2019 | DDoS攻击

态势分析报告

CUiSEC 联通智慧安全

UNI SAFE 联通云盾

关于联通智慧安全科技有限公司

联通智慧安全科技有限公司是中国联通的全资子公司，基于通信运营商禀赋，全面整合中国联通内外部优势资源与能力，充分发挥网络资源、运营支撑体系及人员优势，面向安全服务、云安全、互联网应用安全、终端安全、5G/ 物联网等安全细分市场，聚焦“云、管、端”与“安全产品 + 安全服务”，着力打造抗D先锋、域名无忧、可信应用、威胁情报、安全岛链、网站护卫、态势感知、数字认证等安全产品，全面构建专业化、差异化、一体化的信息安全综合服务能力，将信息安全业务打造成为中国联通的创新业务，为践行“网络强国战略”提供有力保障。

百度安全 有AI更安全

关于百度安全

百度安全是百度公司旗下，以AI为核心、大数据为基础打造的知名安全品牌，是百度在互联网安全20年安全实践的总结与提炼。 业务由AI安全、移动安全、云安全、数据安全、业务安全五大矩阵构成，全面覆盖百度各种复杂业务场景，同时向个人用户和 商业伙伴输出安全产品与行业一体化解决方案。百度安全以技术开源、专利共享、标准驱动为理念，联合互联网公司、安全厂商、终端制造商、高校及科研机构， 推动AI时代的安全生态建设，让全行业享受更安全的AI所来带来的变革。

关于联通智网中心

中国联通集团智能网络中心是承担集团创新产品的研发应用、新型网络的智能化建设的生产机构。在规建维研一体化工作模式下，推进中国联通网络建设智能化、网络运营集约化与智能化，支撑网络能力开放，实现创新网络产品化运营。智网中心依托运营商独有的整体网络资源，进行智能网络的能力开发和服务能力挖潜，在监测、防护、服务、态势等多方面打造覆盖全网的安全能力。

1 序言

1.1 序言

本报告由中国联通和百度联合发布，针对 2019年发生的 DDoS攻击事件进行汇总分析。报告给出了2019年中国联通全网范围内监测到DDoS攻击事件的数量、攻击强度、持续时长、受害者地域分布等多个维度的情况分析，并对发起DDoS攻击的攻击源进行追溯和分析，从而力争达到对DDoS攻击形成立体宏观的刻画，为治理DDoS攻击，净化网络空间提供数据支撑。

1.2 2019年攻击情况摘要

攻击数量小幅回落： 2019年中国联通全网范围内共监测到DDoS攻击36万余次，相对于2018年的46万余次，在攻击数量上有所减少。

攻击强度两级分化： 300Gbps以上的超大流量攻击达到1040次，相比2018年增加2个百分点；1Gbps以下的小流量攻击较2018年有大幅度增加，呈现超大型攻击和小流量攻击增多的态势。本年度，单次攻击峰值最大达到640Gbps。

瞬时骚扰性攻击为主： 攻击持续时长仍以瞬时攻击为主，持续时间在5分钟以下的攻击占据41%，攻击者以短时、多次的骚扰性攻击为主要手段。

攻击手段集中： 攻击手段方面，UDP Flooding和 TCP SYN Flooding仍是攻击的主要手段，共占总体的82.7%，但HTTP Flooding等应用型流量攻击较2018年大幅度增加，反射攻击整体活动放缓。

地域： 中国境内，浙江、北京、山东、广东等经济发达地区是遭受DDoS攻击最集中的地域。全球范围内，中国和美国是遭受DDoS攻击最频繁的国家。

行业： 金融，游戏，能源电力基础设施，IDC等行业都是极易遭受DDoS攻击的重灾区。

黑客团伙： Mirai，Gh0st等僵尸网络较为活跃。发现CoAP等新兴反射型攻击方式；webscan，sql注入等传统方式仍为web攻击主流。

1.3 DDoS攻击总体发展趋势

近年来，DDoS攻击技术门槛逐渐降低，僵尸网络主机价格大幅度降低，智能化DDoS攻击工具也逐渐成为攻击者首选；同时随着大量IoT设备进入互联网，攻击者可操控的肉鸡数量呈几何级上升。各种基于物联网僵尸网络的木马病毒变种快速增加，传统的windows平台僵尸主机被IoT平台取代。这些因素导致DDoS攻击愈演愈烈，其影响范围和破坏力也逐年增大。

1.4 2019年重大DDoS事件回顾

2019年，网络安全事件频发，黑客团体频频发动以政治诉求和经济利益为目的的攻击，其中知名度和影响程度较大的攻击事件如下。

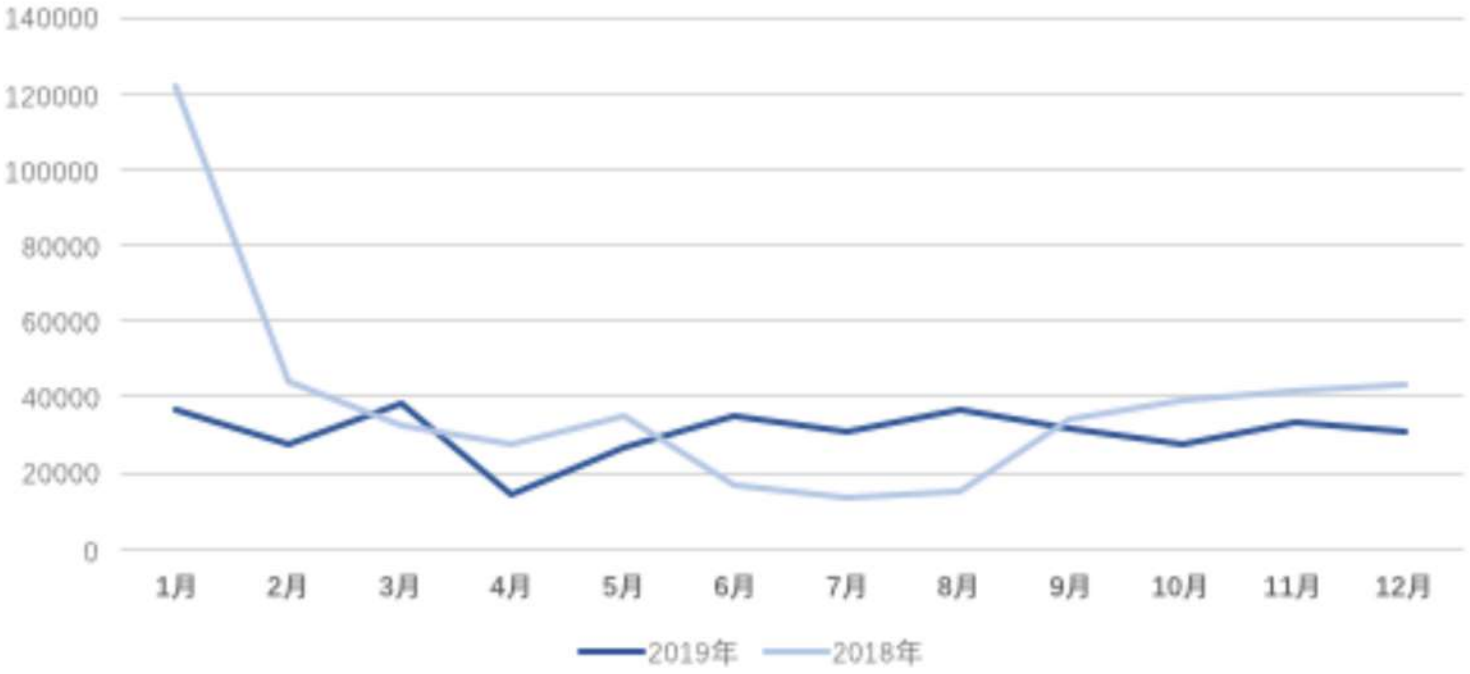
2月	国内某短视频APP上千万账户遭撞库攻击，其中上百万账户密码被泄露。
3月	俄罗斯50多家大型企业遭到未知攻击者勒索。
4月	Facebook发生数据泄露事件，导致5400万Facebook相关的记录，包括姓名、ID、密码、喜好、照片、加入的组织等用户重要信息被流出到第三方公司平台。
5月	湖北省首例入侵物联网破坏计算机信息系统的刑事案件破获。
7月	委内瑞拉水电站遭到电磁攻击导致首都加拉加斯10余个州发生大规模停电，地区供水和通信网络也因此受到极大影响。
9月	维基百科遭受恶意网络攻击事件。该攻击导致多个国家的网站脱机，主要影响欧洲、中东和非洲的用户使用。这次攻击在攻击流量和持续时长上都是异乎寻常的。
11月	印度独立网络核电站Kudankulam遭遇疑似APT组织攻击，印度官方发布声明承认遭到外部攻击者渗透。

2 2019年DDoS攻击态势分析

2.1 攻击数量趋势

2019年全年，中国联通全网范围内共监测到DDoS攻击36万余次，较2018年的46万余次下降21.7%。从1至12月各月监测攻击次数看，全年遭受攻击趋势相对平滑，除二季度攻击稍有减少外，其余各季度攻击次数较为平均。

2019 VS 2018各月攻击数量趋势如图:

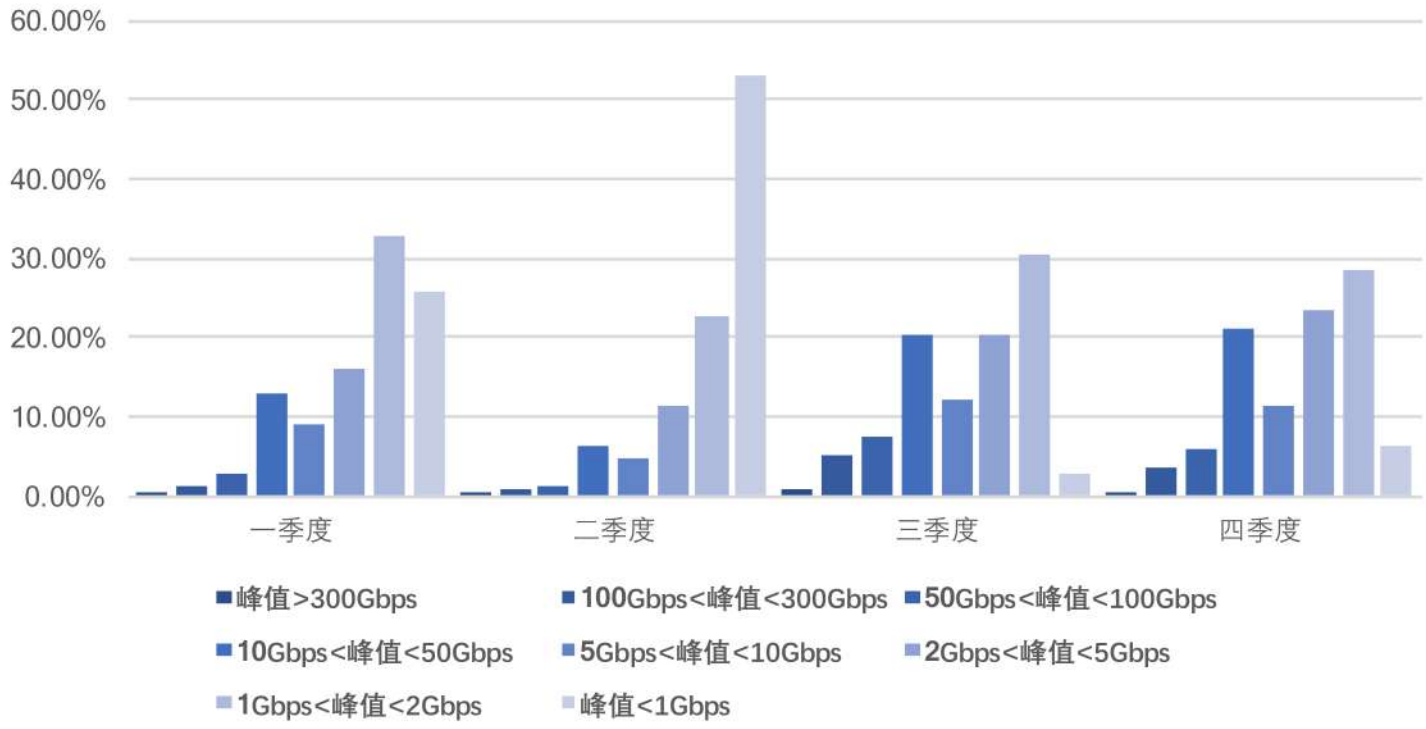


2.2 攻击峰值趋势

2019各季度攻击峰值占比统计

2019年DDoS攻击仍然以峰值在10Gbps以下的攻击为主，占全部攻击总数的76.8%。纵观全年各季度攻击峰值占比情况，可以看出三、四季度10Gbps以上的大流量攻击数量较上半年有所增加。

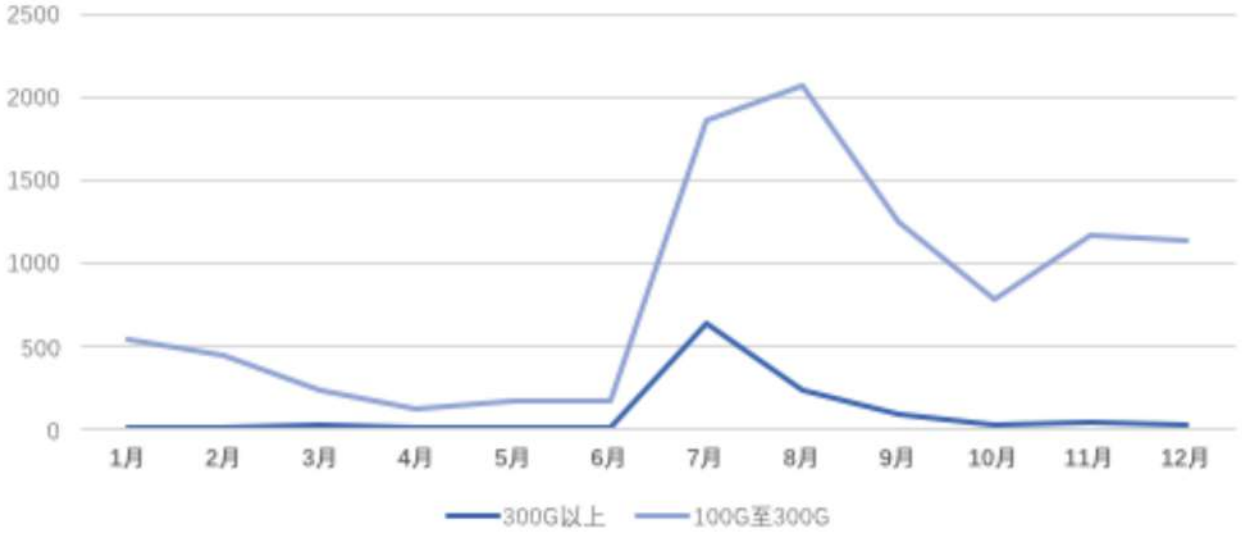
2019年各季度攻击峰值分布情况如图。



2019大流量攻击次数统计

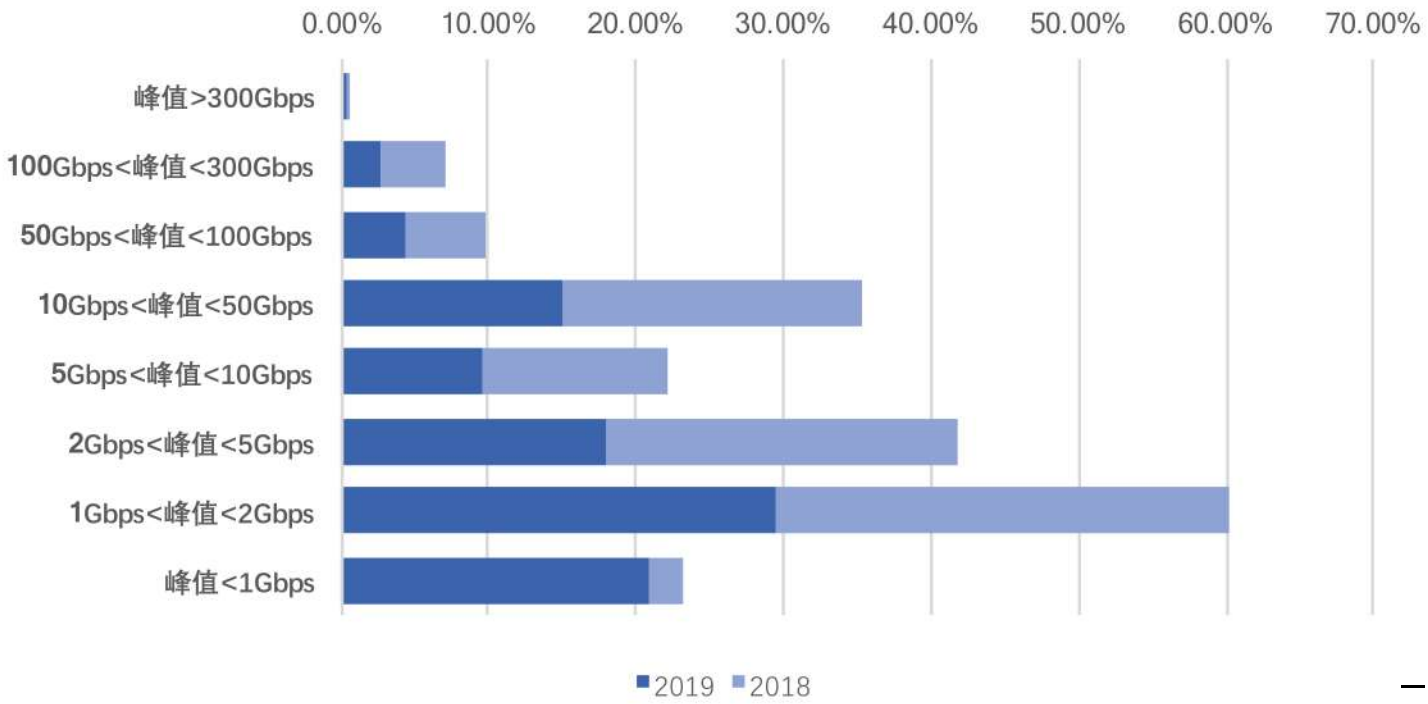
2019年全年共监测到100Gbps以上大流量攻击10935次，占全部攻击的3%。其中300Gbps以上超大型流量攻击共计1040件，并主要发生在第三季度。年度最大规模攻击发生在3月，攻击峰值达到640Gbps。

2019年各月大流量攻击次数分布如图。



2019 VS 2018攻击峰值占比对比

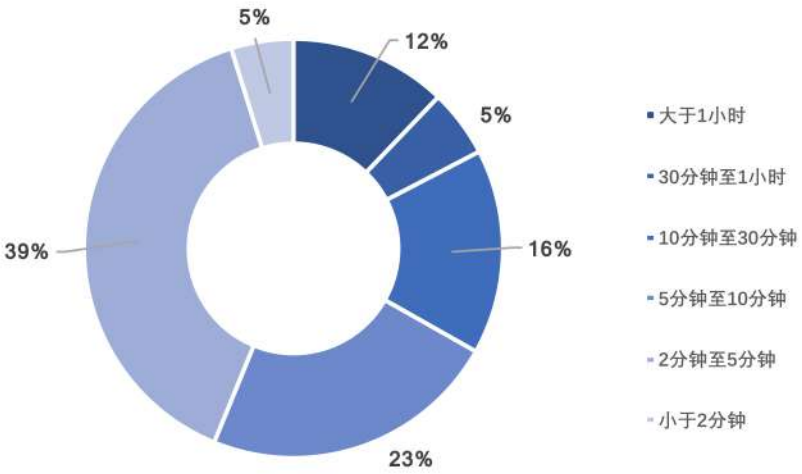
与2018年相比，2019年整体攻击峰值呈现减小趋势，除300Gbps以上超大型攻击占比0.3%，高于2018年的0.1%外，1Gbps以上规模攻击占比均小于2018年。2019年1Gbps以下规模的小规模攻击呈明显增多趋势，占全部攻击的20.48%，该数字远远大于2018年的2.35%。2019年攻击规模向两极化趋势分布，300Gbps以上超大型攻击和1Gbps以下小规模攻击均呈增多趋势。攻击峰值方面，2018年受新兴起的Memcached反射攻击影响，最大攻击峰值达到1.3Tbps，2019年则有所回落，为640Gbps。大量智能化攻击平台的使用，是导致DDoS攻击整体规模放大的主要原因。



2.3 攻击时长趋势

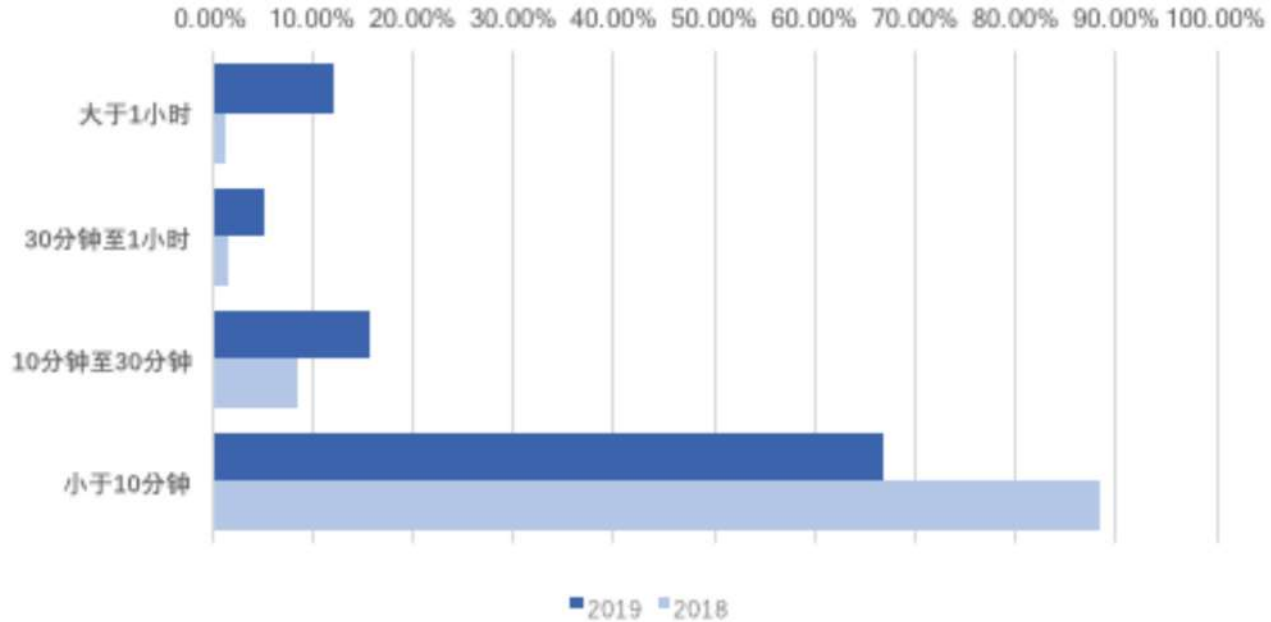
2019攻击持续时长统计

2019年DDoS攻击仍是以短时攻击为主，持续时长在10分钟之内的攻击占全部攻击的67%，其中以持续时长为2至5分钟的攻击占比最大，达到39%，攻击时长在30分钟之内的攻击占到攻击总量的83%。另一方面，攻击时长大于1小时的攻击占全部攻击的12%，其中持续时间最长攻击发生在10月，达到400小时之久。
2019年攻击持续时长分布如图。



2019 VS 2018攻击持续时长对比

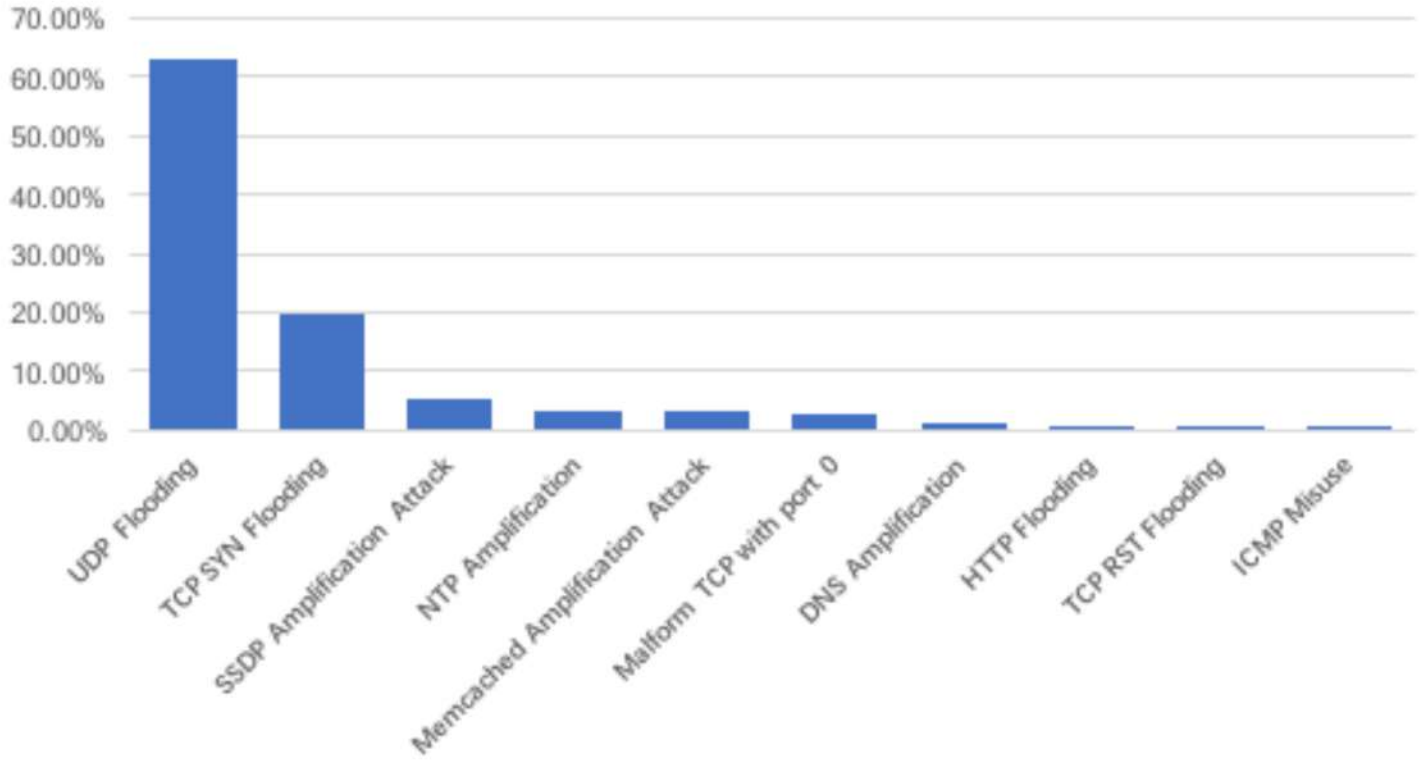
相比较于2018年，2019年攻击持续时长有增长趋势，大于1小时的攻击占比达到12%，远高于2018年的1%。同时，持续时长在30分钟至1小时和持续时长在10分钟至30分钟的攻击占比也比2018年有较大幅度增长。攻击时长和攻击流量的增加，反映出DDoS攻击成本的降低，同时也反映出攻击者对目标业务持续干扰，不达目的不罢休的态度。



2.4 攻击手段分析

2019各季度攻击手段占比分析

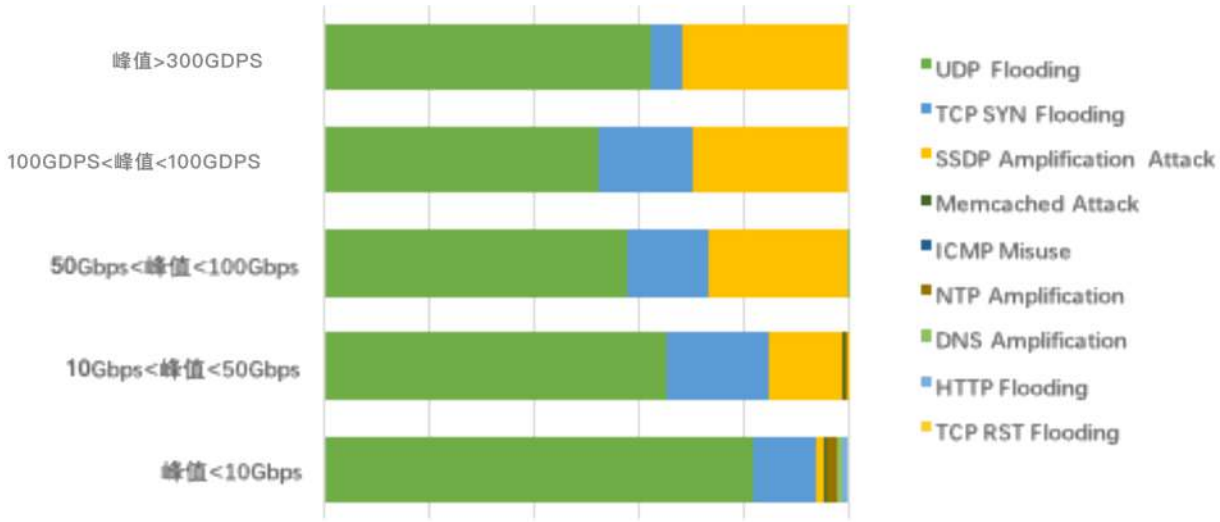
2019年，DDoS攻击主要以UDP Flooding、TCP SYN Flooding为主要攻击手段，其中尤其以UDP Flooding攻击为主，占全部攻击总量的62.8%，成为流量型攻击的主要手段来源。TCP SYN Flooding攻击，作为另一种主要的攻击手段，也占据19.9%的比重，且成为包处理型攻击的主要手段。反射攻击依然盛行，SSDP、NTP、Memcached、DNS等反射型攻击，占据了总量的15%。
2019年攻击类型TOP10如图。



2019攻击类型各流量区间分布

2019年，UDP Flooding仍在各峰值流量分布区间中占主导地位，但随着攻击峰值的增大，SSDP反射攻击所占比例逐渐增大。

2019年各峰值区间攻击类型分布如图。

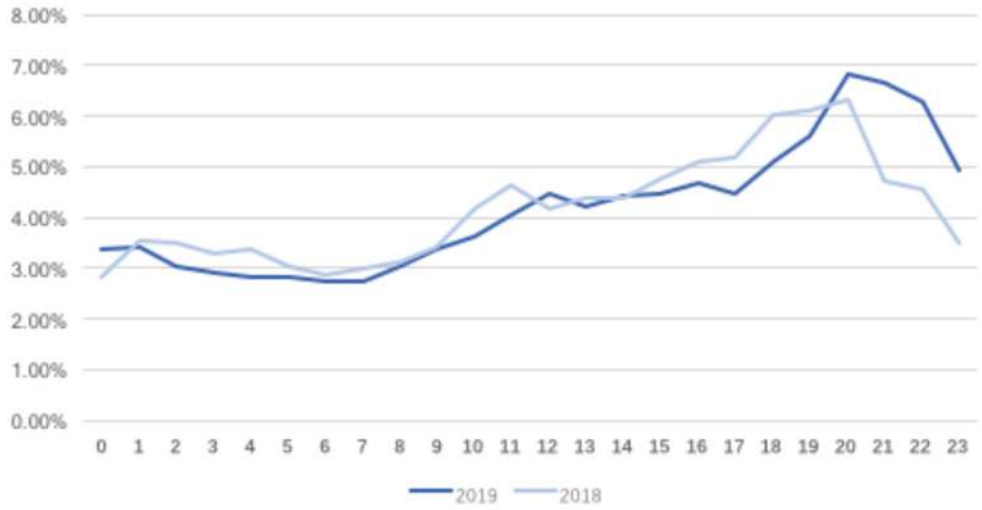


2.5 攻击发生时段分析

2019一天24小时内攻击发生分布

从一天24小时发生DDoS攻击的占比分布分析，攻击数量从8点开始攀升，直至24点，均为DDoS高发期。其中又以17点至24点为攻击最频繁时段，在21点左右达到攻击发生频率最高峰。2019年，攻击在24小时内各时段发生的频度与2018年较为一致，可以看出DDoS攻击者均选择在业务高峰期发起针对目标的攻击。

2019 VS 2018 24小时内攻击发生频度分布如图。



2.6 DDoS攻击目标地域分布

国内受攻击地域分析

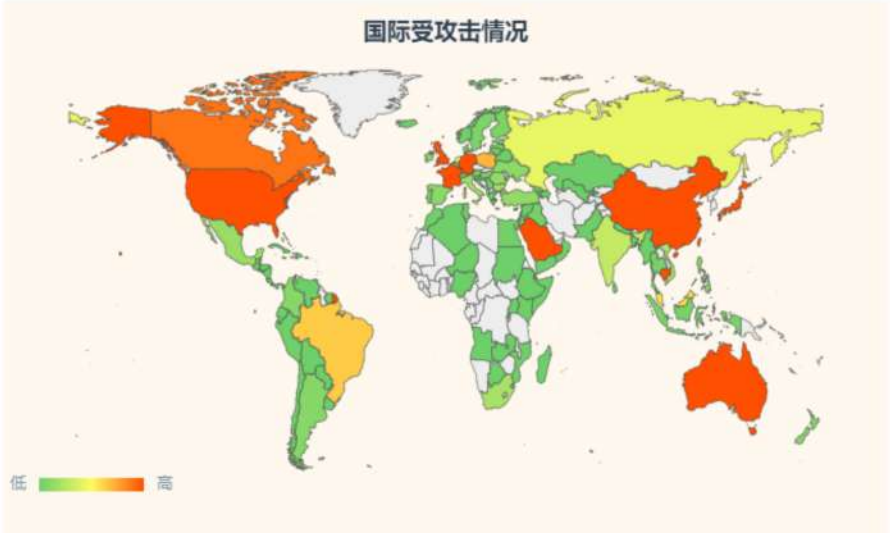
2019年，中国境内受攻击最多的省份为浙江，全年累计遭受攻击5万余次，约占全国受攻击总数的18.4%，随后排名依次从第二至第五位的省份和地区分别为北京、山东、广东、香港。2019年香港地区遭受DDoS攻击数量明显增多。

2019年中国境内遭受DDoS攻击情况如图。

全球受攻击地域分析

2019年，据监测数据显示，中国和美国成为遭受DDoS攻击最严重的国家，其次是英国、澳大利亚、加拿大等国家。

2019年国际遭受DDoS攻击情况如图。



2.7 攻击源地域分布

国内攻击源地域分布

对2019年中国境内参与DDoS攻击的终端和设备进行溯源分析和数量统计，山东成为具有最多活跃攻击资源的省份，所拥有参与DDoS攻击主机数量占全国总量的12.1%，此外广东、辽宁、河南也是拥有活跃攻击资源较多的省份。攻击资源主要集中在沿海省份和东北三省。

2019国内攻击源地域分布如图:

全球攻击源地域分布

从活跃攻击资源的全球分布来看，中国和美国存在较多的攻击活跃资源，其次为澳大利亚、中国香港、英国等国家和地区。

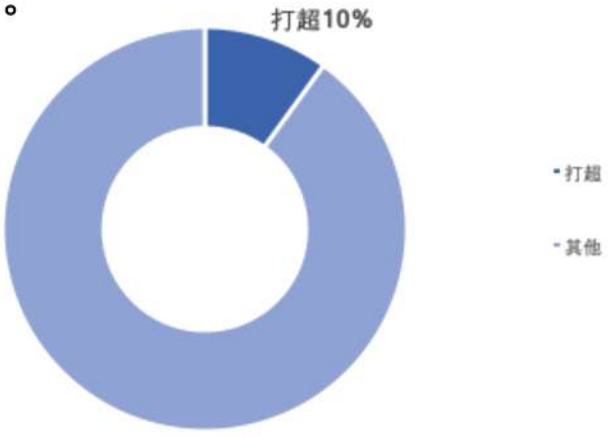
2019全球攻击源地域分布如图:

3 行业DDoS安全状况分析

近几年，随着移动互联网、大数据、云计算、人工智能、区块链等新一代信息技术的快速发展，围绕网络和数据的服务与应用呈现爆发式增长，丰富的应用场景下暴露出越来越多的网络安全风险和问题。网络安全涉及到的行业也越来越广，不再仅仅局限于互联网行业。频繁发生的大规模DDoS攻击，都给这些行业带来了巨大的威胁。

3.1 数据中心、云服务商

传统IDC数据中心，云服务商等行业，本身不但是互联网系统的基础构建者，同时也是DDoS攻击的最大受害者之一。对于各类数据中心，带宽是最为宝贵的资源，如果因为DDoS攻击而打超，耗尽了带宽，那将带来非常大的损失。而从我们获得并分析的数据来看，带宽被打超的比例占到了10%，也就是每10次攻击中就有可能打超瘫痪一个机房。



2019 DDoS攻击带宽被打超比例如图。

3.2 电力基础设施行业

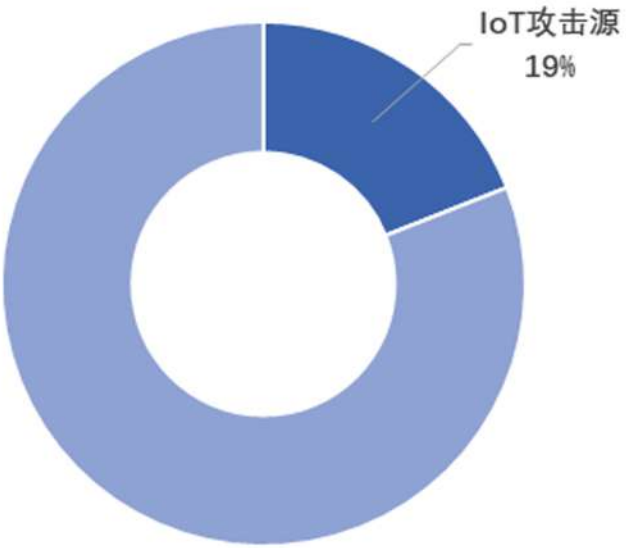
能源电力等基础设施行业是支撑整个社会、国家正常运转的重要行业。而随着近几年工业互联网的迅速发展，大量的能源监控管理系统暴露在互联网上，有巨大的网络安全风险。

而这类针对能源基础行业的攻击已经有不少实际攻击事件发生。2019年3月5日美国西部几个州提供电力的能源公司遭到大规模的DDoS攻击，导致当天电气系统运行中断超过10小时。

3.3 安防、智能家居行业

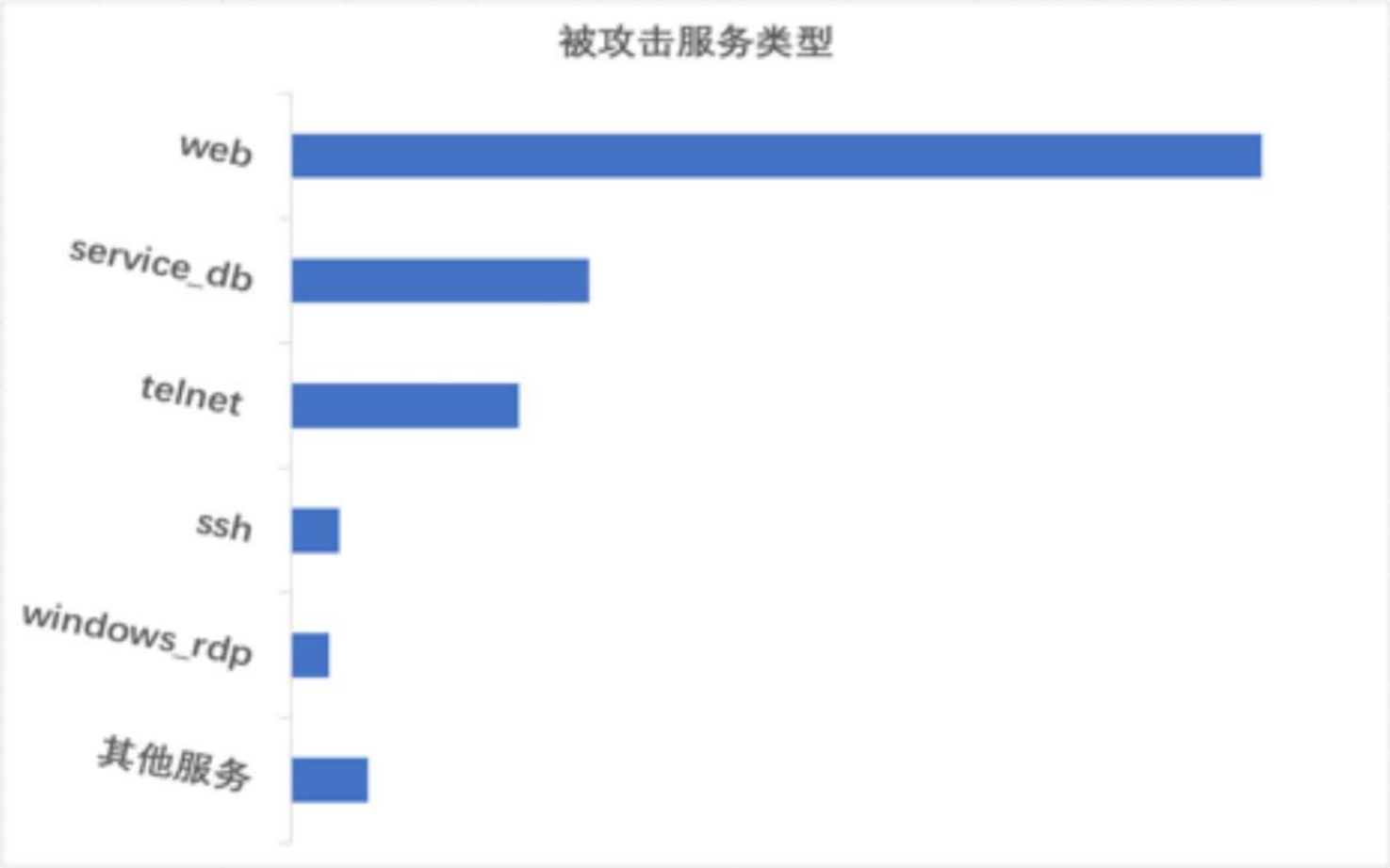
安防与智能家居行业都是近几年随着IoT设备兴起的新兴行业，发展迅速，前景巨大。但是这两个行业都包含了大量的摄像头等监控设备，与其他行业主要遭受攻击危害不同，IoT设备的主要威胁在于沦为DDoS设备的攻击工具。据百度安全团队的分析，2019年所检测到的DDoS攻击中，至少有 19%的攻击来源来自于被黑客利用的IoT设备。

2019 DDoS中IoT攻击源占比如图：



3.4 游戏、电商等其他行业

除以上行业之外，电商，游戏等其他行业也同样易受到DDoS攻击的危害。例如随着区块链技术的兴起，大量的虚拟币交易平台以web的形式存在互联网，一旦受到攻击，交易就将陷入瘫痪，进而受到威胁勒索。电商，游戏，政府门户等往往也以网站或APP的方式存在。而从2019年度，我们对遭受的互联网服务分析中发现，web类的服务仍然是DDoS攻击的重灾区。



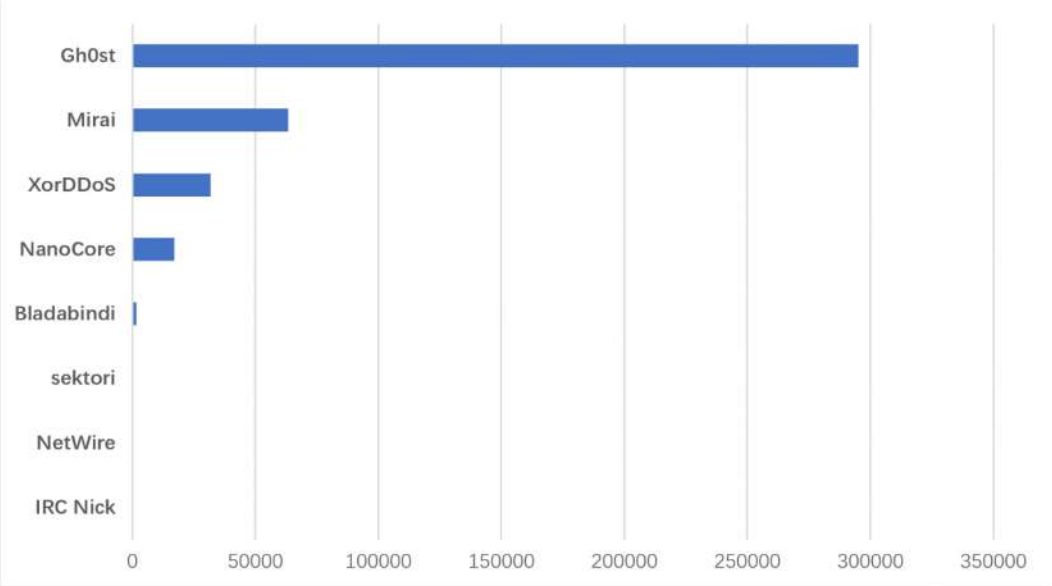
4 黑客团伙攻击手法分析

各类专门从事DDoS攻击的黑客团伙，最主要的攻击手段主要为两类，一类是通过其木马家族感染的庞大僵尸网络，向目标发起大规模流量攻击。另一类则是利用一些设备的协议，接口等漏洞，通过反射放大流量，来对目标进行攻击。以下我们就对此两类攻击手段的现状做了简要的分析。

4.1 僵尸网络分布情况

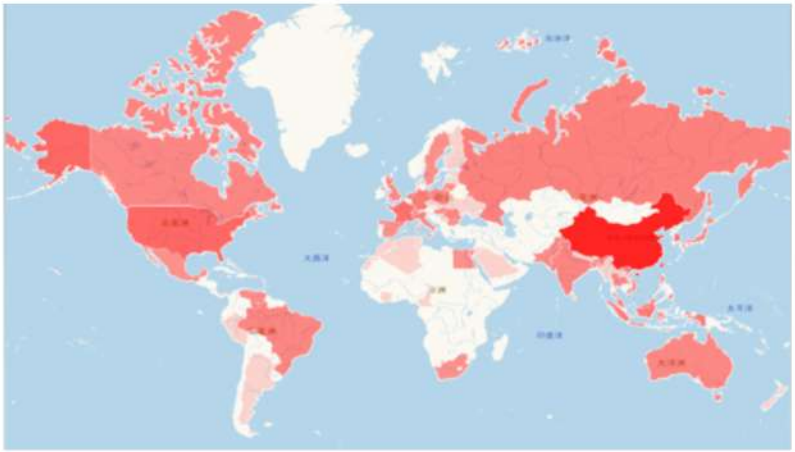
根据2019年对各类活跃的僵尸网络进行监控分析后，发现Gh0st是最大的僵尸网络感染木马家族，其次是Mirai和XorDDoS等。

2019主要的僵尸网络感染情况如图（单位：个）。

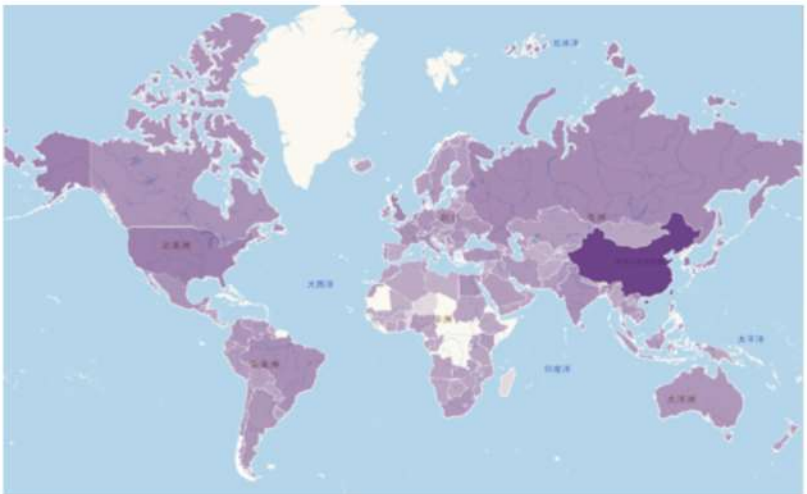


可以看到，虽然Mirai木马家族在近几年臭名昭著，但就感染的数量而言，Gh0st更为广泛。而这些僵尸网络的主控全球分布如下，中国与北美依然是僵尸网络分布最广泛的区域。

主控分布情况



肉鸡分布情况



4.2 典型僵尸网络介绍

1.Mirai

Mirai可以说是近几年最红的僵尸网络，Mirai是一种IoT类型的僵尸网络，最早在2016年8月被安全研究人员发现，从此迅速爆发，肆虐网络。2018年1月，Mirai恶意软件的3名开发者与美国司法部达成认罪协议。但是Mirai蔓延的势头已经无法阻挡，2019年还出现了其多个变种。

2.Gh0st

Gh0st最初是国内开源的RAT类软件，用于远程控制计算机。但因为其功能的全面性，以及开源的关系，尤其获得黑客青睐，对其进行改造作为木马使用，以至于网络上至少出现了40种以上的变种，感染范围极大。

3.XorDDoS

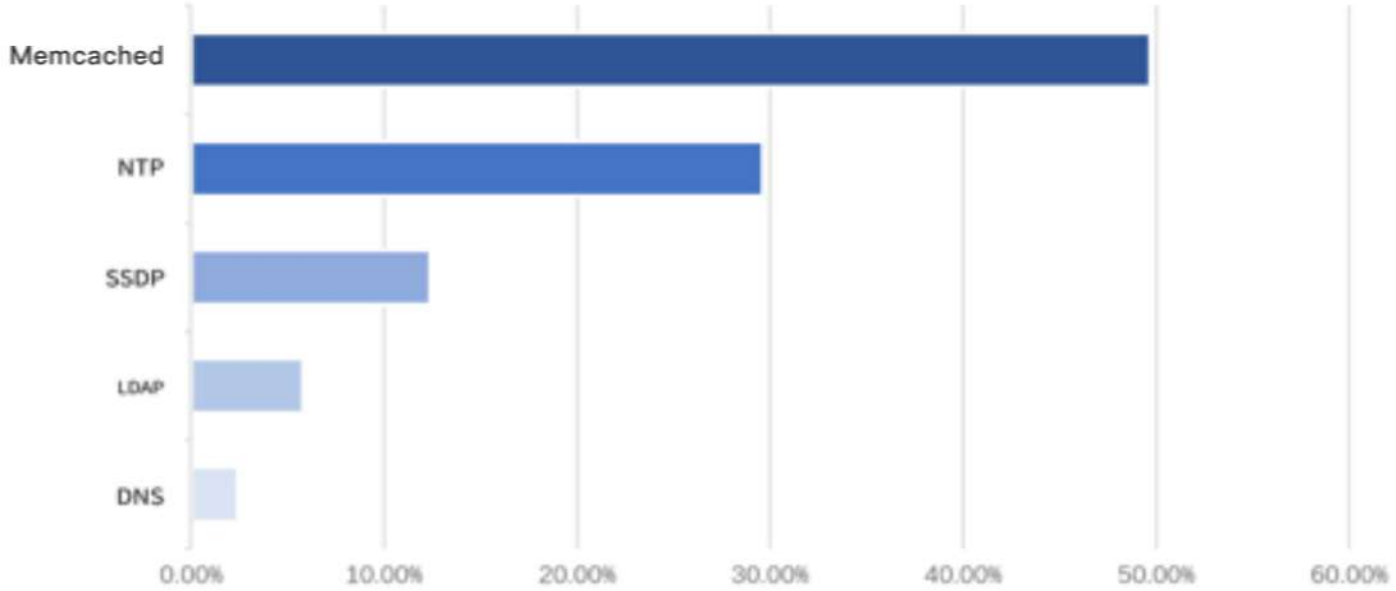
XorDDoS是一个相对古老的僵尸网络，最早于2014年就被研究人员发现。其名字XorDDoS来源于大量使用的XOR加密，该加密方法同时用于恶意软件和到C&C服务器的网络通信中。XorDDoS恶意家族主要特点是，用暴力猜解目标主机ssh弱密码的方式，入侵目标主机，然后执行相应的shell脚本安装XorDDoS恶意家族感染客户主机。

5 反射攻击

除了僵尸网络外，反射型攻击是黑客团伙手中另一把利器。在反射型的 DDoS 攻击时，攻击者并不直接攻击目标服务 IP，而是利用互联网的某些特殊服务开放的服务器，通过伪造被攻击者的 IP 地址、向有开放服务的服务器发送构造的请求报文，该服务器会将数倍于请求报文的回复数据发送到被攻击 IP，从而对后者间接形成 DDoS 攻击。

而在反射型攻击中，可以看到近些年新发现的Memcached反射攻击方式仍然非常受黑客团体的青睐。

TOP5的反射攻击如图



除此之外，2019年，还发现了多个其他新型的反射攻击

1.基于CoAP协议的物联网设备参与DDoS反射攻击

百度安全智云盾团队在2019年4月为某第三方IDC提供DDoS防御能力时，捕获到一种新型的利用物联网设备发起的DDoS事件。智云盾系统检测到攻击时，自动对流量进行了采样，安全专家对采样包及时进行了深层次的分析和演练发现，本次攻击事件中黑客利用了基于物联网的CoAP协议发起了DDoS反射攻击。目前观察到的CoAP的攻击事件中，我们推测此次放大倍数在11.76倍。从SHODAN上对5683相关的端口进行检索发现，全球约有72万台主机暴露了5683端口，CoAP作为物联网设备联网的基础协议，将随着物联网网络的普及进一步的扩大，这些设备都将可能被用作反射源。

CoAP协议设备全球分布	
TOTAL RESULTS	
719,719	
TOP COUNTRIES	
China	369,255
Ressian Federation	328,081
Ukraine	6,826
United States	4,938
Belarus	1,937
TOP ORGANIZATIONS	
China Mobile Guangdong	261,006
China Mobile Shandong	67,014
Rostelecom	52,996
Beeline Home	27,775
China Mobile	16,767

2.基于WS-DISCOVERY的物联网设备参与DDoS反射攻击

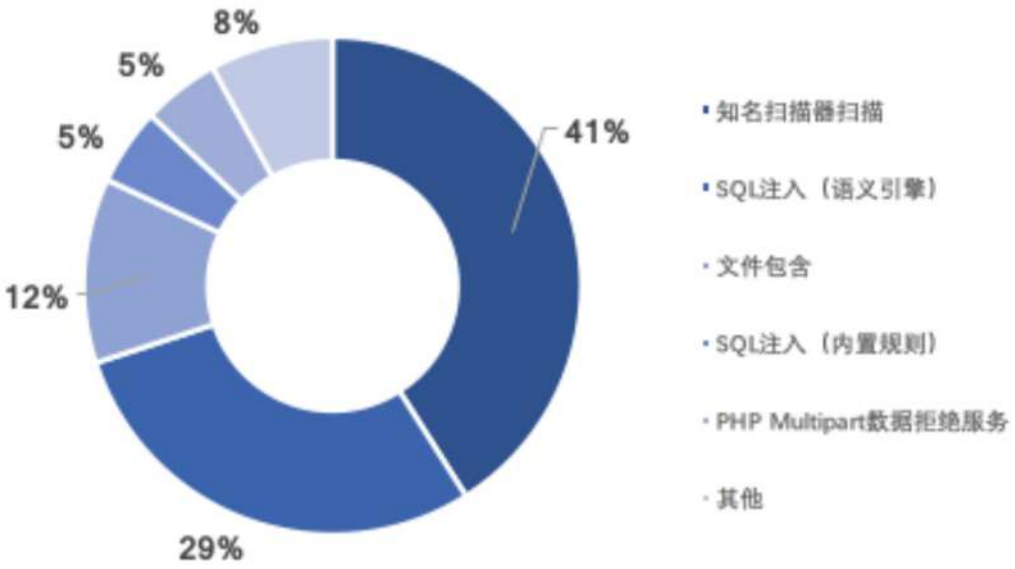
2019年2月份，百度安全智云盾团队监测到首次以WS-DISCOVERY接口发起的DDoS反射攻击，ONVIF规范中设备管理和控制部分所定义的接口均以Web Services的形式提供。本次黑客使用的WS-DISCOVERY接口是ONVIF协议定义的设备发现接口。黑客利用了其基于UDP协议且响应大于请求的属性发动了DDoS反射放大攻击。反射类型的DDoS攻击并不会直接攻击受害者IP，而是以受害者的IP构造UDP数据包，对反射源发送伪造的数据包，反射源向受害者IP响应的流量远超过攻击者伪造UDP流量的数据，DDoS黑客组织依靠此方式对受害者实施DDoS攻击。从目前观察中我们推测此次放大倍数在5-14倍。SHODAN上对3702相关的端口进行检索发现，全球约有21万台主机暴露了3702端口，如果支持ONVIF协议，都可能被用作反射源攻击。

ONVIF协议设备全球分布	
TOTAL RESULTS	
212,096	
TOP COUNTRIES	
Viet Nam	30,299
China	22,149
United States	21,811
Korea,Republic of	14,096
TOP ORGANIZATIONS	
Vietnam Posts and Telecommunications(VNPT)	13,615
Viettel Group	9,011
Korea,Telecom	7,784
HiNet	6,168
Telmex	3,827
TOP OPERATING SYSTEMS	
Linux 3.x	1

6 Web攻击手法分布

Web攻击是黑客团队用来捕获各类肉鸡的主要手段，对此百度安全基于WAF防御的数据对各类攻击手法情况做了分析汇总。
可以看到，利用知名的工具进行扫描，SQL注入，文件包含等漏洞是Web攻击的主流。

2019 Web攻击手段分布如图。



而这个检测结果，和我们对黑客团体的跟踪结果也是非常吻合的。据我们对大量僵尸网络的监控发现，使用各类扫描器进行webscan，SQL注入，文件包含等传统Web攻击方式仍是各类黑客团队常见的手段。
例如我们发现的某个利用Mirai Variant感染组成僵尸网络的黑客团伙，掌控了1000多个主控，2W多个肉鸡，遍布东亚，北美和欧洲。其主要手段就是web-scan。特别是针对Struts 2.3.20-28 RCE, CVE-2018-7600, CVE-2018-9866, CCTV-DVR Vendors RCE等漏洞。

7 结语与展望

2019年攻击统计分析数据告诉我们，网络安全形势严峻，DDoS攻击和各种网站入侵攻击泛滥，APT攻击更多的发生，重点设施及业务遭到破坏，重要数据遭到泄露，都反映出网络攻击已全面进入产业化时代，黑产处心积虑利用各种攻击手段获取高额利益。随着2019年5G网络正式商业化以及后续的广泛运用，使连接设备数量大幅度增长，如果这些设备安全性管理不善，将给DDoS攻击者带来海量可以利用的肉鸡工具，同时增大了DDoS攻击溯源的难度。此外，随着工业互联网的发展，DDoS攻击黑手，也会触及工业及社会生产的各个领域，网络空间安全将面临前所未有的严峻考验。