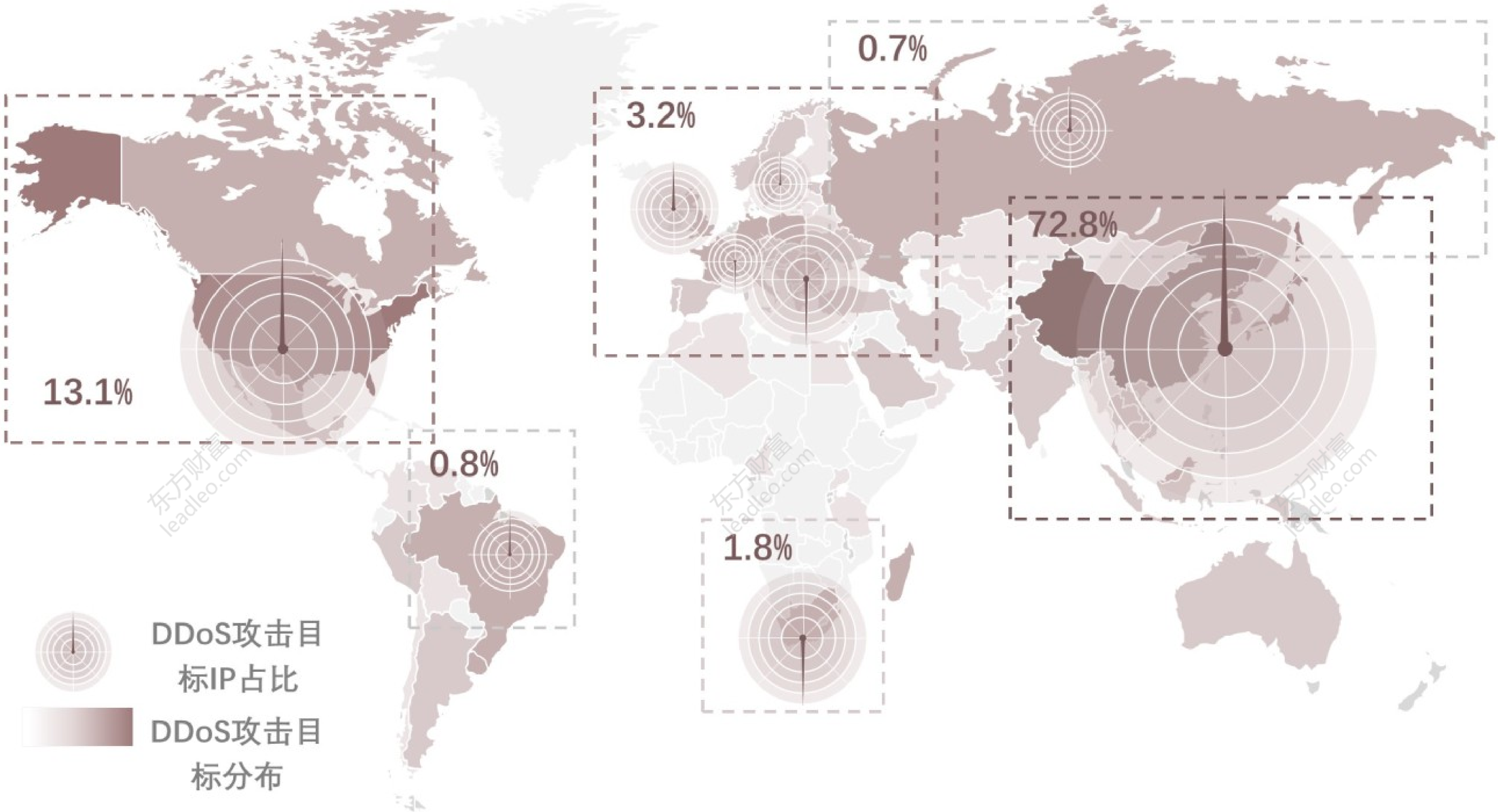
- DDoS攻击主要针对攻击目标系统弱点以耗尽其系统资源，进而其系统安全的核心可用性
- DDoS攻击平台化与产业化带动攻击形态多样化，主要可划分为网络层攻击、传输层攻击、应用层攻击、混合型攻击四种
- 中国网安态势态势严峻，国家监管力度趋严。但随着物联网设备的爆发性增长，未来中国云抗DDoS行业挑战与机遇并存
- 随着DDoS攻击黑灰产业链不断成熟，DDoS分工精细化、SaaS平台化程度持续加深，危害程度及影响范围同步增长

中国DDoS攻击态势——DDoS攻击基本定义

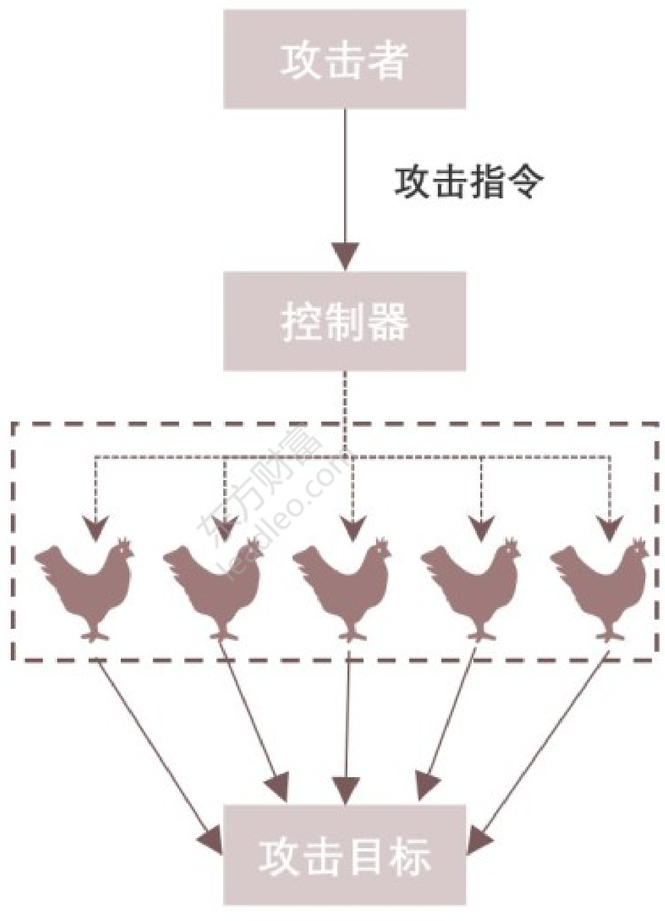
- DDoS攻击主要针对攻击目标系统弱点以耗尽其系统资源，进而其系统安全的核心可用性

全球DDoS攻击态势

全球DDoS攻击地理分布，2020年



传统DDoS攻击流程



DDoS攻击主要针对攻击目标系统弱点以耗尽其系统资源，进而其系统安全的核心可用性

DDoS攻击(分布式拒绝服务攻击）是指依靠客户与服务器技术将多台计算机（又称“肉鸡”）联合操控以形成规模化的攻击平台，进而对单或多攻击目标发起成倍杀伤力的网络攻击。不同于数据泄露与防护绕过，DDoS攻击的主要攻击目标为信息安全三大要素（保密性-Confidentiality、完整性-Integrity、可用性-Availability）中的可用性。

从全球网络安全现状看，2020年疫情下，中国仍是DDoS攻击的重灾区。根据头豹数据显示，中国受攻击目标IP占全球的72.8%，其中3-4成攻击源至海外，整体国家级网络安全态势严峻。

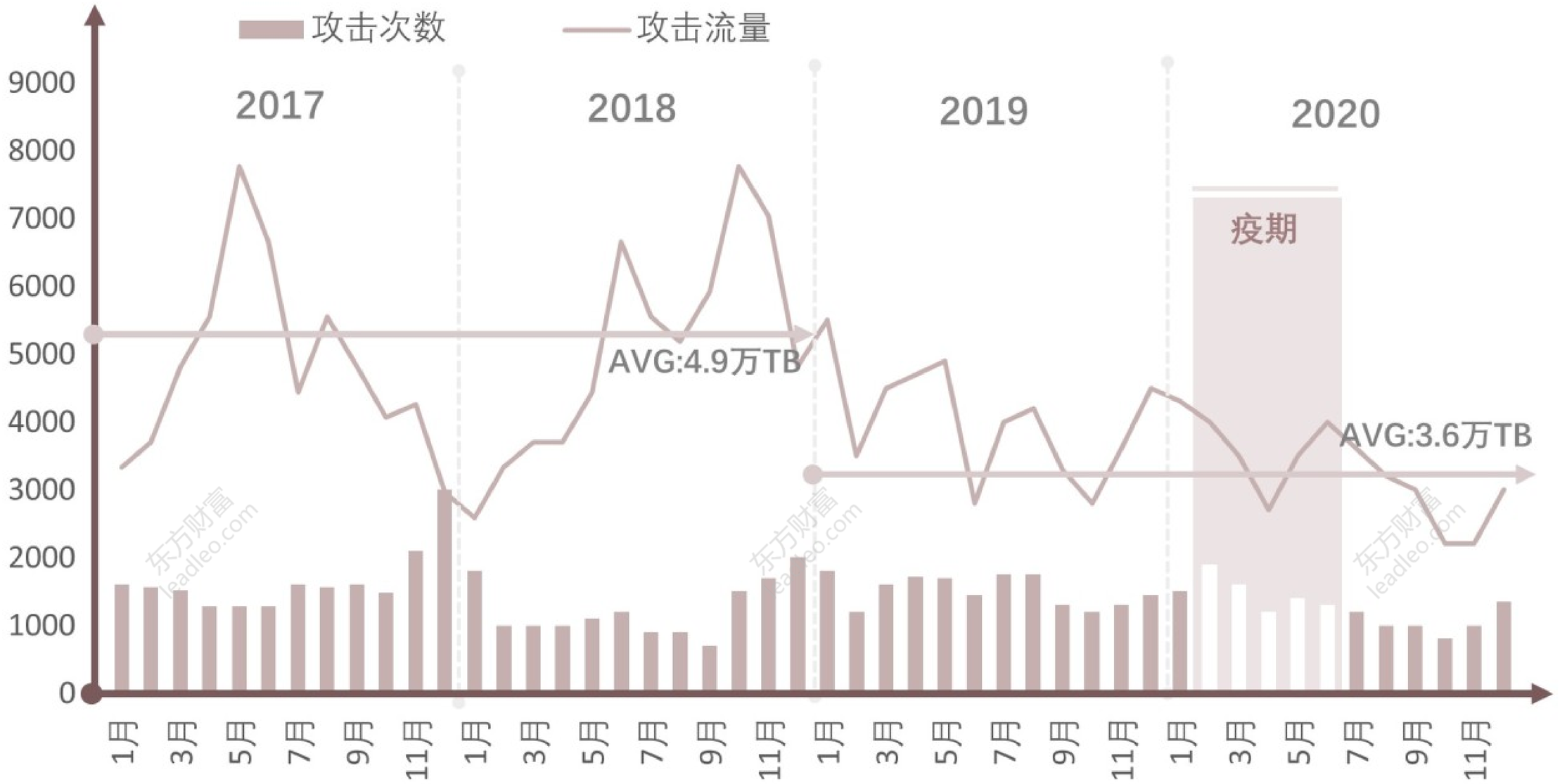
绿盟科技、中国电信云堤、头豹研究院

中国DDoS攻击态势——DDoS攻击频率与强度态势

- 中国网安态势态势严峻，国家监管力度趋严。但随着物联网设备的爆发性增长，未来中国云抗DDoS行业挑战与机遇并存

DDoS攻击频率与强度态势分析

DDoS攻击次数与流量峰值分布，2017-2020年

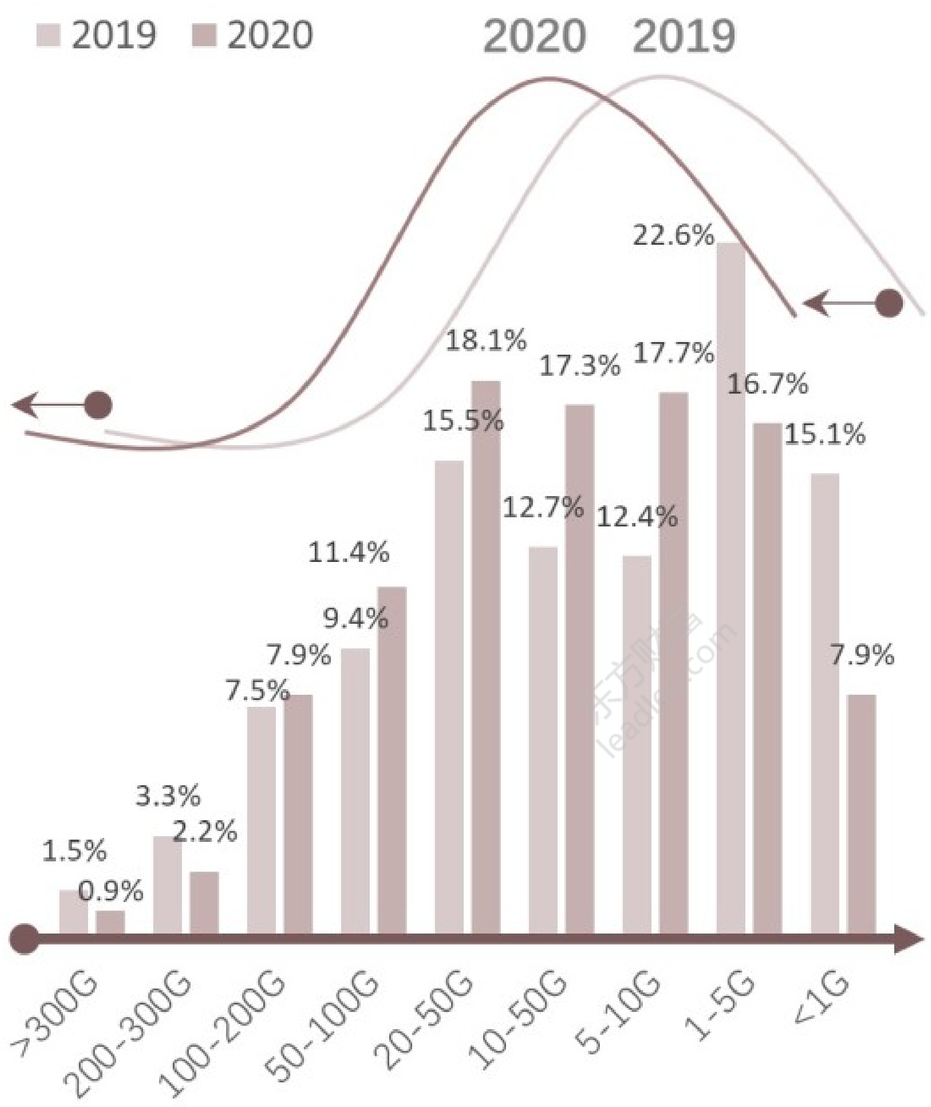


- **中国网安态势态势严峻，国家监管力度趋严。但随着IPV4地址耗尽、物联网设备的爆发性增长，未来中国云抗DDoS行业挑战与机遇并存**

回顾过去，2019年后国家网络安全监管趋严，“净网2020”等专项整治和打击下，2019年后DDoS攻击次数及攻击流量均呈现双回落。根据头豹数据显示，相较于2017年与2018年，2019年至2020年的年均攻击流量从4.9万TB下降至3.6万TB。

然而，在流量峰值分布方面，随着5G商用进程的加速，DDoS攻击的可用宽带大幅增长，防护难度随之增长。未来，随着IPV4地址耗尽、物联网设备的爆发性增长，DDoS防护门槛及可用肉鸡规模预计将大幅提升。中国云抗DDoS行业挑战与机遇并存。

DDoS攻击流量峰值分布，2020年



安全即服务（周凯）、CSDN、腾讯云、墨者盾、头豹研究院

中国DDoS攻击态势——DDoS攻击类型态势

- DDoS攻击平台化与产业化带动攻击形态多样化，主要可划分为网络层攻击、传输层攻击、应用层攻击、混合型攻击四种

DDoS攻击类型态势

DDoS攻击类型分析

	通讯层级描述	核心攻击目标	典型攻击手段
应用层攻击	■ ***层级效用：****涵盖应用层、表示层、会话层，分别负责为应用程序提供服务、数据格式转化与加密、会话建立与维护* ■ ***主要协议：****HTTP协议*	■ ***攻击形式：****基于HTTP协议等应用层协议攻击，整体较为复杂：攻击者需对应用层协议进行理解，应用用户行为模拟与用户界面交互的方式进行攻击；其攻击难以识别，攻击效果最佳，主要以每秒请求数来衡量攻击* ■ ***攻击目标：****耗尽应用资源*	■ *HTTP Flood Attack* ■ *DNS Query Flood Attack* ■ *Low & Slow Attack*
传输层攻击	■ ***层级效用：****传输层主要负责端到端连接的建立、管理与维护* ■ ***主要协议：***TCP协议、UDP协议	■ ***攻击形式：****基于 TCP、UDP等传输层协议进行攻击，并针对TCP、UDP等协议特点及弱点攻击，由每秒数据包为单位进行攻击测量* ■ ***攻击目标：****目标是占用服务器资源，或防火墙和负载平衡器的资源*	■ *TCP SYN Flood Attack* ■ *UDP Flood Attack* ■ *UDP-Based Amplification Attack*
网络层层攻击	■ ***层级效用：***网络层则是负责IP选址和路由选择 ■ ***主要协议：***IP协议、ICMP协议	■ ***攻击形式：****主要基于IP、ICMP网络层协议进行DDos攻击，网络层的攻击多偏向于流量攻击，通过每秒位数(Bps)为单位计算攻击量* ■ ***攻击目标：****占用带宽资源，致使服务器带宽资源饱和以实现站点无法使用*	■ *Ping Flood Attack* ■ *Ping of Attack* ■ *Smurf Attack*

❑ **2020年DDoS攻击平台化与产业化进一步带动攻击形态多样化，现主要可划分为网络层攻击、传输层攻击、应用层攻击、混合型攻击四种**

DDoS攻击与DoS攻击可追溯至1974年，沿用至今，已逐步成为（承接下文）

安全即服务（周凯）、CSDN、腾讯云、墨者盾、头豹研究院

（承接上文）较为普遍的网络攻击形式，这主要得益于DDoS攻击成本低、并发量大、连续性高、致死率高、针对性强、损失巨大且影响深远等特点。同时，随着DDoS攻击的平台化、工具化与产业化，DDoS攻击种类也随之层出不穷。根据TCP/IP协议类型分类，自下至上，DDoS攻击可分为网络层攻击、传输层攻击、应用层攻击及混合型攻击四种。

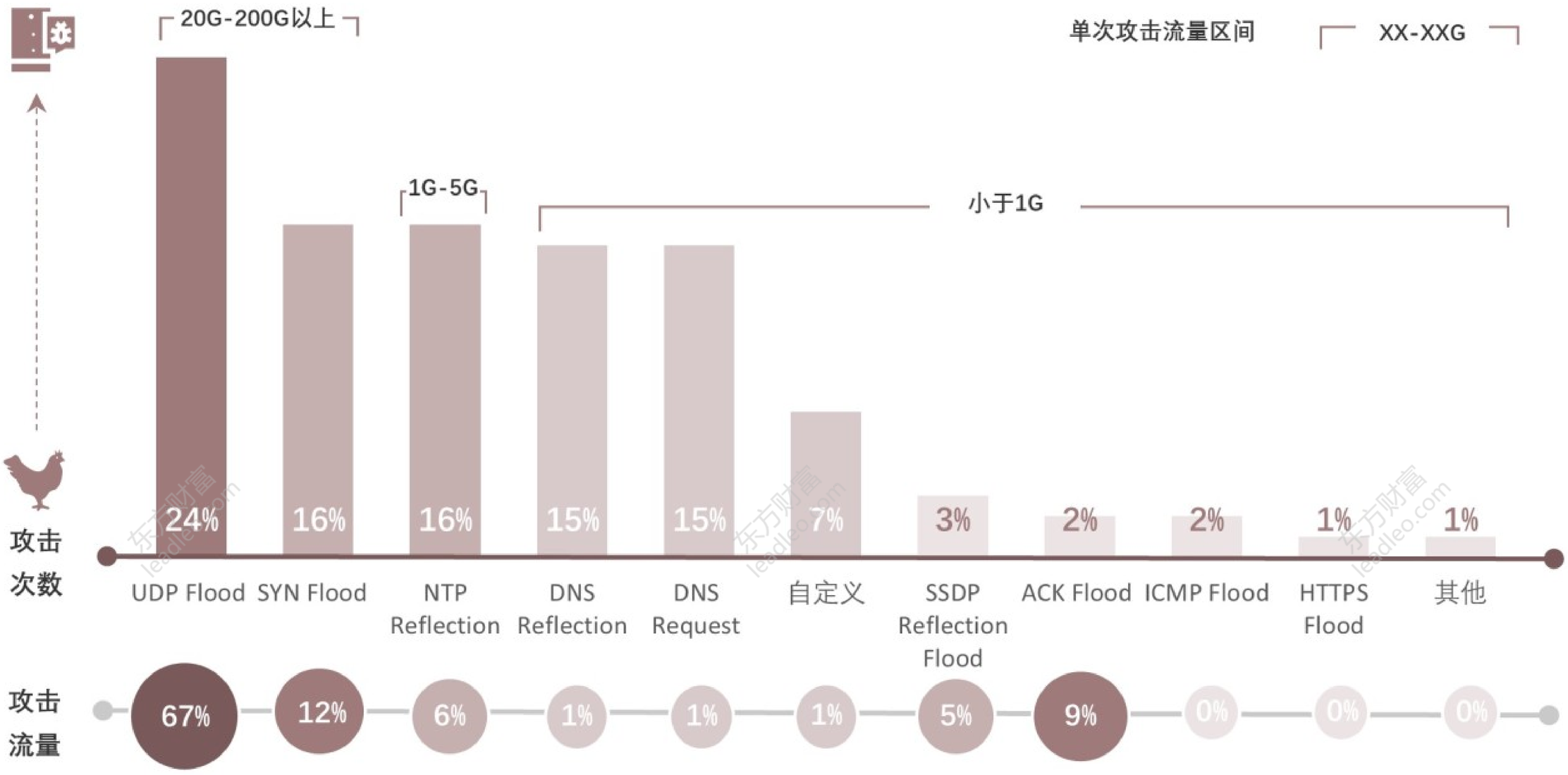
- 网络层攻击与传输层攻击应用程度较为广泛，其中UDP Flood与SYN Flood是2020年的主流攻击方式

网络层攻击与传输层攻击应用程度较为广泛，分别针对以IP、ICMP为代表的网络层协议与以TCP、UDP为代表的传输层协议进行DDoS攻击。较为不同的是，网络层攻击较偏向于流量型攻击手段，以快速拥堵带宽、耗尽服务器资源核心目的，从而实现目标站点业务不可用及关键服务中断。而传输层攻击则侧重于攻击TCP、UDP协议弱点以达到尽快消耗TCP连接等系统性资源的目的。

在应用表现方面，UDP Flood Attack与SYN Flood Attack两大2020年主流攻击方式均属于网络层/传输层DDoS攻击，但两者针对攻击的核心目标系统资源各异。SYN Flood Attack通过利用TCP连接请求响应系统性弱点（特点）并采用伪造IP地址，耗尽目标系统TCP连接资源，进而可导致服务器宕机及常规用户需求响应困难。如SYN Fllood Attack模式分析图所示，（承接下文）

DDoS攻击的攻击方式应用分析

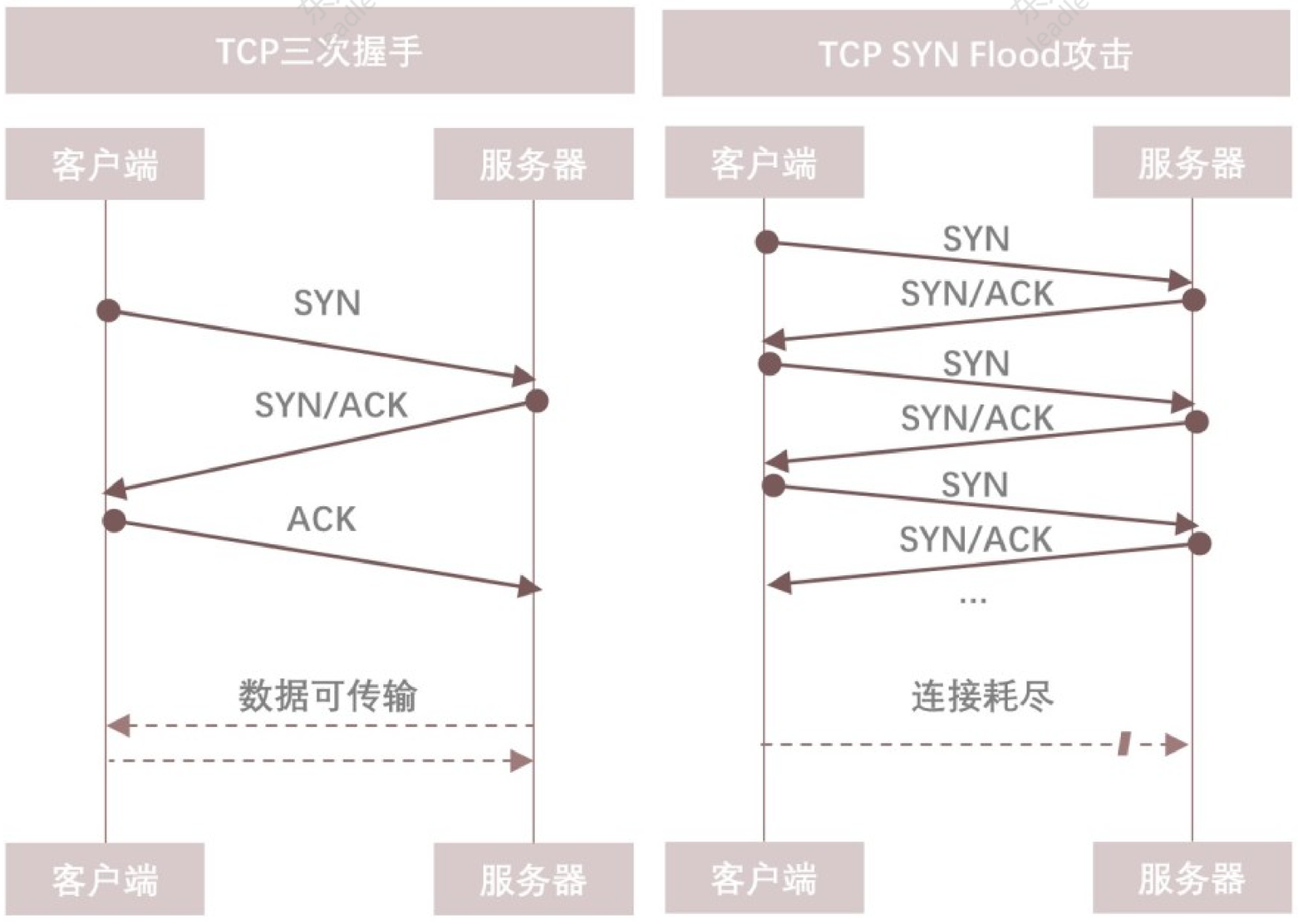
DDoS攻击方式与单次攻击流量区间分布，2020年



安全即服务（周凯）、CSDN、腾讯云、墨者盾、绿盟科技、中国电信云堤、极鹰云、火龙果软件、头豹研究院

DDoS攻击的主流攻击方式分析

SYN Flood Attack攻击模式分析



（承接上文）在非攻击情况下，用户端将向服务器端发送SYN连接请求，服务端接受请求后返还SYN/ACK响应消息，表示服务器已接受客户端连接请求。第三次客户端发送ACK响应请求，确认TCP三次握手连接成功。而攻击情景下，攻击者则是利用上述三次连接的核心系统缺陷：当第三次握手的过程中，攻击者将发送伪造地址，导致目标服务无法接收ACK响应请求，达到半开连接状态。同时服务器需记录未完成连接信息，指导连接建立。但由于半开连接数量及资源有限，若用户端连接过多时，半开连接列队资源将耗尽，进而导致服务器正常用户请求响应中止。

相较于SYN Flood Attack依托于TCP连接状态，UDP Flood Attack利用的UDP数据包属于无连接协议，主要通过利用现行工具向目标服务器快速发送大量源地址与报文内容伪造的UDP数据包于目标服务器。目标器接收伪造报文后将尝试对内容处理分析并检测目标应用端口。但当系统检测没有相应应用端口将向伪造IP地址发送发送错误信息以耗尽目标服务器资源，进而堵塞目标服务器网络网络，造成系统性拒绝服务。

从2020年中国整体攻击类型分布态势来看，UDP Flood Attack与SYN Flood Attack总攻击次数占比共计40%。同时两者均属于大流量型攻击，在100G以上的攻击中，UDP Flood Attack与SYN Flood流 Attack量占比超90%，是现有大流量攻击中的主流。

安全即服务（周凯）、CSDN、腾讯云、墨者盾、绿盟科技、中国电信云堤、极鹰云、火龙果软件、头豹研究院

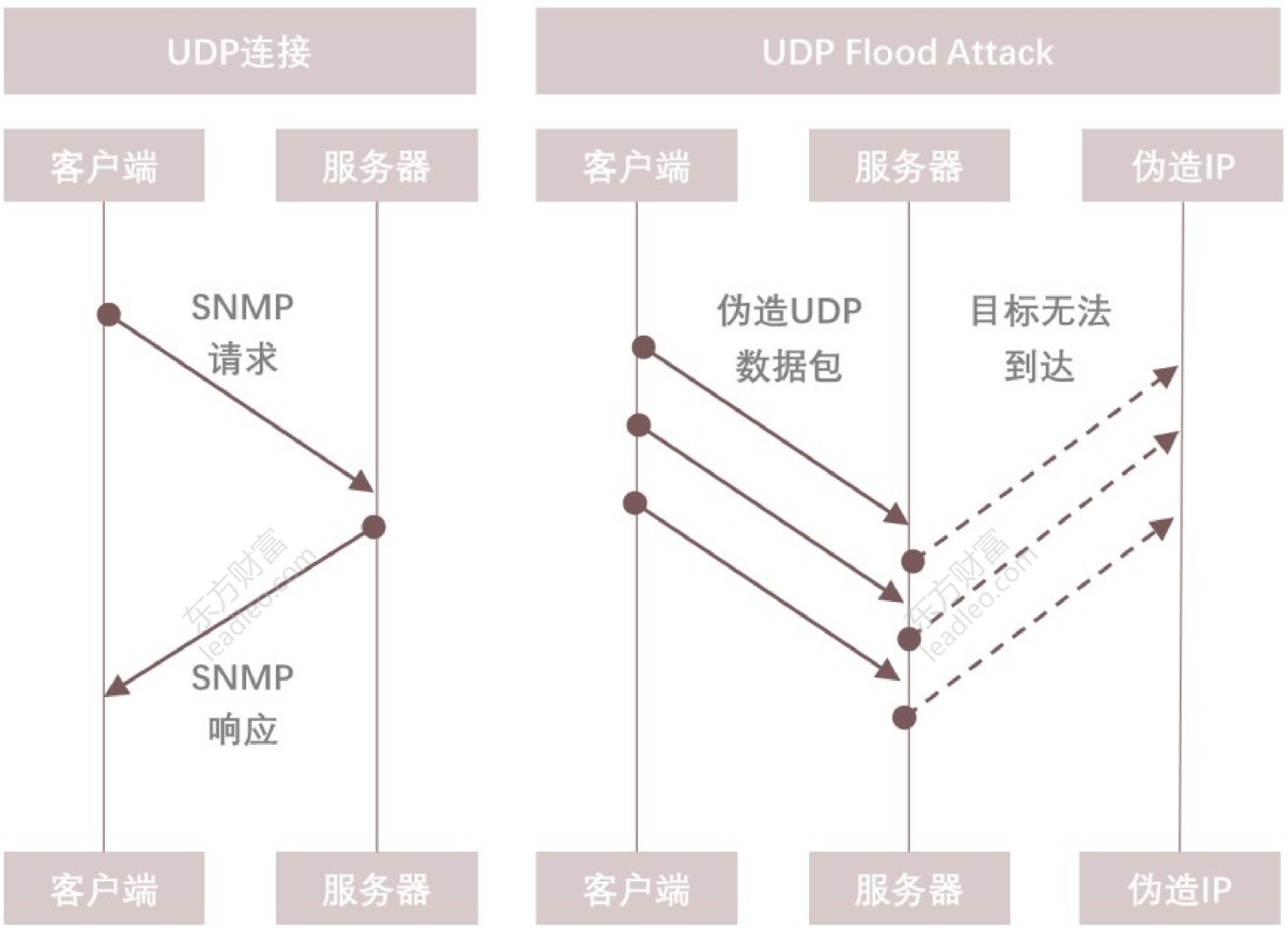
- 应用层攻击通常不需要大流量型攻击实现目标攻陷，主要通过对应用层协议进行理解，户行为模拟与用户界面交互发起DDoS攻击

而应用层攻击方面，应用层攻击通常不需要大流量型攻击实现目标攻陷，主要通过对应用层协议进行理解，并应用用户行为模拟与用户界面交互以实现崩溃Web服务器请求并针对OpenBSD、Windows等软件漏洞发起攻击。相较于网络层与传输层等中层协议攻击，应用层攻击针对上层协议，业务关联性更高，防御情况更为复杂，导致其识别与防御难度随之高，因此应用层攻击整体攻击效益最佳。其中，HTTP Flood攻击较为典型，主要以发起便利、防御困难、伤害持续性高著称。首先，HTTP攻击可摆脱肉鸡收集及控制过程中收集周期长、流量易识别、资源损耗快、攻击持续性低等弊端。HTTP攻击依靠端口扫描以寻求HTTP或SOCKS匿名代理；该类匿名代理资源丰富、收集时效性强，几日便可获取足量匿名代理，进而对攻击目标发起HTTP请求。其整体发起难度低、高强度攻击的维持性强。其次，HTTP Flood能够模仿常规用户行为，整体攻击识别难度高，同时具备对后端业务层逻辑及数据库服务的长效连锁打击效果。

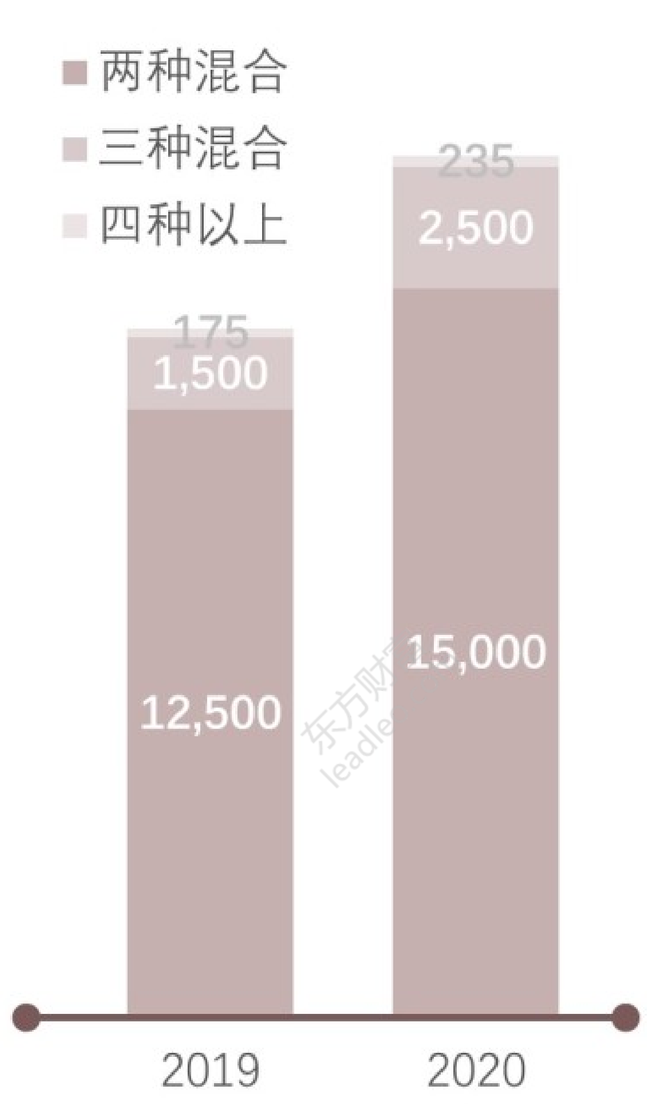
此外，相较单一攻击，混合型攻击将采用多种方式、手段和工具以寻求最佳攻击路径，是较为高阶攻击方式。从宏观攻击态势看，较之于2019年，2020年中国总攻击次数差异较小，但整体混合型攻击次数涨幅同比上涨26.1%。可见，短期内攻击方式多元化、混合化已成现攻击者攻击偏好趋势。

DDoS攻击的主流攻击方式分析

UDP Flood Attack攻击模式分析



DDoS混合攻击分布，2020年



安全即服务（周凯）、CSDN、腾讯云、墨者盾、绿盟科技、中国电信云堤、极鹰云、火龙果软件、头豹研究院

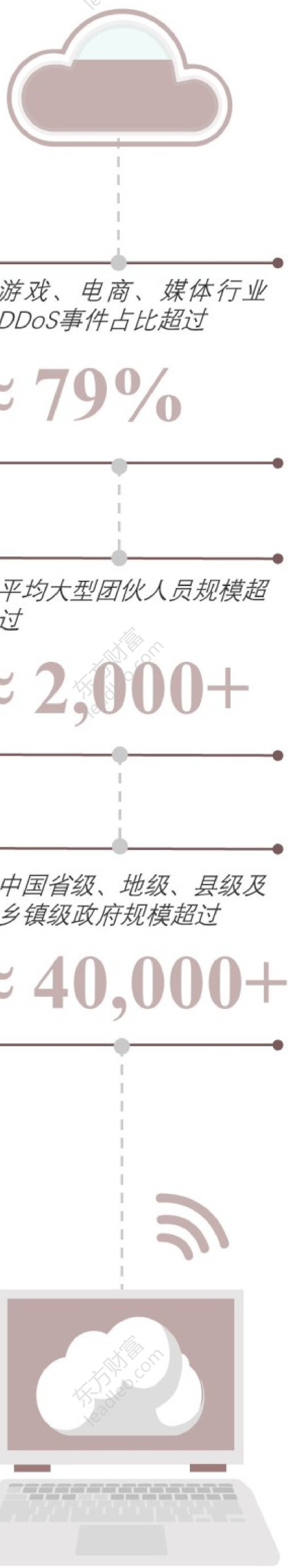
中国DDoS攻击态势——DDoS攻击黑灰产业分析

- 随着DDoS攻击黑灰产业链不断成熟，DDoS分工精细化、SaaS平台化程度持续加深，危害程度及影响范围同步增长

DDoS攻击黑灰产业分析

DDoS黑灰产业攻击链与防守链

YUNDUN、黑客技术、白云科技、云鼎实验室、REEBUF、中国电信云堤、绿盟科技、华为、头豹研究院



- 催化DDoS黑色产业体系成熟的核心底层动机主要表现为商业竞争、敲诈勒索、恶性报复三方面

在传统DDoS攻击流程中，攻击者需要根据攻击需求方（金主）的打击需求逐一完成软件开发、肉鸡集群、攻击工具部署、肉鸡控制、发起攻击等流程，但随着DDoS攻击黑灰产业链不断成熟，DDoS分工精细化、SaaS平台化程度持续加深，危害程度及影响范围同步增长。从需求侧的维度分析，催化DDoS黑色产业体系成熟的核心底层动机主要表现为三方面：

1) **商业竞争：**同业间恶意商业竞争是DDoS攻击黑灰产化的核心驱动。攻击需求方可通过即时通讯软件、电商平台、DDoS中介、SaaS平台等渠道雇佣攻击者，并对同业线上服务发起DDoS攻击；该手段可导致其同业线上业务频繁不可，大幅降低客户体验感，并造成关键客户流失、口碑受损，进而达到其恶性行业竞争目的。从攻击态势分布上看，恶性竞争为主要驱动的DDoS攻击事件集中于游戏、电商、媒体等即时性强、侧重客户体验感、产品多元替代性强的行业。根据华为未然实验室数据显示，2020年全球DDoS攻击事件中，游戏、电商、媒体行业DDoS事件占比超过79%。

2) **敲诈勒索：**敲诈勒索型DDoS攻击通常由专业组织及大型团伙发起，通过要挟企业支付相应敲诈勒索费以避免团伙针对企业业务高峰期和重大事件节点对其业务发起DDoS攻击。该类组织团伙多藏匿于海外，组织规模大。根据绿盟科技威胁情报中心数据显示，绿盟2020年发现的活跃团伙中，平均团伙规模超过2000以上。同时团队与组织内软件、财务、攻击、后勤等环节分工明确，组织能力强、流程化程度高。此外，大型团伙与专业组织的DDoS攻击技术突出、IDC与物联网等攻击资源丰富，主要针对发展暂处于成长关键期、IT资源及防护能力均存在上升空间的企业。

3) **恶性报复**：不同于前两大动机均为经济利益导向，恶性黑客DDoS事件具备相应政治导向性，多发于具备信息开放性质与公众性质的党务、政务、高校及公共社会组织；其核心目的在于篡改公开网页内容，迎合热点发布相关虚假恶意言论以煽动社会情绪。同时随着政府信息公开化进程演进，恶意报复型DDoS攻击预计将呈现加剧态势。

YUNDUN、黑客技术、白云科技、云鼎实验室、REEBUF、中国电信云堤、绿盟科技、华为、头豹研究院

- 服务模式与DDoS攻击服务相结合，进而形成一站式的标准化、自动化、平台化的服务体系及成熟的服务流程

服务模式与DDoS攻击服务相结合，进而形成一站式的标准化、自动化、平台化的服务体系及成熟的服务流程。相较于传统DDoS攻击流程，攻击需求方可免去DDoS攻击的爆破、下载、连接等渗透阶段，直接登录网页端并通过平台线上支付系统，在网页端快速完成DDoS攻击的购买与交付；该模式不仅降低了DDoS攻击的操作复杂度及技术门槛，同时资金回流及攻击效益得以双向提升。

- DDoS攻击服务采取分级定价模式可符合各型客户的需求，进而避免固定定价导致的客户流失及利润缩减

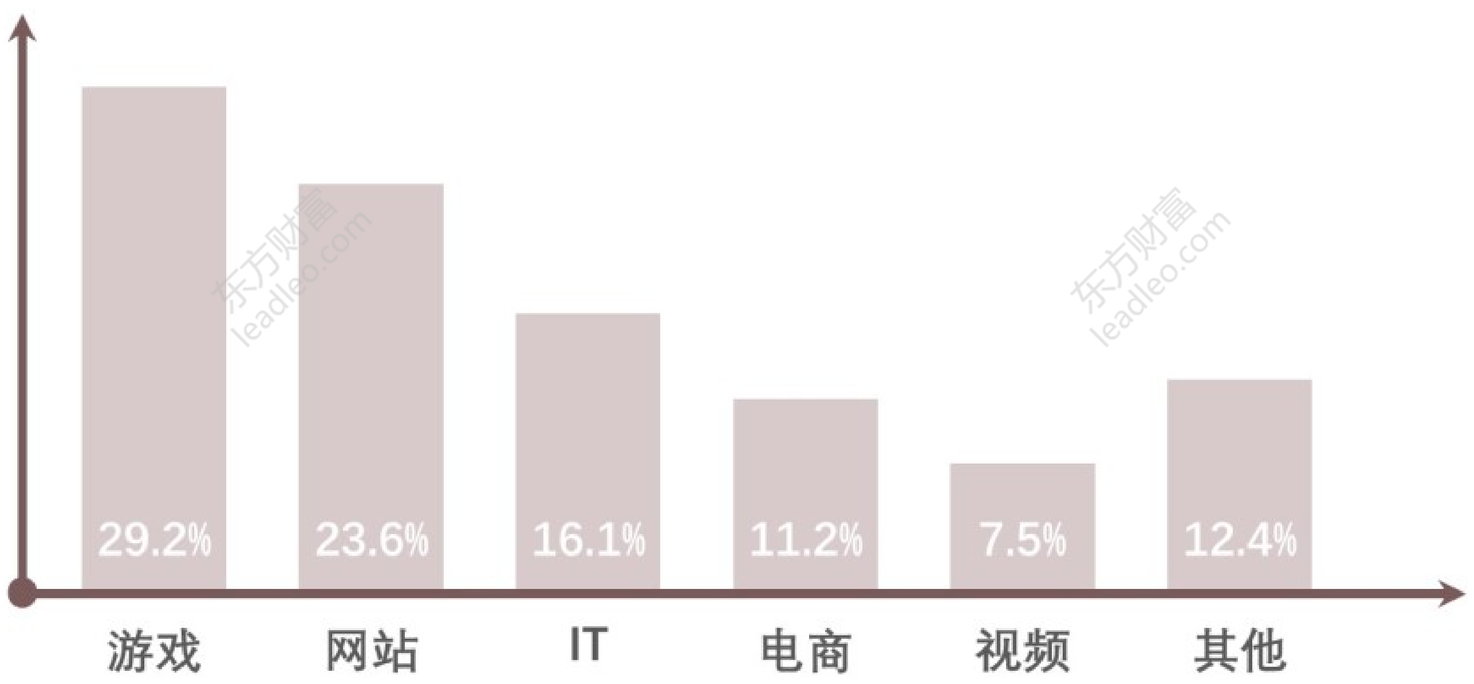
在定价策略上，DDoS攻击服务与部分互联网产品模式类似，主要采取分级定价模式：根据攻击需求方所需DDoS攻击并发量、攻击时长、日均攻击次数、标准洪流等诉求差异提供阶梯型服务包，可符合各型客户的需求，进而避免固定定价导致的客户流失及利润缩减。

此外，DDoS攻击服务同时提供单次攻击及包月攻击服务。单次攻击价格区间于200至300元人民币不等。相较于单次攻击收费模式，包月攻击费用模式在800元至1500元之间，整体价格较高，但换算单次攻击费用不到2元；该策略的核心目的在于透过包月服务的价效比增加现有客户的消费粘性，进而稳定DDoS平台的资金回流，利好平台服务者的长期收益。

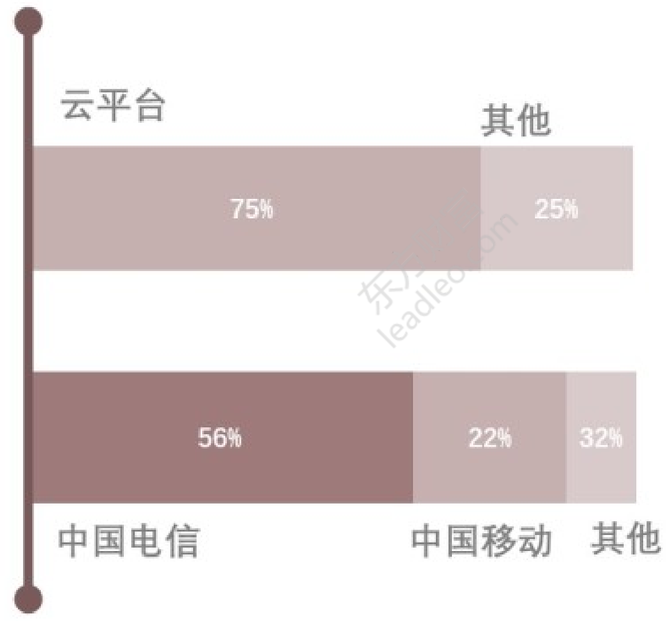
而在受害者方面，根据华为未然实验室及头豹研究院数据显示，游戏、门户网站、IT、电商等行业是DDoS攻击的重灾区。2020年疫情下，随着宅经济模式转型，未来侧重客户体验感、即时性强的泛娱乐行业DDoS攻击集中度预计将整体上升。

DDoS目标受害者分析

DDoS攻击直接受害者



DDoS攻击间接受害者



YUNDUN、黑客技术、白云科技、云鼎实验室、REEBUF、中国电信云堤、绿盟科技、华为、头豹研究院

中国DDoS攻击态势——DDoS攻击通用防护

- 面临日渐严峻的DDoS攻击态势，攻击防御方可采取的DDoS的通用防御手段大致可划分资源扩容、硬件抗D与云抗D三种

DDoS攻击通用防护

DDoS攻击通用防护手段方案效益分析

防护手段价值密度

通用抗D方案种类

	资源扩容	硬件抗DDoS	云抗DDoS
方式	可直接扩容带宽、升级服务器等目标攻击资源，扩大资源饱和上限	直接在企业客户互联网接入边界直接部署硬件ADS抗DDoS设备。通过设备进行流量监测，并将可疑攻击流量牵引至清洗设备进行清洗回注	云抗DDoS是基于云原生部署的虚拟化一站式抗DDoS服务；其模式大致可划分为基于硬件云抗DDoS与基于CDN的云抗DDoS
优势	操作方便简单	具备相应防护与清洗能力	零部署、运维简单；按需收费、弹性防护、综合费用低廉、防护价效比高；专业抗D团队、DDoS攻击快速响应
劣势	防御无目的性；盲目资源扩容费用高昂、价格效比弱；面对大规模攻击，资源饱和难题难以解决	硬件抗D设备仍然受限于企业带宽，难以抵御超过带宽上限的攻击；部署复杂，运维难度高；数据分析能力有限、误杀漏杀概率高、安全策略持续性低	在公有云部署中，流量数据需经过公有云清洗中心、数据高防中心、CDN节点，数据的绝对机密性与封闭性难以保障。而私有云抗D平台搭建费用高昂、后期带宽投入大，综合成本高，部分企业机构预算有限，难以实现私有部署落地。

- 面临日渐严峻的DDoS攻击态势，攻击防御方可采取的DDoS的通用防御手段大致可划分资源扩容、硬件抗D与云抗D三种

安全即服务（周凯）、网宿科技、头豹研究院

面临日渐严峻的DDoS攻击态势，攻击防御方可采取的DDoS的通用防御手段大致可划分为三种：

1) **资源扩容：**由于DDoS攻击的本质是攻击信息网络安全的可用性，因此其攻击方式主要针对于耗尽目标系统计算、存储、带宽等资源。直接扩容相关资源以提高资源饱和上限是最为简单便利的方式。但是该防御方式无针对性。同时盲目资源费用高昂，仍旧难以抵抗大规模DDoS攻击，整体防御价效比弱。

2) **硬件抗DDoS设备：**硬件抗DDoS属于传统型抗D防御方式，可通过硬件抗D设备进行流量监测，并将可疑攻击流量牵引至清洗设备进行清洗与回注。但当攻击流量超过互联网接入的带宽容量，硬件防护能力骤降。而面对小流量攻击时，传统硬件抗D防护也面临部署复杂、部署运维费用高昂、防御务杀漏杀概率高、安全策略效益与可持续性等痛点。

3) **云抗DDoS服务：**不同于传统硬件抗D，云抗D服务客户可免去前期硬件设备采买投入与技术人员培训费用，直接与云平台共享硬件设备、网络带宽、技术专家运维等高成本资源，弹性按需收费、防御性价比可观。此外，云抗D服务提供一线攻防团队，实战经验丰富，大幅缩减攻击检测与攻击响应周期。同时，服务团队提供针对企业的持续安全策略调整，降低企业DDoS防御体系中的木桶效应。

- 相较于硬件部署与资源扩容，云抗DDoS服务在防护价效比、运维团队防护与响应专业性、综合定制化安全防护策略及安全架构等维度优势显著。

纵观三种通用防护方式，以云清洗为代表的云抗DDoS商用防护是市场较为主流且重要的防护方式之一。相较于硬件部署与直接资源扩容。云抗DDoS服务在防护价效比、运维团队防护与响应专业性、综合定制化安全防护策略及安全架构等维度优势显著，是游戏、电商、政府、金融等行业客户的优先选择方案。

从行业内厂商分类及玩法的维度分析，云抗DDoS市场玩家主要涵盖云平台服务商、网络营运商、传统安全企业及CDN服务商四类。由于四类玩家基础资源、行业经验、技术累积、资源投入等相对优势各异，其云抗DDoS服务的服务形态、底层技术、标的客群存在差异。但整体来看，抗DDoS行业抗D竞争核心将仍集中于带宽资源及抗D技术两大维度。

安全即服务（周凯）、网宿科技、头豹研究院

Chapter 2

云抗D服务模式

- 就短期而言，传统安全服务商与网络营运商的云抗DDoS服务主要依托于硬件，整体防护手段及目标客群存在差异
- 网络营运商主要通过与本地网络安全服务商合作，采购清洗设备并搭建与运营商私有云平台，进而提供的以硬件为基础的营运商云清洗服务
- 云服务商云抗DDoS服务模式基于CDN技术：可通过在互联网内设置数个缓存代理节点，并将用户访问请求导向缓存节点进而稀释DDoS攻击

中国云抗DDoS服务模式——传统安全商与网络营运商

就短期而言，传统安全服务商与网络营运商的云抗DDoS服务主要依托于硬件，整体防护手段及目标客群存在差异

云抗DDoS服务模式	模式描述	模式优势	模式痛点
传统安全模式	■ *模式搭建：前期通过硬件抗DDoS设备搭建节点，依靠流量牵引方式将攻击流量牵引至安全厂商的远端机房，进行流量清洗。随之节点规模的累积，未来目标向CDN技术方向发展* ■ *主要防护：云清洗、专家运维* ■ *核心目标客群：政府部门、基础建设、金融、本地运营商*	■ *综合抗D：通过硬件抗DDoS起步，具备专业抗DDoS团队，其技术架构、交付流程较成熟，在DDoS攻击处理效率、准确性经验丰富。整体检测能力强，具备全协议支持能力。其中对应用层攻击的清洗效果相对较好* ■ *客户资源：安全厂商深耕抗DDoS行业多年，政务、营运商、金融等大客户关系良好，较易形成投标过程中的优势。同时客户整体支付能力相对较高，可盈利空间大。*	■ *节点规模：现阶段而言主要的传统安全商云清洗服务仍依赖其硬件搭建的安全清洗中心，节点搭建规模及成熟度等维度存在上升空间。* ■ *CDN技术投入高：以绿盟为代表的安全企业目标向CDN技术发展，但服务器、带宽等投入高，年均花费达上亿级别*
营运商模式	■ *模式搭建：通过购买安全厂商硬件设备，并部署于其私有云中心搭建抗D平台* ■ *主要防护手段：流量预压制、BGP高防、攻击流量过滤* ■ *核心目标客群：大型互联网公司、IDC、二级SP、大型央国企专线网络客户*	■ *全网检测：利用核心网路由器数据进行流量检测，可对经过营运商大网任意互联网目标IP进行在线实时流量监控，监控覆盖面广，大流量规模测度准确性高* ■ *近源防护：准确分辨攻击来向，调度IP承载网路由器和流量清洗设备将攻击流量在最近节点上对攻击流量的进行清除* ■ *攻击溯源：了解骨干网所有网络资源位置，不依赖探针与IP归属映射，溯源能力强*	■ *单线BGP：营运商更偏向于其营运商自身机房内的流量攻击清洗，若涉及跨营运商，可用带宽相对较小、肉鸡流量清洗难度高* ■ *抽样检测：数据检测基于Netflow抽样，以慢速攻击代表的低流量攻击的检测效果较差*

❑ 网络营运商主要通过与本地网络安全服务商合作，采购清洗设备并搭建与运营商私有云平台，进而提供的以硬件为基础的营运商云清洗服务

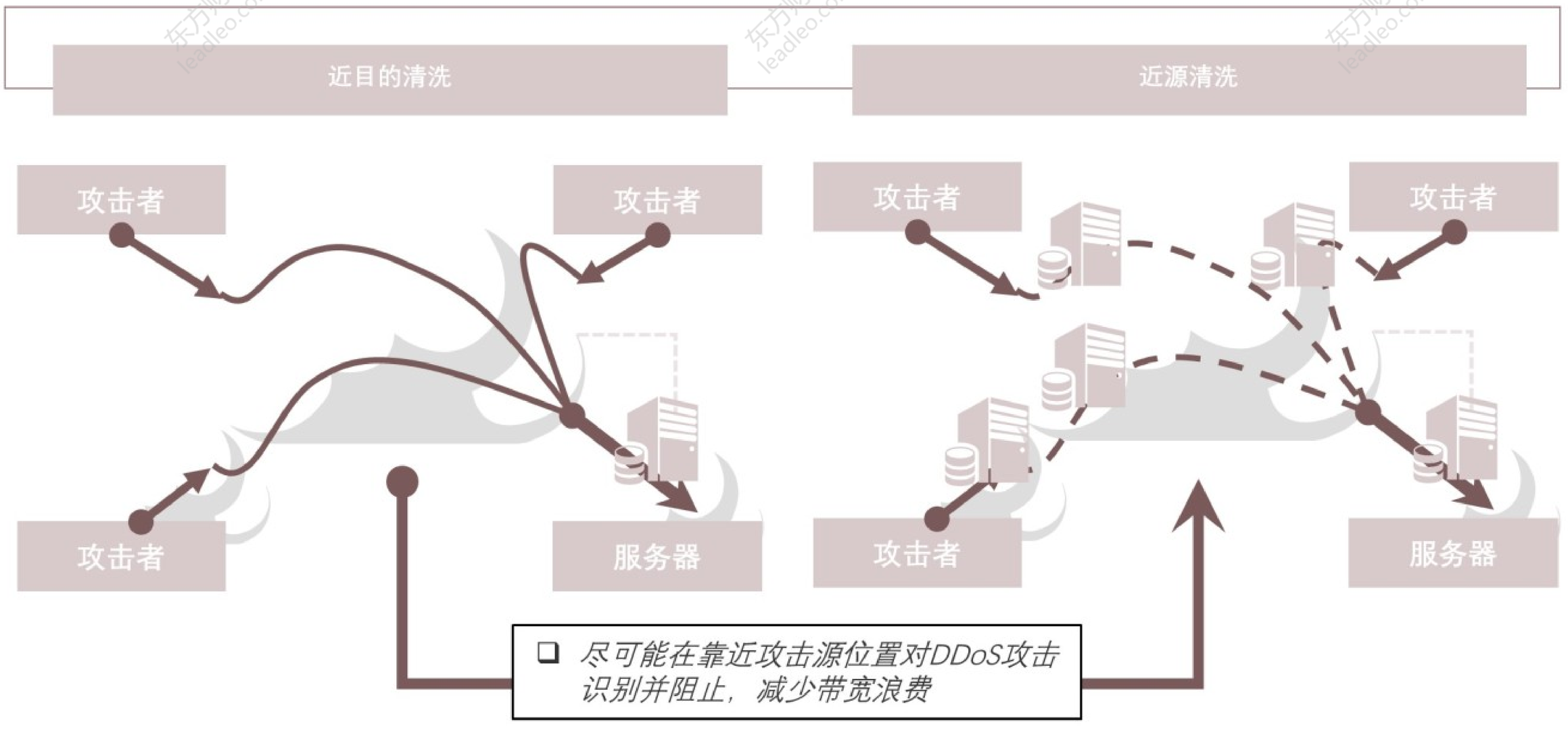
不同于其他类型云抗DDoS服务商，以中国电信为代表的网络营运商的云清洗平台主要通过与本地网络安全服务商合作，采购清洗设备并搭建与运营商私有云平台，进而提供的以硬件为基础的营运商云清洗服务。

从防护手段的角度看，营运商抗DDoS服务还该流量压制、攻击流量过滤、BGP高防IP等。其中流量压制及流量过滤分别在防御超大流量攻（承接下文）

CSDN、小蚁安全、头豹研究院

营运商清洗模式

近目的清洗与近源清洗



（承接上文）击与反射类攻击方面效果显著。而BGP高防IP主要是将所有流量牵引至BGP高防IP集群，并通过端口协议转发将客户流量转发回源站，而攻击流量则于BGP高防IP集群清洗。相较于流量压制及黑洞路由方式，该类牵引、清洗、回注的防御方式网站用户体验的影响相较小，但整体防御成本较高，同时响应延时存在在上升空间。

整体来看，营运商云抗DDoS服务模式优势主要表现为全网检测、近源防护、攻击溯源三方面：

1. 网络营运商可利用核心网路由器数据进行DDos攻击流量检测：经过营运商大网任意互联网目标IP进行在线实时流量监控。整体的网络监控覆盖面广，大流量规模测度准确性相对较高。
2. 在源站防护层面上，网络营运商可准确分辨攻击来向，调度IP承载网路由器和流量清洗设备将攻击流量在最近节点上对攻击流量的进行清除。
3. 由于营运商了解骨干网所有网络资源位置，可不依赖探针与IP归属映射溯源攻击，整体安全溯源能力表现最佳。然后，营运商云抗D服务受限于单线BGP为基础的防御方式：营运商模式偏向于其营运商自身机房内的流量攻击清洗与防护，若涉及跨营运商，可用带宽相对较小、肉鸡流量清洗与防护难度随着增加。此外，营运商数据数据检测基于Netflow抽样，以慢速攻击代表的低流量CC攻击的检测效果较差。

（在下游客群方面，营运商带宽主要的标的客户为大型互联网公司、公用云服务商、网络安全云清洗厂商等。营运商的核心竞争优势在于其丰富的宽带资源，可为上述客户提供应针对超过客户自身带宽储备与防御能力的大规模流量攻击的补充性防护抗D服务。该类大型客户支付能力及支付意愿相对较高，可盈利空间相对较广。但由于DDoS攻击主要由事件驱动，突发性及不稳定性相对较高，导致营运抗D服务收入及资金流量稳定性存在上升空间。

- 传统安全厂商前期主要通过其自身抗硬件抗DDoS设备搭建云清洗中心，依靠流量牵引方式将将客户攻击流量牵引至安全厂商的远端机房，进行流量清洗与过滤

以绿盟科技为代表的传统安全厂商前期主要通过其自身抗硬件抗DDoS设备搭建云清洗中心，依靠流量牵引方式将将客户攻击流量牵引至安全厂商的远端机房，进行流量清洗与过滤。

在服务优势方面，安全厂商通过硬件抗DDoS起步，具备专业抗DDoS专家团队及多年抗DDoS防护经验，其整体的抗DDoS技术架构、交付流程较较为成熟。同时，相较于其他类型的云抗D服务商，安全厂商在DDoS攻击处理效率、准确性等多维度占据相对优势。整体检测能力强，具备全协议支持能力，面对与业务关联性及防护难度相对较高的应用层攻击的防护能力较为出色。同时，由于安全厂商深耕抗DDoS行业多年，政务、营运商、金融等大客户关系良好，较易形成投标过程中的优势。客户整体支付能力相对较高，可盈利空间大。

从发展的维度分析，传统安全抗DDoS服务模式仍然基于硬件为主，云清洗节点的搭建暂未形成规模效应。以绿盟为代表的安全服务商有望将其云清洗服务模式向CDN技术形态转移。

随着未来节点规模的累积及分布扩展，传统安全商以CDN为基础的云抗DDoS服务模式的成熟度将随之提升。但短期来看，基于CDN技术的云抗DDoS服务前期资金投入规模相对较大，需要大量服务器、机房、带宽等资源，年均花费超过上亿级别，整体财务负担相对较高。

中国云抗DDoS服务模式——云服务厂商与CDN服务商

- 云服务商云抗DDoS服务模式基于CDN技术：可通过数个缓存代理节点，将用户访问请求导向缓存节点进而稀释DDoS攻击

云抗DDoS服务模式	模式描述	模式优势	模式痛点
云服务商模式	■ *模式搭建：拥有大量机房、服务器及带宽资源，统一控制，实现基于DNS与BGP牵引的流量分发* ■ *主要防护：分布式云清洗、高防IP、高防机房、DNS智能解析、专家运维* ■ *核心目标客群：主要包括游戏、电商等互联网企业。但细分行业客户选择各异，通常选择同业同生态的“圈内”厂商*	■ *IP隐藏：CDN域名解析只针对解析记录值，不针对源服务器IP，从而隐藏源服务器IP地址* ■ *流量复用：利用其冗余的带宽进行DDoS防护，整体防护成本及边际效益占有绝对优势* ■ *高防服务：用户可以通过配置高防IP与高防机房服务，确保源站业务稳定可靠。高防服务提供7×24的实时防护，秒级响应*	■ *公有云信任度：安全敏感度较高的行业对公有云抗D的认可度较低，偏向于自建机房或具有私有云部署能力得安全厂商* ■ *攻击源站IP：当源站IP透明时，直接攻击源站IP等方式难以借助CDN缓存节点分流稀释攻击* ■ *非HTTP协议攻击：若CDN云清洗依赖DNS牵引，对非HTTP协议的攻击防护能存在上升空间*
CDN厂商模式	■ *模式搭建：基于自身CDN业务带宽资源提供的云抗服务* ■ *主要防护：高防CDN、DNS智能解析、专家运维* ■ *核心目标客群：同云平台服务商相似，行业客户偏向于互联网企业为主，但偏向于游戏、电商、媒体等具备缓存加速需求的企业客户*	■ *分布式清洗：依靠多节点代理缓存，将用户访问请求导向缓存节点进而分散与稀释DDoS攻击* ■ *IP隐藏：CDN域名解析只针对解析记录值，不针对源服务器IP，从而隐藏源服务器IP地址* ■ *BGP Anycast: 该类方式由于境内环境不支持，主要应用于境外。其主要通过将攻击流量导向于网络拓扑结构结构的最近节点，进而于该节点稀释流量*	■ 攻击源站IP：当源站IP透明时，直接攻击源站IP等方式难以借助CDN缓存节点分流稀释攻击 ■ 非HTTP协议攻击：若CDN云清洗依赖DNS牵引，对非HTTP协议的攻击防护能存在上升空间 ■ 资源投入：CDN仍是其主营业务，抗Ddos业务的资源倾斜意愿较低

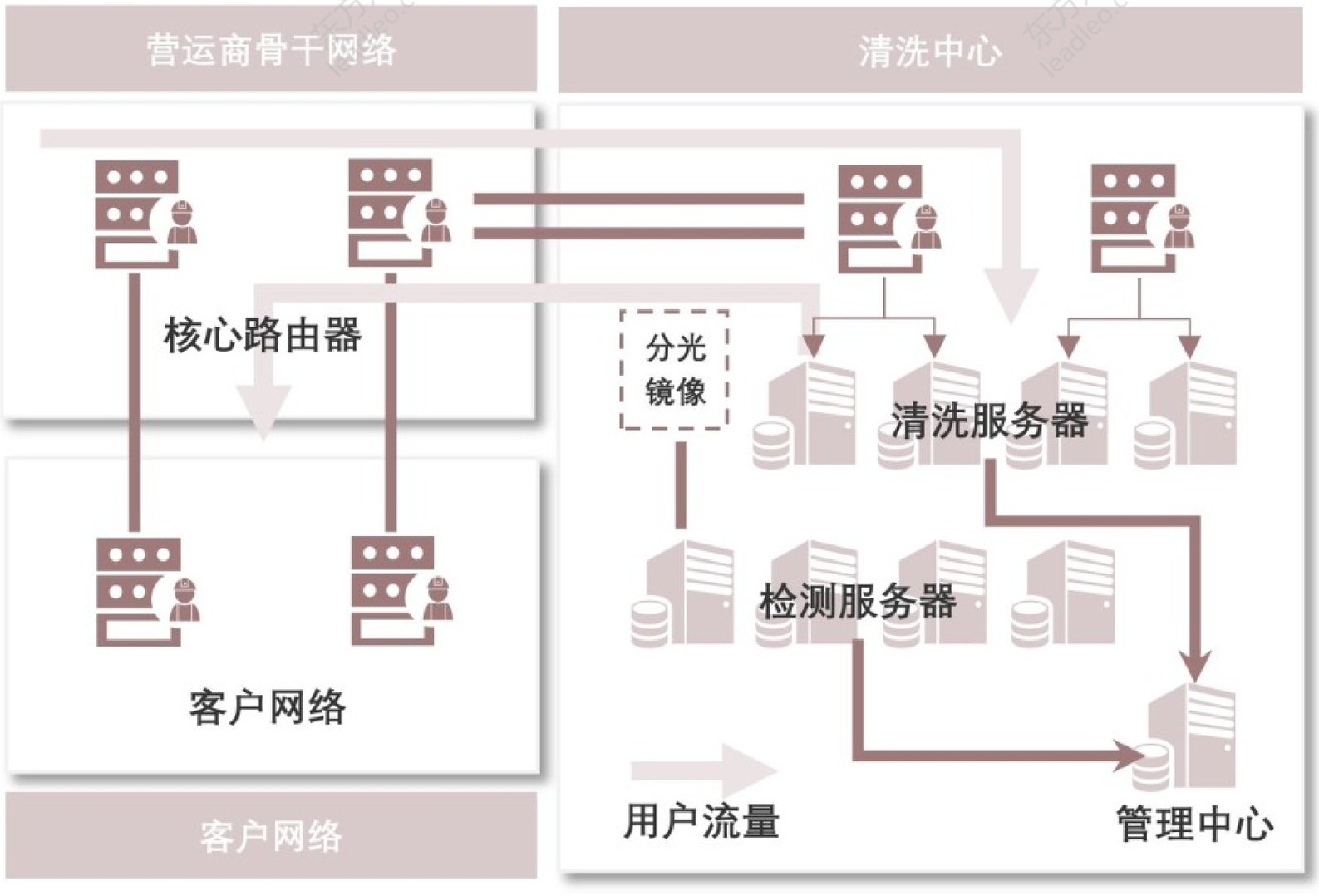
❑ 云服务商云抗DDoS服务模式基于CDN技术：可通过在互联网内设置数个缓存代理节点，并将用户访问请求导向缓存节点进而稀释DDoS攻击

同CDN服务商相似，云服务商云抗DDoS服务模式同是基于CDN技术；该技术可通过在互联网内设置数个缓存代理节点，并将用户访问请求导向缓存节点进而分散与稀释DDoS攻击。同时CDN域名解析只针对解析记录值，不针对源服务器IP，实现对源服务器IP地址隐藏，进而避免DDoS攻（承接下文）

Freebuf、头豹研究院

云服务商清洗模式

云服务商攻击流量清洗流程。



（承接上文）击者对源站客户直接打击。此外，以腾讯为代表的云服务商为用户提供配置高防IP与高防机房服务。当源站客户面对攻击峰值高达50G至100G的DDoS攻击时，高防机房服务提供提供7×24的实时防护，秒级响应，实现源站业务秒解，确保源站业务稳定可靠。但整体高防机房及高防IP服务整体费用相对较高，常规客户的月均花费在20万以上，因此该细分服务的核心标的客群主要集中于业务稳定性需高、侧重客户体验感及即时感的游戏、电商等行业。

纵观各型服务模式，云服务商抗DDoS模式的竞争优势主要可表现为两方面。首先，公有云服务商拥有大量机房及带宽资源，高防节点规模累积及地理分布占据相对优势。同时，云服务商云抗DDoS服务利用其冗余的带宽进行DDoS防护，整体防护成本及边际效益相对较高。此外，行业客户较为偏向于选择圈内玩家。因此深耕电商生态的阿里云与发展游戏生态的腾讯云在下游行业客户获客能力较为出众。

但整体而言，云服务商抗DDoS服务模式存在痛点。首先，云服务商CDN云清洗若依赖DNS牵引，对非HTTP协议DDoS攻击防护能力较为受限。其次，当部分源站IP透明时，攻击者将直接攻击源站IP，云服务厂商难以借助CDN缓存节点分流稀释DDoS攻击。最后，由于下游客户对公有云的信任程度存在上升空间，以政务及金融等安全敏感度较高的行业对公有云抗D的认可度较低，主要偏向于自建机房或具有私有云部署能力得安全厂商。

方法论

- 头豹研究院布局中国市场，深入研究10大行业，54个垂直行业的市场变化，已经积累了近50万行业研究样本，完成近10,000多个独立的研究咨询项目。
- 研究院依托中国活跃的经济环境，从社会保险、人工智能、大数据等领域着手，研究内容覆盖整个行业的发展周期，伴随着行业中企业的创立，发展，扩张，到企业走向上市及上市后的成熟期，研究院的各行业研究员探索和评估行业中多变的产业模式，企业的商业模式和运营模式，以专业的视野解读行业的沿革。
- 研究院融合传统与新型的研究方法，采用自主研发的算法，结合行业交叉的大数据，以多元化的调研方法，挖掘定量数据背后的逻辑，分析定性内容背后的观点，客观和真实地阐述行业的现状，前瞻性地预测行业未来的发展趋势，在研究院的每一份研究报告中，完整地呈现行业的过去，现在和未来。
- 研究院密切关注行业发展最新动向，报告内容及数据会随着行业发展、技术革新、竞争格局变化、政策法规颁布、市场调研深入，保持不断更新与优化。
- 研究院秉承匠心研究，砥砺前行的宗旨，从战略的角度分析行业，从执行的层面阅读行业，为每一个行业的报告阅读者提供值得品鉴的研究报告。

法律声明