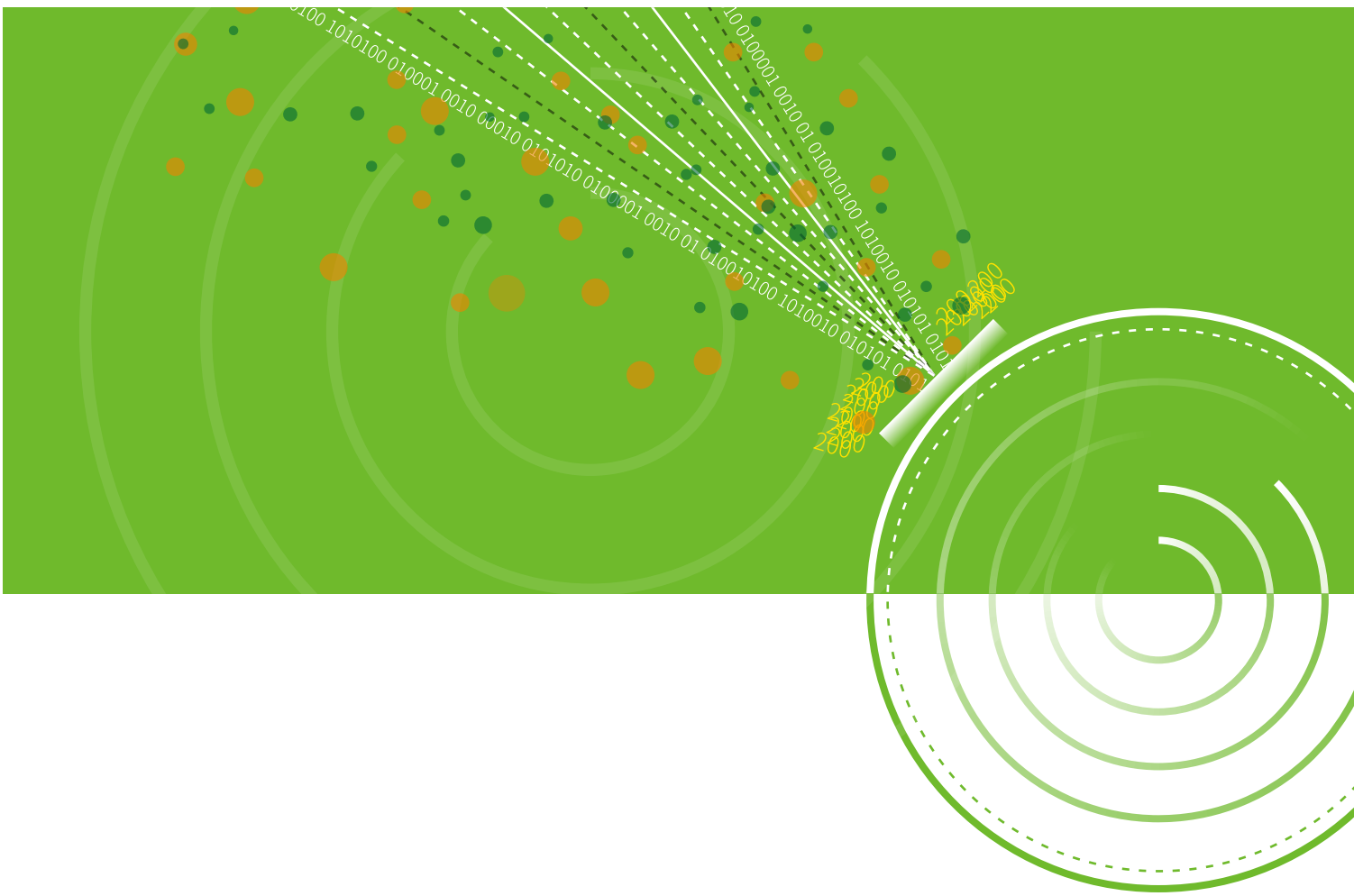
中国电信·云堤 CHINA TELECOM

NSFOCUS

2018 DDoS攻击态势报告



关于中国电信云堤

2008 年以来，中国电信开始着力于网络 DDoS 攻击防护能力建设，已形成了覆盖国内 31 省和亚太、欧洲、北美等主要 POP 点的一体化攻击防御能力。2014 年，中国电信首次在业界系统性提出电信级网络集约化安全能力开放平台框架，并将“云堤”作为对外服务的统一品牌。

几年来，中国电信云堤一方面致力于高效、可靠、精确、可开放的 DDoS 攻击防护能力建设，同时，面向政企客户提供运营商级 DDoS 攻击防护服务。目前已涵盖互联网、金融、能源制造、政府机构等各个行业。

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。在国内外设有 40 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在检测防御类、安全评估类、安全平台类、远程安全运维服务、安全 SaaS 服务等领域，为客户提供入侵检测 / 防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及安全运营等专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

目录 CONTENTS

目录

1

执行摘要

执行摘要

2018 年，得益于互联网的快速发展，以及云计算、大数据、人工智能、物联网和工业 4.0 等技术与概念的落地，变革的触角伸向了网络空间和现实世界的各个角落，无时无刻不影响着人民的生活、商业的发展和国家的实力。在技术高速革新的背景下，网络空间面临的威胁，也在随之改变和升级。

技术环境和产业环境在变，攻防战场在变，网络攻击的手段和强度在迭代更新，DDoS 攻击从未缺席。在 2018 年 2 月，一次针对 DNS 服务器，并且基于 IPv6 协议的 DDoS 攻击首次载入史册，根据 DNS 提供商 Neustar 的研究，黑客正在部署新的 IPv6 攻击方法，而不是简单地使用 IPv6 协议复制 IPv4 攻击 [1]。2018 年 3 月，著名代码托管网站 GitHub 遭受到峰值达到 1.35Tbps 的 DDoS 攻击，攻击者利用暴露在公共互联网上的大批量 Memcached 服务器 (一种分布式缓存系统)，以及 Memcached 协议上存在的认证和设计缺陷，无需僵尸网络即能实现大规模的攻击流量；截至目前，基于 Memcached 协议的 DDoS 反射攻击已经创造了达到 1.7Tbps 峰值攻击 [2]。

攻击手段有效性和获利便捷性是 DDoS 攻击经久不衰的主要原因，DDoS 和挖矿活动在近两年高居攻击者选择榜首。在 2017 年，随着《网络安全法》的实施，以及下半年以比特币为代表的虚拟货币开始暴涨，黑产掌控下的优质 Botnet 资源从犯罪成本较高的 DDoS 攻击活动，转向了犯罪成本相对较低但收益更高的挖矿活动中。比特币价格的涨跌和 DDoS 的攻击流量有着明显的相关性。2018 年，我们发现，当挖矿的短期收益降低的时候，攻击者选择 DDoS 攻击的倾向性则相应增高。获利是攻击者永恒的诉求，DDoS 始终是攻击者手中的利剑之一，不容忽视。

本报告的第二章为 2017 年与 2018 年的 DDoS 态势对比分析以及总结 2018 年 DDoS 攻击的重要特点。在第三章，本报告通过攻击流量、频次、攻击规模变化情况，结合攻击资源分析，攻击类型分析，攻击持续时间、攻击地域分布、物联网设备参与度、攻击目标行业分布等多个维度力求全面呈现 2018 年 DDoS 攻击变化趋势，以便抛砖引玉，帮助组织及机构持续改善自身网络安全防御技术及体系。

1 https://www.scmagazineuk.com/first-true-native-ipv6-ddos-attack-spotted-wild/article/1473177

2 https://www.wired.com/story/github-ddos-memcached/

2

2018年DDoS攻击态势概览

2.1

2018 VS 2017

下降	攻击次数14.8万次，比2017年下降了28.4%
平稳	攻击总流量64.31万TB，与2017年相比变化不大
增加	单次攻击平均峰值达到了42.8Gbps，比2017年增加了204%
持平	单次攻击最高峰值1.4Tbps，与2017年基本持平
下降	平均攻击时长为42分钟，比2017年下降了17%

2.2

重要观点

观点1 2018年DDoS攻击规模持续普遍增大，DDoS即服务增长迅速。

观点2 DDoS攻击活动受政策监管、国家治理和利益驱动的影响明显。

观点3 DDoS反射型攻击放缓，综合多种攻击手段的DDoS攻击值得关注。

观点4 物联网威胁日渐增强，恶意软件利用的漏洞涵盖多种物联网设备。

观点5 DDoS攻击多发生于业务使用高峰期，以实现对目标的精准打击。

观点6 攻击目标的行业排名前三的是云服务/IDC，游戏，电商，行业内恶意竞争是主要攻击动机。

观点7 僵尸网络控制端主要分布在美国和中国。

观点8 中国仍是首要攻击源与攻击目标。

3

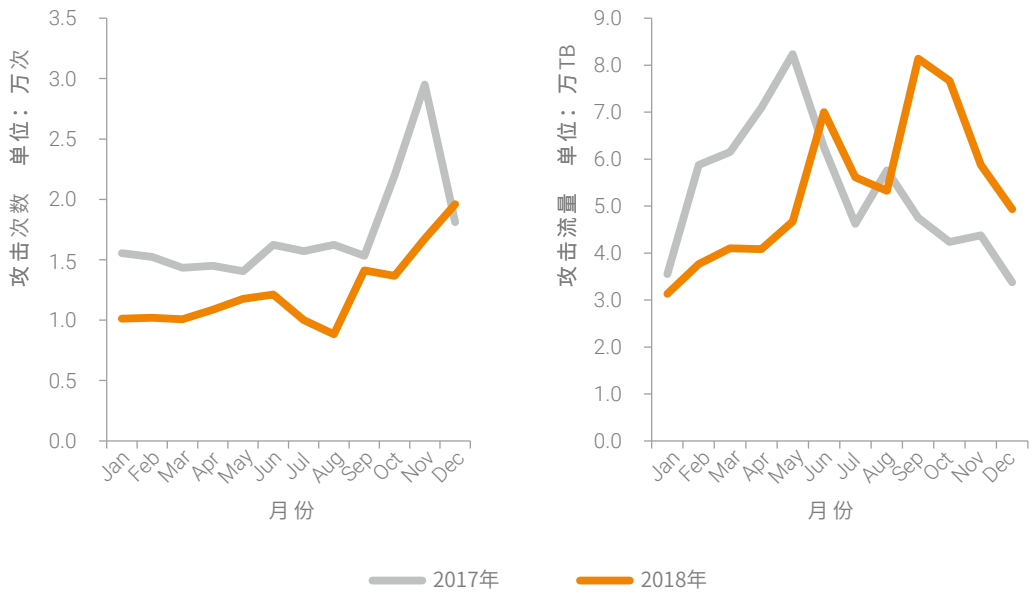
2018年DDoS攻击分析

3.1 DDoS 攻击次数和流量峰值情况

3.1.1 DDoS 攻击次数和攻击流量

2018 年，我们监控到 DDoS 攻击次数为 14.8 万次，攻击总流量 64.31 万 TB，与 2017 年相比，攻击次数下降了 28.4%，攻击总流量没有明显变化。这主要是因为 DDoS 攻击规模逐年增大，即中大型规模的攻击有所增加，具体见 3.1.2 节。

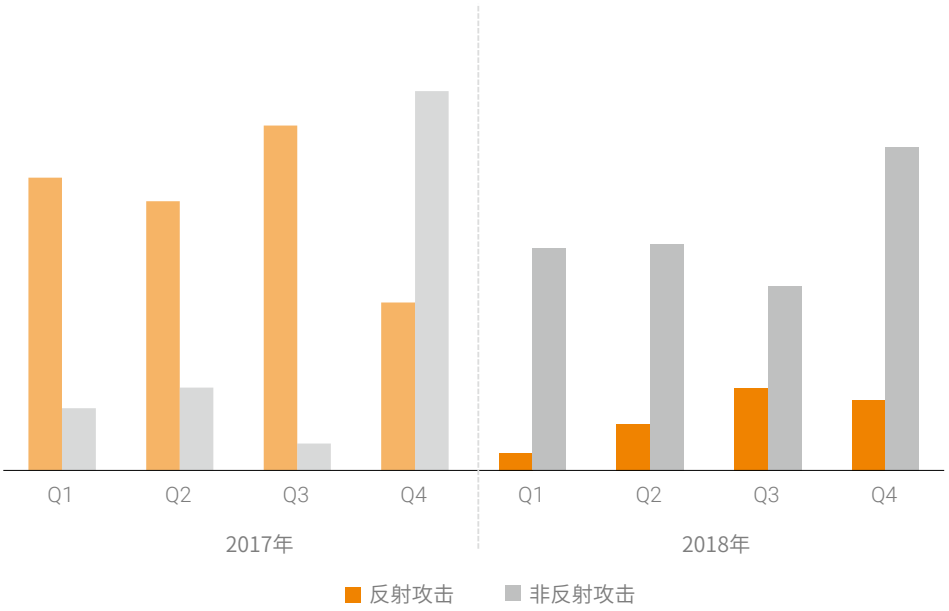
图 3.1 攻击次数与攻击流量



数据来源：中国电信云堤

从全年来看，2018 年 DDoS 攻击次数明显下降，得益于对反射攻击有效的治理。2018 年以来，CNCERT 组织各省分中心，联合各地运营商、 云服务商等对我国境内的攻击资源进行了专项治理，包括使用虚假源地址治理以及对反射攻击源通告等手段。通过治理，有效的减少了反射攻击的成功率，迫使攻击者转向其它攻击手段。从数据来看，2018 年反射攻击减少了 80%，而非反射攻击增加了 73%，反射攻击仅占 DDoS 攻击次数的 3%。

图 3.2 反射攻击次数与其他类型的攻击次数对比图



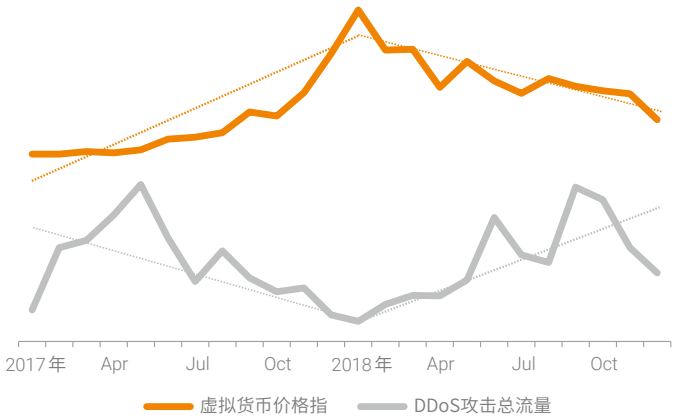
数据来源：中国电信云堤

从 2018 年各月攻击次数来看，上半年 DDoS 攻击逐月小幅增长，而下半年有加速增加的趋势。我们认为，DDoS 攻击逐月增加，与虚拟货币的价格回落相关。在《2017 DDoS 与 Web 应用攻击态势报告》[1] 中，我们指出，随着虚拟货币的升值，黑产开始将掌握的“优质” Botnet 资源从犯罪成本较高的 DDoS 攻击活动转而投向犯罪成本相对较低但收益更高的挖矿活动中。在 2018 年，随着虚拟货币的价格回落，挖矿的收益日益减少，攻击者选择 DDoS 攻击的倾向增高，DDoS 攻击逐月增加。

将各月份比特币价格与 DDoS 总流量趋势对比，其 Pearson 相关系数为 -0.48，呈一定的负相关性，这更加证实了我们去年的观点。

1 http://blog.nsfocus.net/2017-ddos-web-report/

图 3.3 比特币价格与 DDoS 攻击总流量趋势对比图

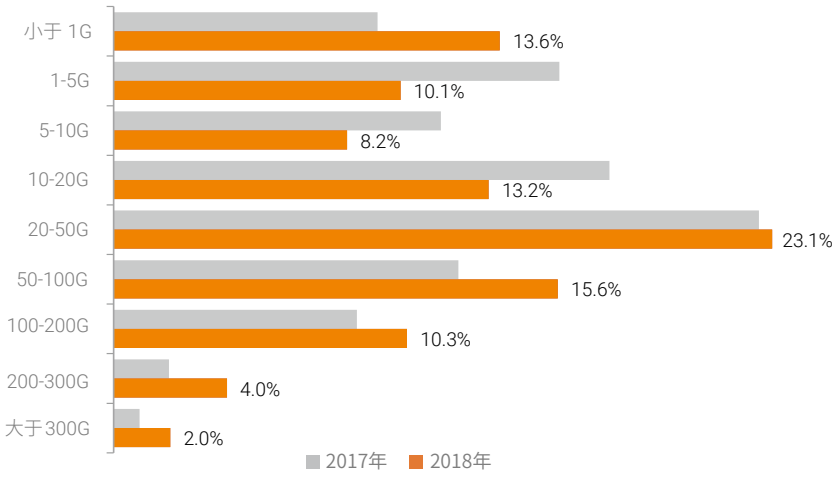


数据来源：中国电信云堤

3.1.2 攻击峰值分布

DDoS 攻击峰值以 20-50Gbps 为主，这部分攻击在全部攻击中占比 23.1%。和去年相比，攻击峰值分布向两侧分化，攻击峰值 20Gbps 以下的小规模攻击减少，攻击峰值 20-200Gbps 以上的中大型 DDoS 攻击有所增加，200Gbps 以上的超大模型攻击比例基本上成倍增加。

图 3.4 攻击峰值分布

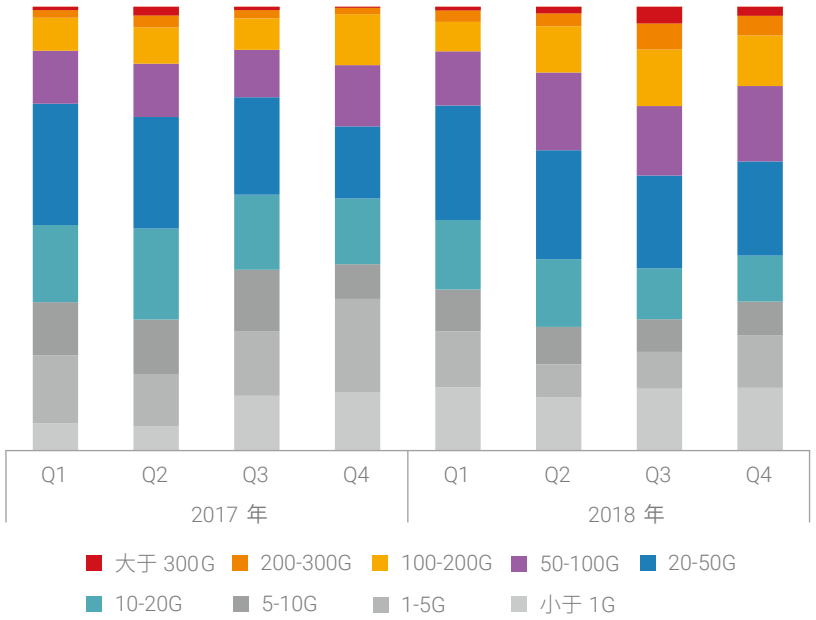


数据来源：中国电信云堤

2018 年 DDoS 攻击分析

从各季度来看，DDoS 攻击峰值在 100Gbps 以上的大型攻击持续增加，在进入 Q2 后，大型攻击明显增加，特别是在 Q3，大型攻击占了全部攻击的 23%。

图 3.5 2017 年 vs2018 年各季度各类规模攻击次数占比



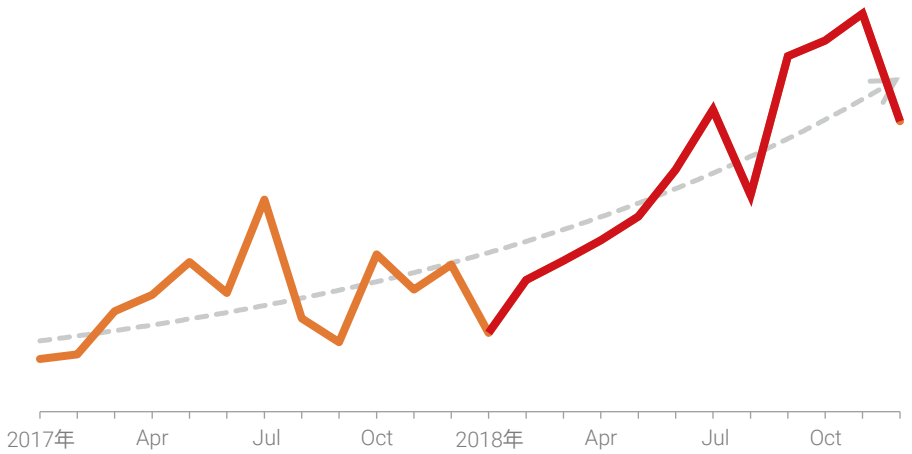
数据来源：中国电信云堤

近年来，超大规模的攻击事件日益普遍。2018 年 3 月，著名代码托管网站 GitHub 遭受到峰值达到 1.35Tbps 的 DDoS 攻击，而截至目前， DDoS 攻击已经创造了达到 1.7Tbps 峰值带宽的攻击[2]。

从最近两年各月数据来看，攻击峰值在 100Gbps 以上的大型攻击的次数呈加速上升趋势。大流量攻击事件的增多，说明攻击者掌握的攻击资源规模上升和攻击能力的增强。

2 https://www.wired.com/story/github-ddos-memcached/

图 3.6 峰值大于 100Gbps 的攻击次数变化



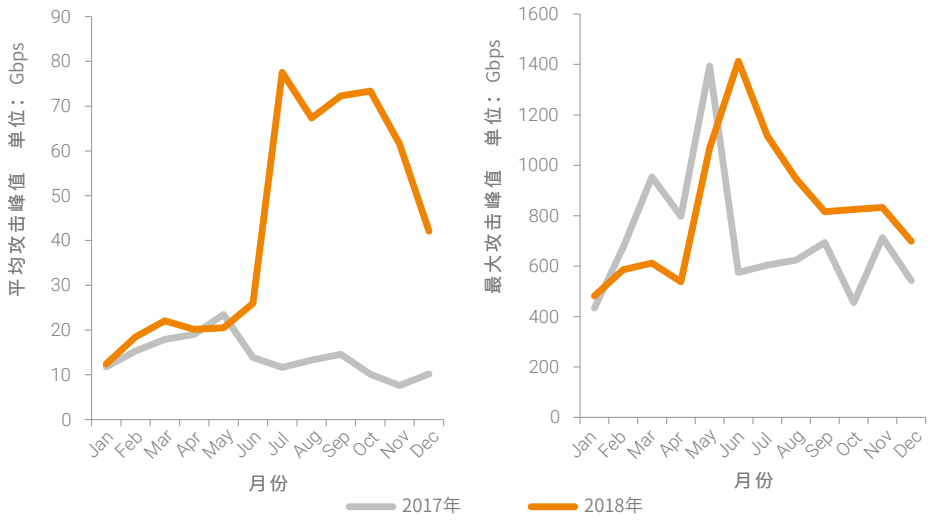
数据来源：中国电信云堤

3.1.3 单次攻击最高和平均峰值

2018 年，DDoS 攻击的平均峰值达到了 42.8Gbps，和 2017 年的 14.1Gbps 相比，增加了 2 倍有余。尤其是在 2018 年下半年，平均峰值达到 67Gbps，主要原因是网络带宽的普遍提高和攻击者掌控的 DDoS 攻击能力有了大幅的提升。

从最大峰值来看，我们检测到 2018 年 6 月份的某次攻击，最大峰值达到了 1.41Tbps，与去年基本持平。

图 3.7 攻击平均峰值和最高峰值



数据来源：中国电信云堤

无论是 DDoS 攻击能力的普遍提高，还是平均峰值创历史新高，都说明 DDoS 攻击态势的严峻性。可以说，黑客普遍拥有了释放特大流量的能力，并且能力仍然处于持续快速提高的进程中，这是防御和治理人员需要应对的挑战。

3.2 DDoS 攻击类型分析

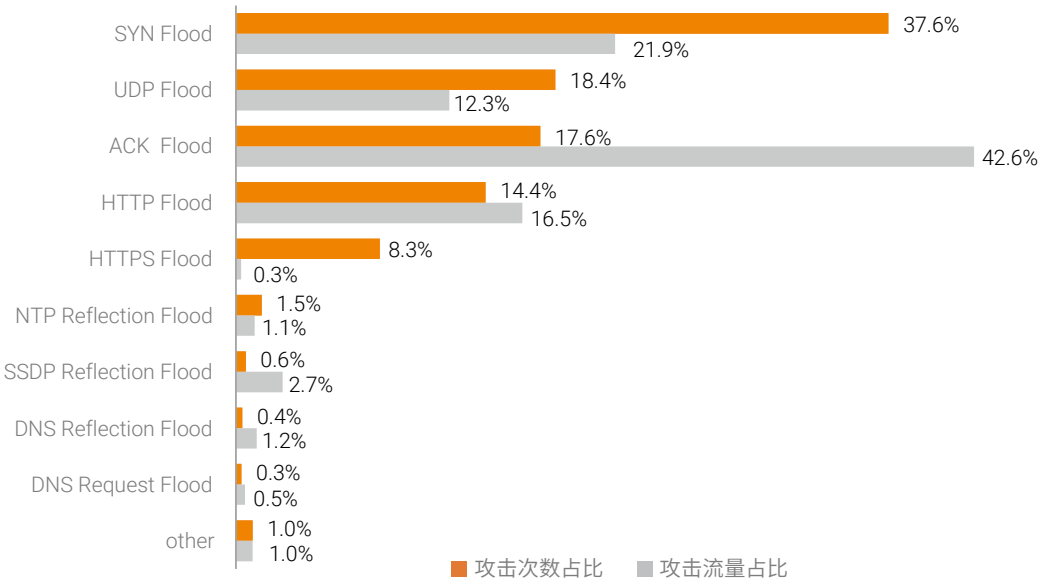
3.2.1 攻击类型占比

2018 年，主要的攻击类型[3]为 SYN Flood，UDP Flood，ACK Flood，HTTP Flood，HTTPS Flood，这五大类攻击占了总攻击次数的 96%，反射类攻击不足 3%。和 2017 年相比，反射类型的攻击次数大幅度减少了 80%，而非反射类攻击增加了 73%，之所以如此，是相关部门对反射源进行了有效的治理（见 3.1.1 节）。

从攻击流量来看，ACK Flood 占了全部流量的 42.6%。因为某些行业（如游戏），用户量大，会话数多，且多为长连接，容易受到 ACK 攻击，并且 ACK 报文比较大，从而产生大量的攻击流量。

3 此处对混合攻击进行了拆解

图 3.8 攻击类型的攻击次数分布



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

SYN Flood 依然是 DDoS 的主要攻击手法。攻击者利用 TCP 协议缺陷，发送大量的 TCP 连接请求，从而使得被攻击方资源耗尽的攻击方法。ACK Flood 很少单独使用，经常与 SYN Flood 一起使用，使主机和防火墙耗费大量的精力来计算 ACK 报文是否合法以致不堪重负，既消耗了目标的资源，又进行了流量攻击。

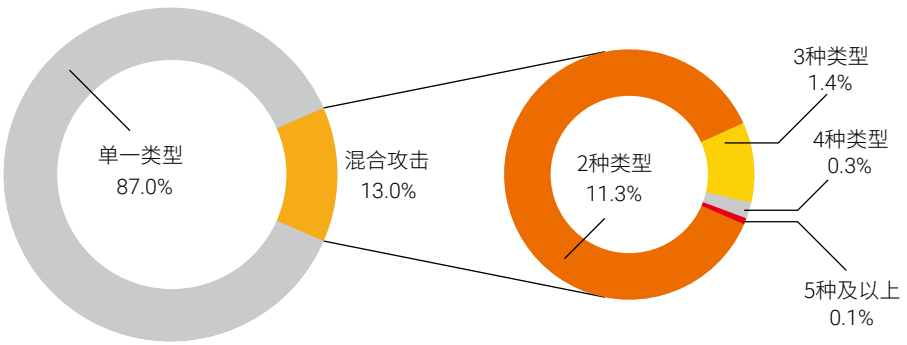
UDP Flood 是长期活跃的流量型 DDoS 攻击。常见的情况是利用大量 UDP 小包冲击 DNS 服务器或 Radius 认证服务器、流媒体视频服务器。UDP Flood 无需建立连接，协议简单，容易打出大流量攻击报文，因此深受攻击者的青睐。

HTTP Flood/HTTPS Flood 是针对 Web 服务在应用层发起的攻击，攻击者通过模拟正常用户对网站执行网页访问行为。这类攻击会引起严重的连锁反应，当客户端不断请求而且附带大量的数据库操作时，不仅直接导致被攻击的 Web 前端响应缓慢，还间接攻击到后端服务器程序，严重的情况下可造成数据库等后端服务卡死、崩溃，甚至对相关的主机，例如日志存储服务器和图片服务器都带来影响。

从 DDoS 攻击事件来看，有 13% 的攻击事件使用了多种攻击手法。攻击者根据目标系统的具体环境灵动组合，发动多种攻击手段，既具备了海量的流量，又利用了协议、系统的缺陷，尽其所能地展开攻

势。对于被攻击目标来说，需要面对不同协议、不同资源的分布式的攻击，分析、响应和处理的成本就会大大增加。

图 3.9 混合攻击分布



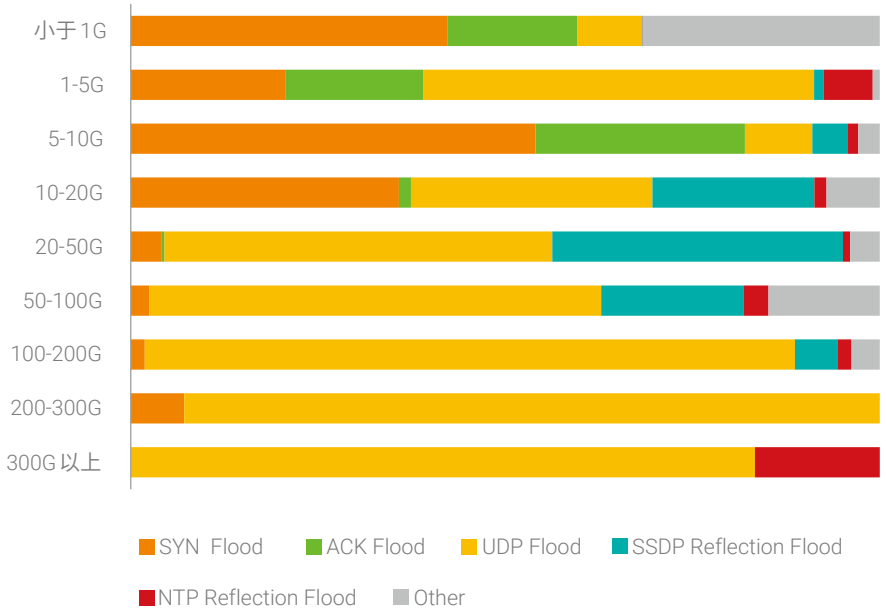
数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

3.2.2 攻击类型各流量区间分布

在 2018 年，峰值 10Gbps 以下的攻击以 SYN 及 ACK 等传统攻击手法为主；10Gbps-100Gbps 的攻击，主要使用了 UDP 及 SSDP 反射攻击两种手法；100Gbps 以上的大流量攻击中，UDP、NTP、SSDP 和 SYN 是主要的攻击手段。

与 2017 年数据相比，UDP 攻击替代了 SYN 攻击，在今年的大流量攻击中占据主导地位。SYN 报文大包的流行是去年 SYN Flood 主导大规模 DDoS 攻击的主要原因，但该攻击手段特征比较明显，较易被防护设备所拦截，也能看出攻防是在不断地迭代演进的。物联网安全态势日渐严峻，大量低功耗联网设备成为肉鸡，同时普遍扩大的带宽，使得 UDP Flood 这种无连接，低性能消耗和高带宽占用的攻击方式成为大规模 DDoS 中的主流。

图 3.10 DDoS 攻击类型各流量区间



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

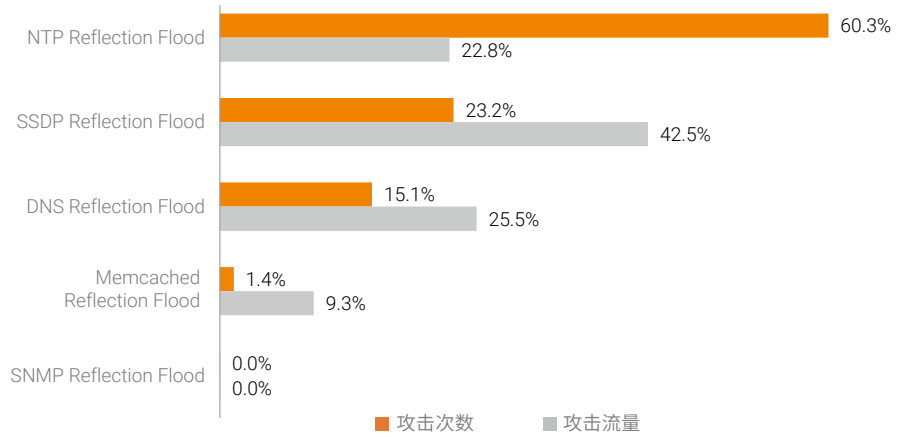
3.2.3 反射攻击

2018 年，虽然反射类型的攻击次数大幅减少，仅占全部攻击的 3%，但攻击流量却占了全部流量的 10%，由于反射攻击对流量的放大作用，其危害仍不可忽视。

从攻击次数来看，NTP 反射攻击独占鳌头，在全部反射攻击中占比 60%；从产生的流量来看，SSDP 反射攻击占了全部反射攻击流量的 42%。

2018 年 DDoS 攻击分析

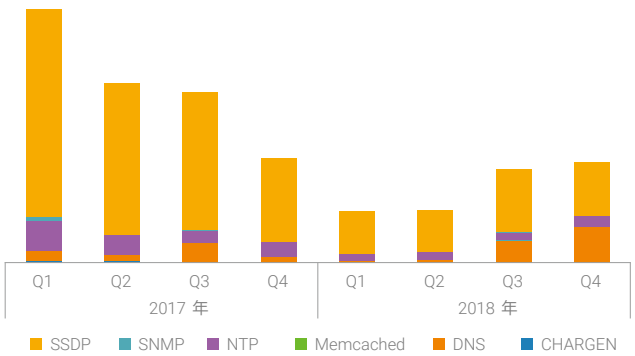
图 3.11 各类反射攻击次数与流量占比



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

从活跃反射源数量来看，2018 年下降了 60%，其中 SSDP 反射源有显著的减少，而 DNS 反射源有一定程度的增加。由此可见，相关部门对攻击源的治理，特别是 SSDP 反射源，是卓有成效的。

图 3.12 活跃反射源数量变化



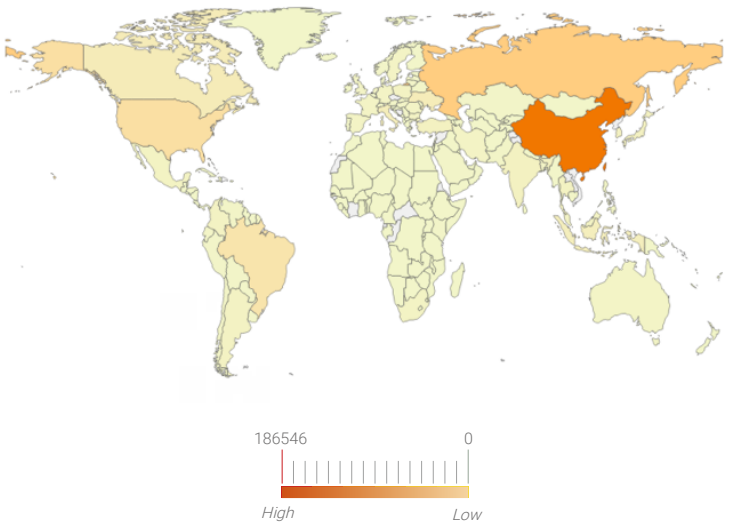
数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

对参与 DDoS 攻击的反射源的地理位置进行分析，从全球来看，反射源主要集中在中国，占了全部反射源的 46%，剩余 TOP5 国家依次是俄罗斯、美国、巴西和加拿大。

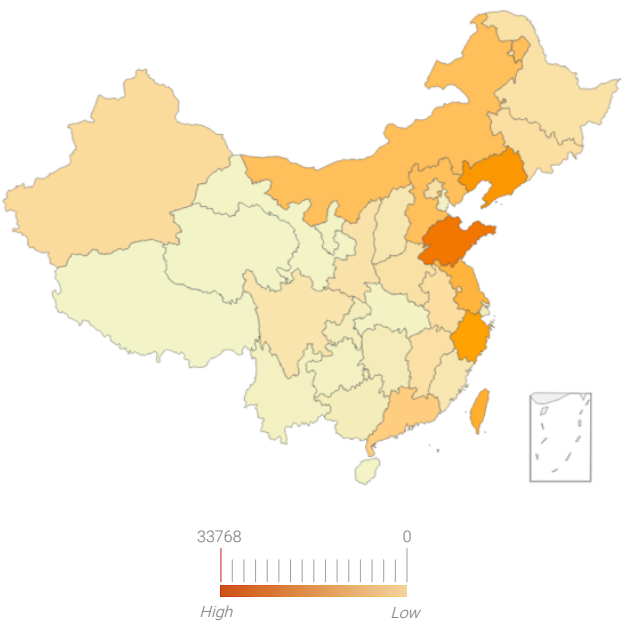
从国内来看，反射源分布最多的是山东省，占了全国反射源的 18%，其它依次为辽宁，浙江，台湾，江苏等省份。

图 3.13 DDoS 反射源境内分布

DDoS 反射源全球分布



DDoS 反射源全国分布



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

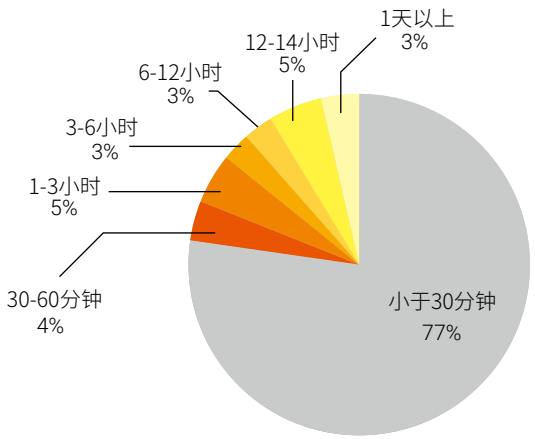
3.3 DDoS 攻击时间

3.3.1 DDoS 攻击持续时间占比

2018 年，DDoS 攻击的平均时长为 42 分钟，和 2017 年相比，下降了 17%，这说明随着 DDoS 攻击的服务化，产业化，工具化，攻击效率有了较大的提升。我们检测到，2018 年，持续时间最长的 DDoS 攻击在 12 天左右，也远远小于前期的攻击时长。

2018 年，短时攻击增加，攻击时长在 30 分钟以内的 DDoS 攻击占了全部攻击的 77%，和 2017 年相比，增加了 33%，但平均攻击流量却增加了 1.5 倍。该数据说明攻击者越来越重视攻击成本和效率，倾向于在短时间内，以极大的流量导致目标服务的用户掉线、延时、抖动。在长周期内，多次瞬时攻击能够严重影响目标服务质量，同时攻击成本得到有效控制。

图 3.14 攻击持续时间占比



数据来源：中国电信云堤

日渐缩短的单次攻击时长也让攻击者能够接收到更多的攻击任务，这也是僵尸网络即服务（Botnet-as-a-Service）和 DDoS 即服务（DDoS-as-a-Service）的重要特点之一[4]。以往，僵尸网络是由攻击者主动制作并扩散恶意软件以感染设备，并根据购买者的需求来操作这些设备发动大规模的 DDoS 攻击，其攻击时间亦完全取决于攻击者的工作时间，也是需要较高的技术水平和长时间的僵尸资源积累方能达成

4 http://blog.nsfocus.net/gafgy-botnet-baas/

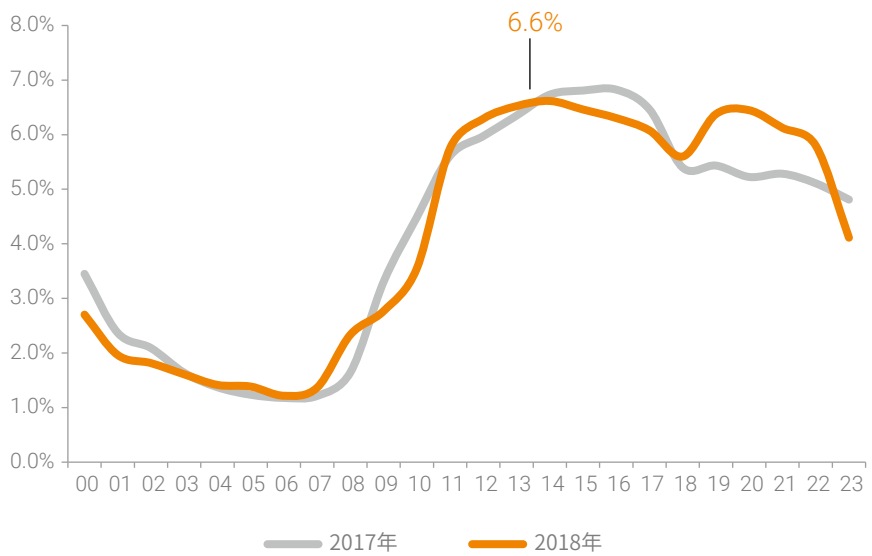
的，因此在很长一段时间内由于杀毒软件的普及，由僵尸网络引起的大规模 DDoS 攻击占比曾一度下降。而 Botnet-as-a-Service 模式的僵尸网络或 DDoS-as-a-Service 服务平台提供了租赁服务，即提供给没有僵尸资源和技术水平的用户一定时间内一定数量僵尸的使用权，并根据用户所需的规模、配置等参数的不同提供定制化的服务，加上自动支付平台的普及，用户们只要付款就可以即时获得一批佣兵式的攻击资源，不仅提供了随时随地发动攻击的敏捷性，也大大提高了作为用户时“一切都在自己控制下”的趣味性及对控制欲望的满足。这些因素降低了大规模 DDoS 攻击的发起门槛，也使得僵尸网络获利更为便捷。

3.3.2 DDoS 攻击时间画像

3.3.3 一天中 DDoS 攻击活动分布

从一天 24 小时攻击占比可知，业务高峰时段（10 点 -22 点）为攻击者发起 DDoS 攻击的高峰期，占全天攻击的 70%。这段时间也是在线业务的访问量高峰区间，攻击者在访问高峰期发起 DDoS 攻击，以此来提升攻击的效果和影响。

图 3.15 一天 24 小时 DDoS 攻击占比

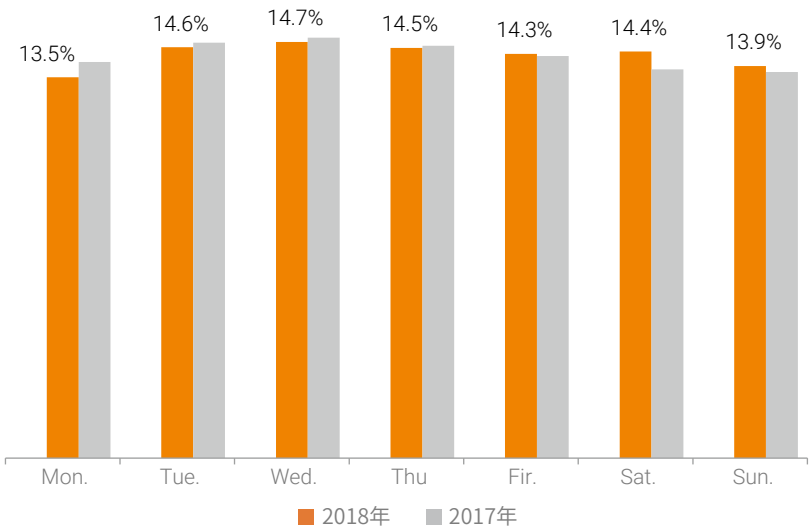


数据来源：中国电信云堤

3.3.4 一周中 DDoS 攻击活动分布

从每周中 DDoS 攻击活动的分布来看，一周中各天所发生的 DDoS 攻击事件比例并无明显差别。背后的一个重要原因是现有网络服务往往提供 7 X 24 服务，因而一周中每一天都可能被攻击。

图 3.16 一周七天 DDoS 攻击占比



数据来源：中国电信云堤

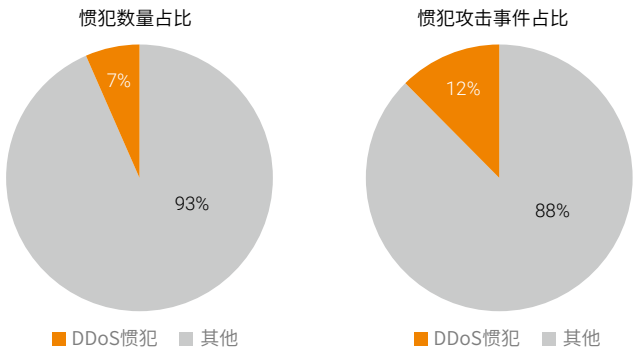
3.4 攻击资源行为分析

在《2018 上半年网络安全观察》[5] 中我们提到，DDoS 惯犯数量不容小觑，所有攻击类型中，25% 的惯犯承担了 40% 的攻击事件。在 DDoS 攻击中，7% 的 DDoS 惯犯承担了 12% 的攻击事件（此处，“DDoS 惯犯”意指发起过 DDoS 攻击且被威胁情报平台标记的攻击源 IP）。可以看出，在 DDoS 攻击中惯犯的比重有所减少，资源重复利用性较低，产生这种现象的原因主要有两个方面：首先，公共互联网上可供利用的攻击资源较多，攻击者通过多次扫描就能获得鲜活的攻击资源，而无需长期保活攻击资源。惯犯大多是互联网上长期存在安全隐患的资源，且极易被世界各地的攻击者利用。其次，DDoS 攻击通常位于攻击链的最后一环，当主机 / 设备资源被利用发起 DDoS 攻击时，此攻击资源也很容易被维护人员发现，

5 http://blog.nsfocus.net/network-security-observation-report-2018/

从而被修复。因此 DDoS 攻击中的僵尸主机，有很大一部分会丢失掉，就是俗称的“掉鸡”，从而需要黑客重新扫描、感染去扩大僵尸网络的规模。此外，我们注意到，无论哪种攻击类型，惯犯产生的攻击占比往往是其数量占比的将近 2 倍，其威胁程度较大，不容忽视。

图 3.17 惯犯的数量占比和攻击事件占比

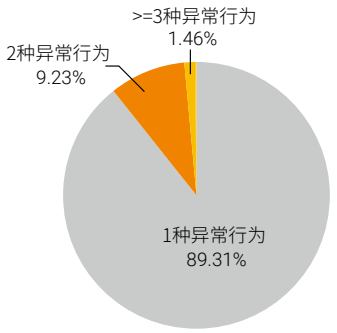


数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

3.4.1 攻击资源异常行为类型分析

参与 DDoS 攻击的攻击资源异常行为类型往往较为单一。在参与过 DDoS 的攻击源中，历史上只发起过一种异常行为的个数占 89%，少数攻击源发起过多种异常行为，最高达到 6 种。

图 3.18 DDoS 惯犯参与的攻击类型数量分布

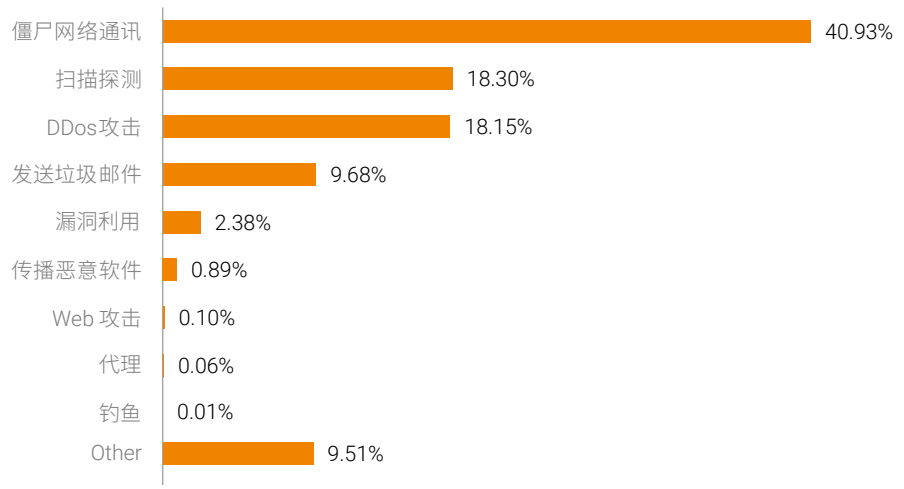


数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

从图 3.18 中的异常行为类型分布可知，41% 的攻击源曾被僵尸网络所控制；18% 的攻击源有过扫

描行为，扫描行为是攻击入侵的前期准备阶段，通过信息收集，掌握目标机器的系统，漏洞信息，对进一步进行入侵攻击起到关键作用；18% 的攻击源被威胁情报标记曾经多次进行 DDoS 攻击，这些攻击源往往包含能够被远程控制且长期未得到修复的漏洞，或具备反射能力。

图 3.19 DDoS 惯犯异常行为类型占比

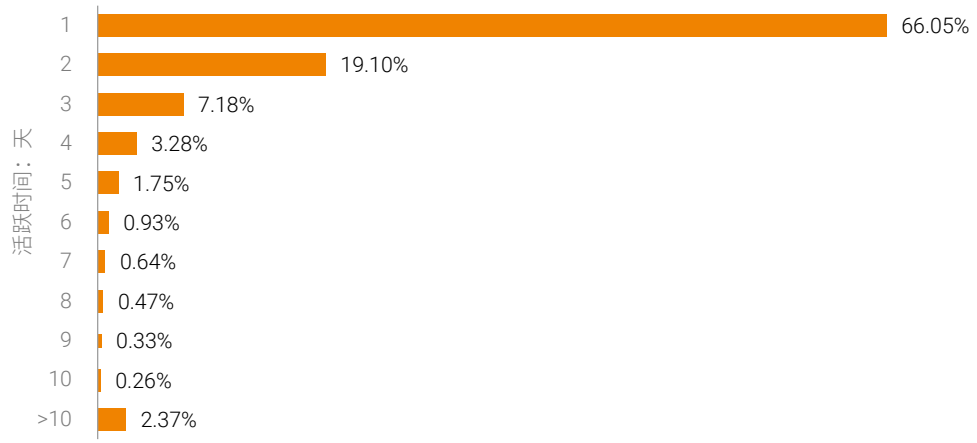


数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

3.4.2 攻击资源活跃度分析

在攻击源活跃时间的监测中发现，10 天是一个分水岭，活跃时间小于 10 天的占比 98%，大于 10 天的仅占 2%，最高达 280 天。95% 的攻击源活跃时间在 1 天到 5 天之间，一方面是由于攻击者为保证攻击资源的鲜活，防止攻击资源进入防护者的黑名单，打一枪换一炮；另一方面也侧面说明了公共互联网存在安全隐患的 IP 资源分布广泛，攻击者的获取成本极低且易行。

图 3.20 短期攻击资源活跃时间分布



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

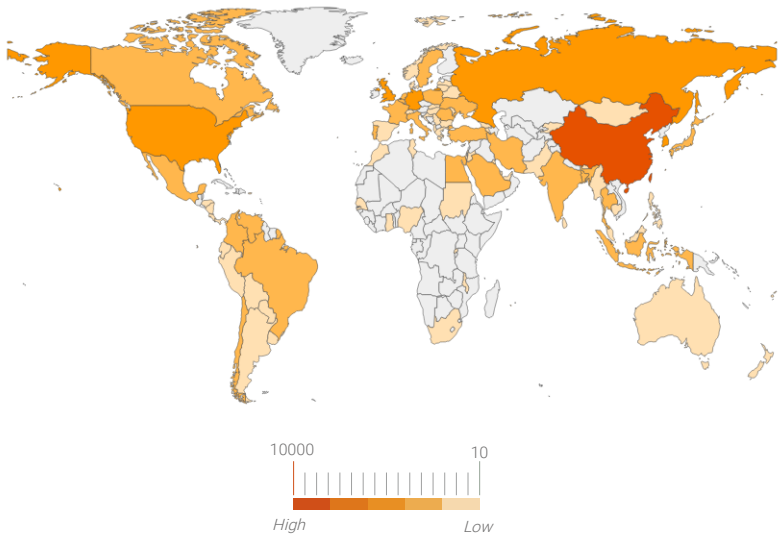
3.4.3 活跃攻击资源地域分布

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。

从全球分布来看，高活跃度攻击源在中国、美国以及俄罗斯数量最多。从国内来看，高活跃度攻击源在沿海和经济发达地区分布密集，其中广东、江苏、北京的高活跃度攻击源最多。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。

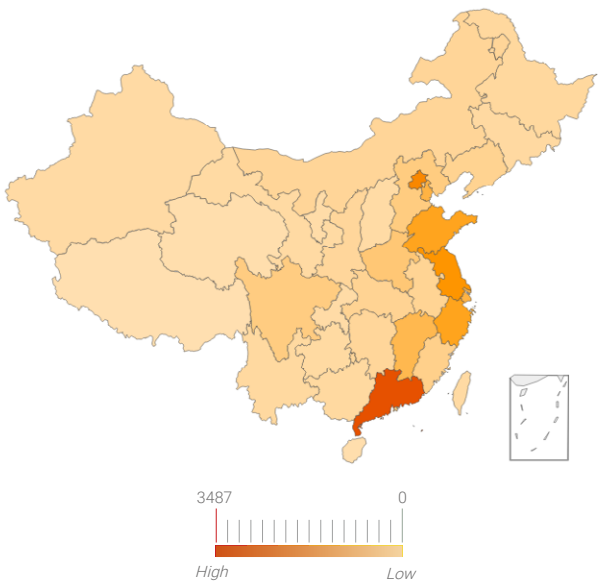
2018 年 DDoS 攻击分析

图 3.21 活跃程度较高的攻击资源全球分布



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

图 3.22 活跃程度较高的攻击资源全国分布



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

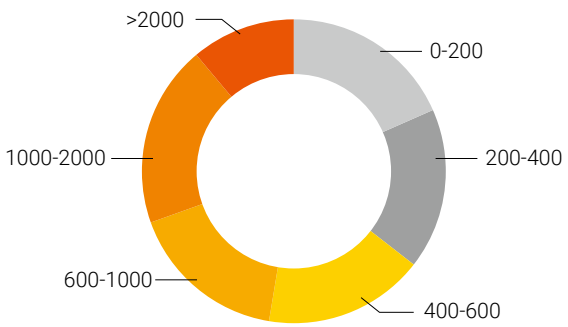
3.4.4 攻击资源团伙行为分析

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。基于绿盟科技近期发布的《IP 团伙行为分析》[6] 报告，我们在此仅从团伙规模和攻击流量、次数三个方面对攻击资源以群体方式勾结“作案”的行为进行简单介绍。

团伙规模

从团伙规模的整体分布来看，大多数团伙成员数量不到 1000，但我们也发现有一个团伙成员数量超过 26,000。

图 3.23 IP 团伙规模分布

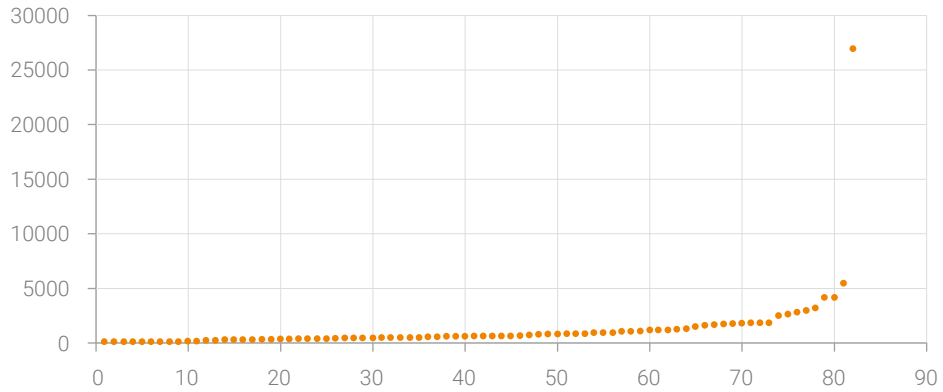


数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

6 http://blog.nsfocus.net/behavior_analysis_of_ip_chain_gangs/

图 3.24 展示了我们所识别的各 IP 团伙按规模大小的分布。图中的每个点代表一个团伙，共有 82 个团伙。

图 3.24 IP 团伙规模分布（每团伙）

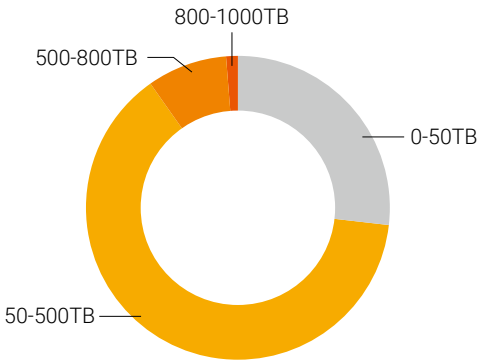


数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

攻击总流量

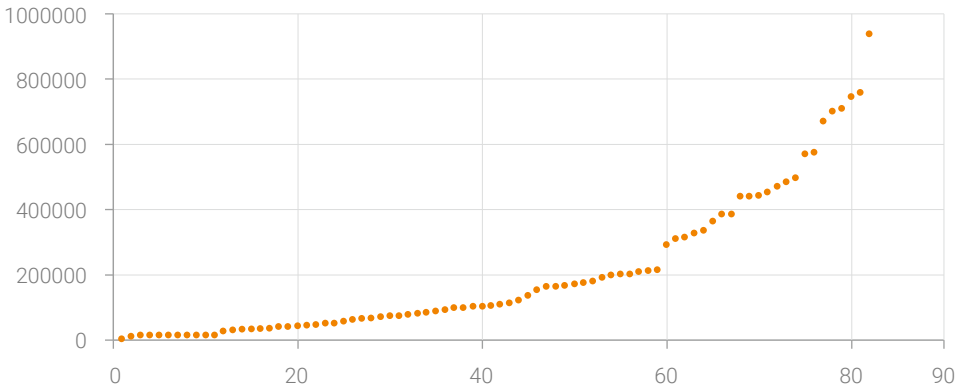
各团伙的攻击总流量分布情况，涵盖了来自同一团伙所有成员的全部攻击。虽然不同团伙的攻击总流量看似存在巨大差异，但大多数团伙的攻击总流量都超过了 50TB。

图 3.25 攻击总流量分布



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

图 3.26 攻击总流量分布 (GB)

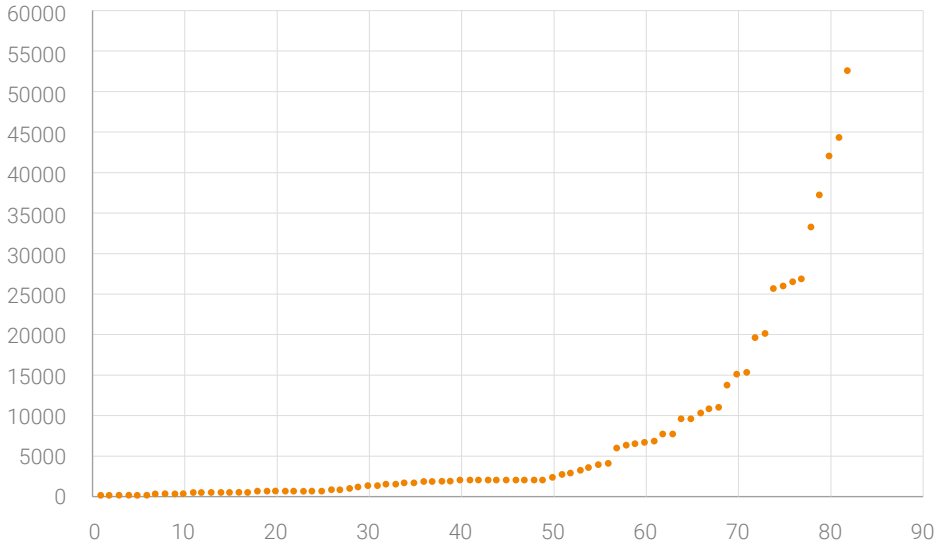


数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

攻击总次数

从各团伙的攻击总次数分布中可以看出近 60 个团伙所发起的攻击次数均在 5000 以内。毫不意外，大约 20%的团伙发起了 80%的攻击。

图 3.27 攻击总次数分布（每团伙）



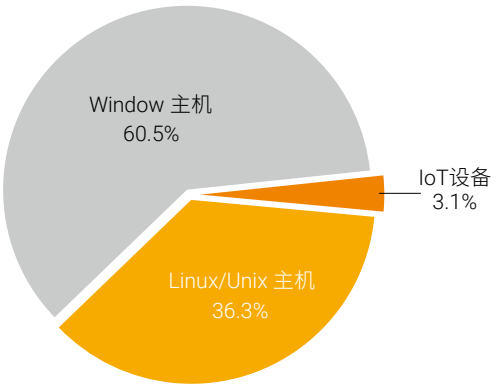
数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

3.5 物联网攻击资源分析

3.5.1 异常物联网设备的 DDoS 参与度分析

结合绿盟科技的物联网威胁情报、DDoS 攻击事件和物联网设备进行关联，进一步分析 DDoS 攻击源 IP 中的物联网设备比例可知，DDoS 攻击源 IP 中有 3.14% 为物联网设备，虽然占比较小，但是由于 DDoS 攻击源 IP 的基数较大，物联网设备所进行的 DDoS 攻击仍然不可小觑。

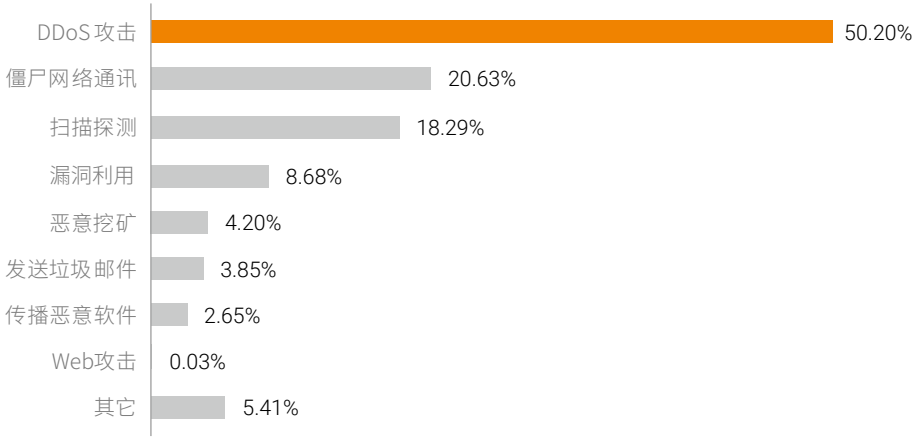
图 3.28 参与 DDoS 的物联网设备 IP 与全部 DDoS 的 IP 占比



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

我们监测到，全球异常物联网设备的 IP 总量为 408685 个，在全球物联网设备中占比 0.94%。其中参与过 DDoS 的物联网设备所使用过的 IP 数量为 205167，占全部异常物联网设备的 IP 总量的 50.20%。通过图 3.29 异常物联网设备异常行为占比可以看出，在异常物联网设备的异常行为中 DDoS 攻击占比是各个种类中最高的。可以说，异常物联网设备主要被利用进行 DDoS 攻击。

图 3.29 异常物联网设备异常行为占比 [7]



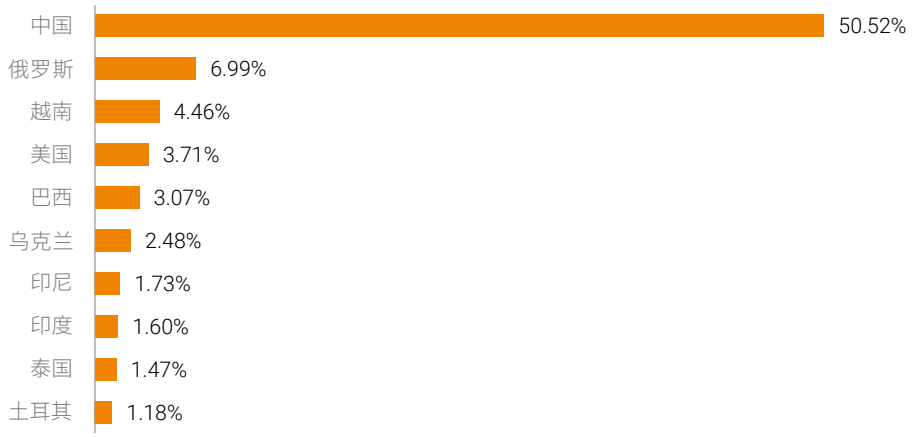
数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

3.5.2 参与 DDoS 攻击的物联网设备的地域分布

从全球视角对参与 DDoS 攻击的物联网设备的地域进行分析发现，参与 DDoS 攻击的物联网设备 IP 最多国家为中国，高达 9 万余 IP，其主要原因可能在于部署在国内的物联网设备的数据收集探针与国外相比较多。参与程度前五名国家还包括俄罗斯、越南、美国和巴西。

7 由于各某些设备有多种异常行为，从而导致图 3.29 中累计百分比大于 100%。

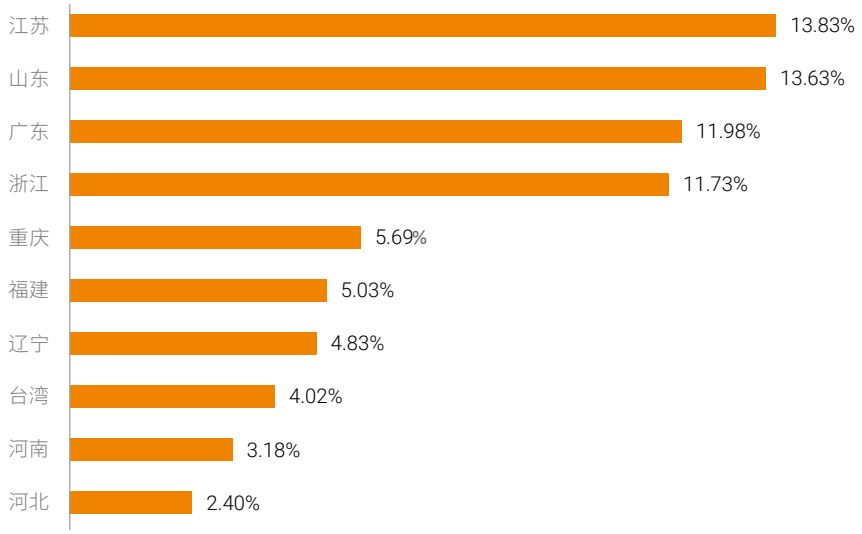
图 3.30 参与 DDoS 攻击的物联网设备的国家分布



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

从图 3.30 可知，中国的参与 DDoS 攻击的物联网设备的 IP 最多，因此接下来对国内省份的参与 DDoS 攻击的物联网设备的 IP 数量进行分析发现，省份总量的前四名分别为江苏、山东、广东和浙江。通过 2018 年各省份全年国内经济生产总值可知，前四名包括广东、江苏、山东和浙江。

图 3.31 参与 DDoS 攻击的物联网设备的国内分布



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

在《2018 年物联网安全年报》[8] 中指出，物联网设备的大批量普及与当地的高科技水平和服务业的繁荣是分不开的，经济发达的省份更有财力和动力采购、部署物联网设备和相关智能系统。广东、江苏、山东和浙江的 GDP 组成中第三产业服务业的产值均为其 GDP 的重要组成部分，这四省的经济总量与物联网设备的部署量是一致的。

因此，在广东、江苏、山东和浙江等省份经济大力发展的同时，也提高了物联网设备的普及程度，增加了省份的物联网设备的总量。由图 3.29 异常物联网设备异常行为占比可知，物联网设备的安全问题最突出的异常行为是 DDoS 攻击，因此在经济发达地区，物联网设备总量较高的地区，物联网设备的 DDoS 攻击威胁更加严重。

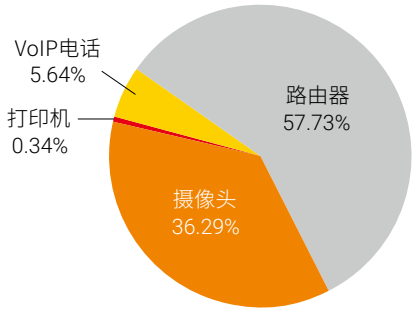
3.5.3 参与 DDoS 攻击的物联网设备类型分布

路由器和摄像头是物联网设备的重灾区，2018 年多个僵尸网络大量利用路由器漏洞和摄像头漏洞对该两类设备进行渗透控制，例如：2018 年 2 月，JenX [9] 利用 CVE-2017–17215 和 CVE-2014-8361 感染华为 HG532 路由器和运行 Realtek SDK 的设备形成僵尸网络，据报道其控制的设备数量至少有 2.9 万台；2017 年底爆出的 IoTroop [10] 的新型僵尸网络，则借用了一部分 Mirai 的代码。与 Mirai 类似，该恶意软件针对的是网络设备，例如由普联（TP-Link）、Avtech、MikroTik、Linksys、Synology 和 GoAhead 等公司制造的路由器和摄像头。据 Insikt Group 称 [11]，在这个僵尸网络中，有 80% 的设备是受感染的 MikroTik 路由器，其余 20% 由其他多种物联网设备组成，包括 Ubiquity、Cisco 和 ZyXEL 路由器等设备。

从设备类型角度进行分析可知，全部参与 DDoS 攻击的物联网设备总量超过 23 万，其中主要的设备类型为路由器和摄像头，该两类设备占总量的 94% 以上，这也符合当前物联网设备总量中的设备类型分布。

8 http://www.nsfocus.com.cn/content/details_62_2916.html
9 https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/jenx
10 https://www.hackeye.net/threatintelligence/13150.aspx
11 https://www.recordedfuture.com/mirai-botnet-iot/

图 3.32 参与 DDoS 攻击的物联网设备类型分布



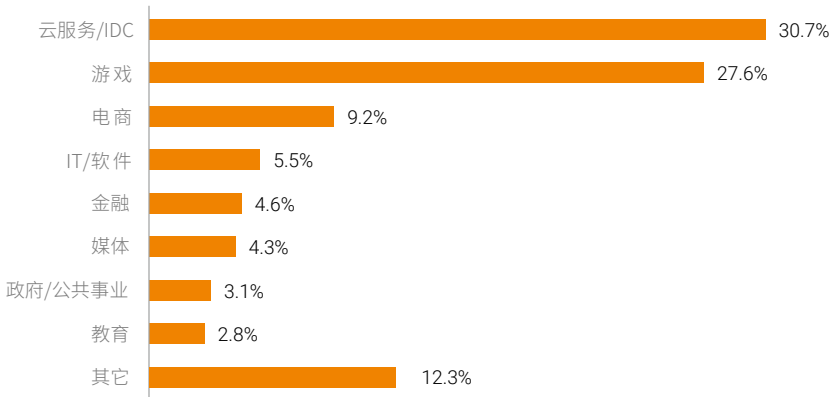
数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

3.6 攻击目标行业分布

从受到 DDoS 攻击的行业分布来看，依次是云服务 /IDC、游戏，电商。云服务 /IDC 为各行各业提供网络基础设施，受到 DDoS 攻击的比例是最高的。

游戏和电子商务这两个行业，由于对数据的即时性，连续性要求高，同行业之间的竞争激烈，且每天的流量大，变现快，成为攻击者眼中的“肥肉”，DDoS 攻击的重灾区。攻击者往往受雇于行业恶意竞争者，对竞争对手发起攻击，以此获得报酬，而竞争者则通过降低对手的服务质量来争抢用户资源。

图 3.33 攻击行业分布



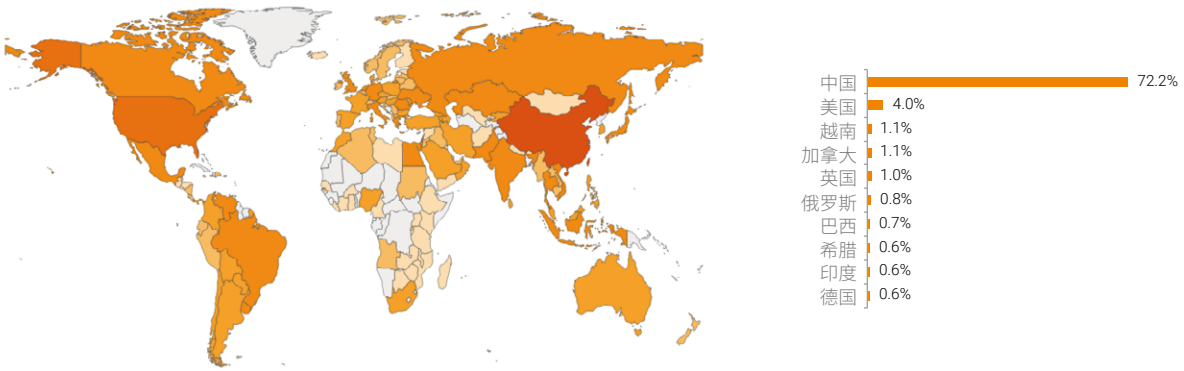
数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)、绿盟科技威胁情报中心

3.7 DDoS 攻击地域分布

3.7.1 DDoS 受控攻击源地域分布

我们监测到，2018 年中国依然是 DDoS 受控攻击源最多的国家，占比为 72%，其次是美国和越南。

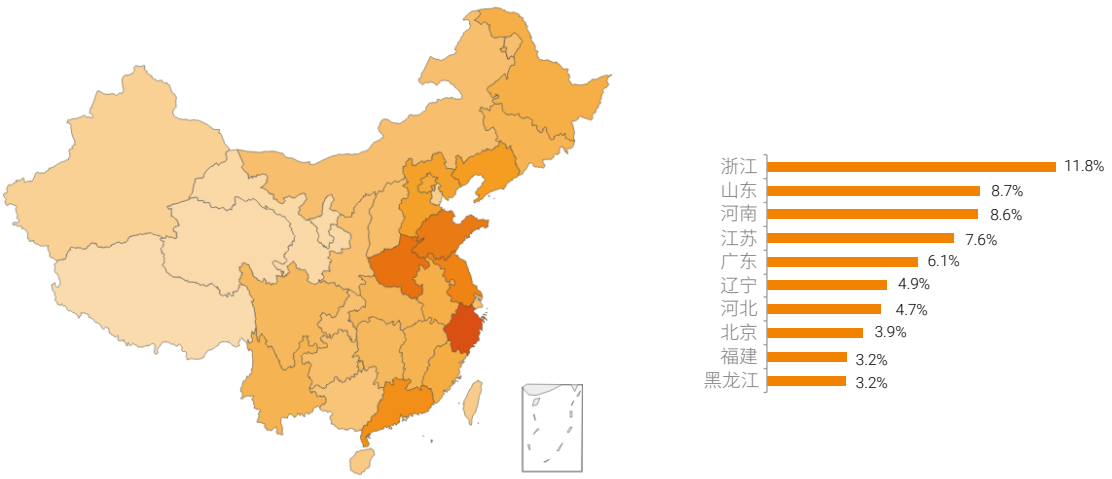
图 3.34 全球攻击源 IP 分布比例



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

2018 年，国内 DDoS 受控攻击源数目前三的省份是浙江，山东，河南。

图 3.35 全国攻击源 IP 分布比例

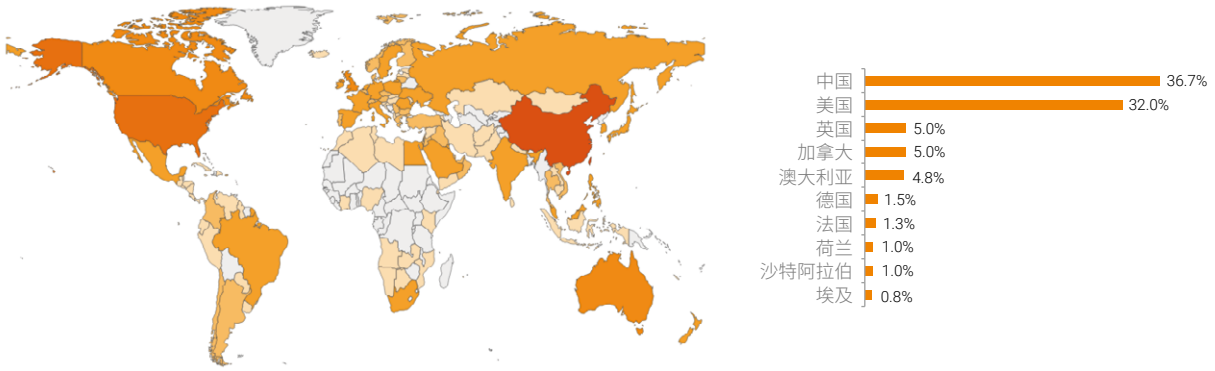


数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

3.7.2 DDoS 攻击目标地域分布

2018 年，受攻击最严重的国家是中国，约占全部攻击国家的 36%；其次是美国，占全部攻击的 32%。

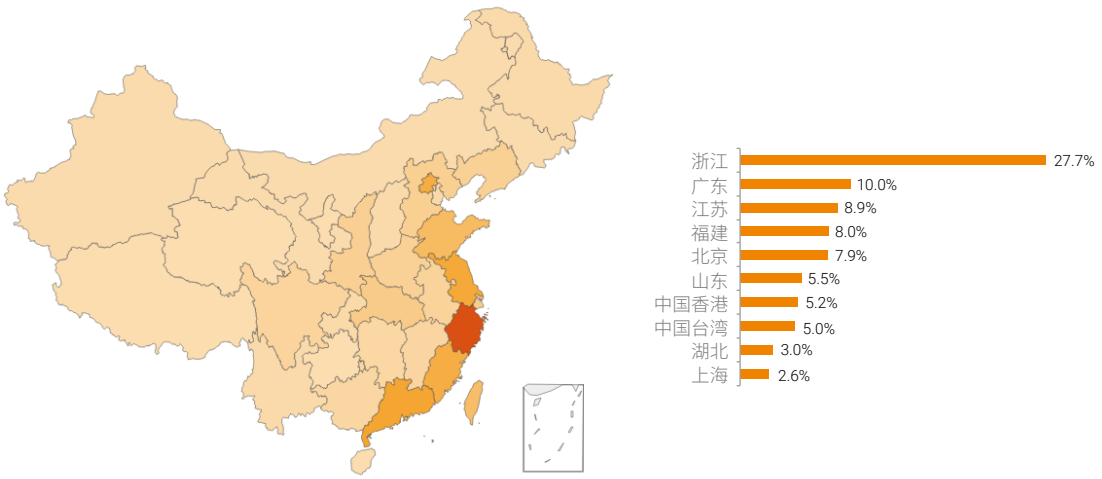
图 3.36 全球攻击目标 IP 分布比例



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

在国内，浙江是受 DDoS 攻击最多的省份，其它依次是广东，江苏，福建，北京。东部沿海依然是被 DDoS 攻击的高危地区。

图 3.37 全国被攻击目标 IP 分布比例

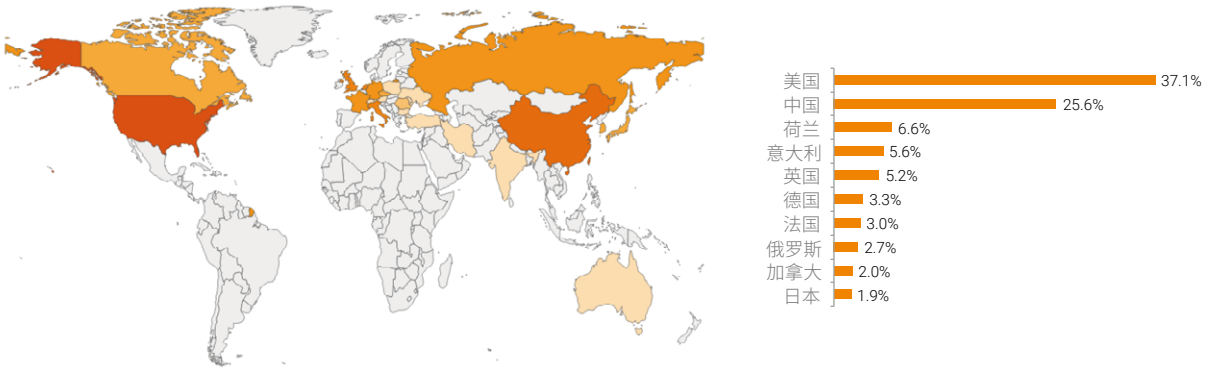


数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

3.7.3 DDoS 控制端地域分布

从世界范围来看，DDoS 控制端 IP 国家分布的 TOP3 为美国、中国和荷兰，三国的控制端数目占可追踪控制端数目的 70%。

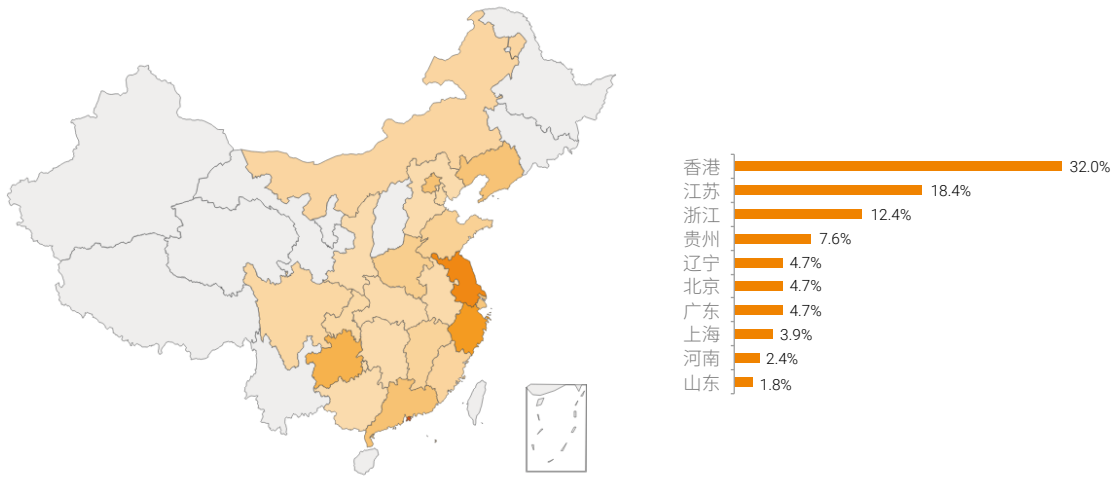
图 3.38 全球控制端分布比例



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

在国内，控制端 IP 数目前三的有香港，江苏，浙江，占国内可追踪控制端的 60% 以上。

图 3.39 全国控制端分布比例



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

4

DDoS防护与治理

DDoS 攻击背后涉及错综复杂的黑色产业利益关系，有效的治理需要从政策、产业、资源、技术多个维度入手。在此，我们从以下几个角度来简单介绍针对 DDoS 攻击的治理的切入点。

4.1 网络架构技术升级

计算机技术及互联网产业的发展过程中，在架构、技术层面，有一些先天缺陷和后天不足，为 DDoS 攻击的发起提供了温床。

比如，缺乏有效的地址识别及溯源手段，以地址伪造为核心的多种攻击方式被广泛利用。在现有的网络架构下，伪造地址一方面能够隐匿攻击者的身份，另一方面，反射攻击正是通过伪造源 IP 的请求数据发起的。

此外，缺乏统一的网络流量管控手段，导致对 DDoS 攻击检测、预警、响应的滞后，扩大了攻击的影响面。DDoS 攻击的规模化、分布式特点，使得现有异构、复杂的网络架构难以及时发现 DDoS 攻击的早期迹象，当 DDoS 攻击全面发起之后，又难以快速隔离恶意流量和目标设备。

庆幸的是，随着网络技术、计算技术的发展，以及相关标准的指定，以上问题得到很大的缓解。例如，以软件定义网络 SDN 为代表的网络数据平面、管理平面分离技术方案，为网络流量、网络节点的全局、智能化管理提供了关键基础；资源虚拟化等云计算核心能力，为云端网络资源的隔离、容错和恢复能力提供了支撑；以数据包标记、过滤为目标的多种算法、标准的提出，能够有效减少伪造地址数据包的传输途径。

4.2 暴露服务管理

DDoS 攻击需要掌握大规模的攻击资源，而互联网中大量的开放服务则是攻击者潜在的可利用攻击资源，例如反射型 DDoS 频繁利用互联网中开放的公共服务，或者意外暴露的内网服务，发起大规模攻击。这些暴露在互联网中并可能被恶意利用的服务资源数量及其庞大。针对开放服务，如对外的 DNS 服务和 NTP 服务等，需要相关部门、资产持有企业排查服务的脆弱性，加强响应策略的控制，部署有效的检测机制，防止被恶意利用；针对意外暴露的内网服务及协议，如 SSDP，Memcached 和内网 DNS 等等，需要相关企业加强网络的隔离措施，强化相关人员的安全意识，防止内网服务的意外暴露。

4.3 僵尸网络治理

僵尸网络一直都是网络黑产发起 DDoS 攻击的主力军。攻击者通过各类蠕虫病毒、恶意软件的投放，感染病控制了大规模的僵尸机器。治理僵尸网络，一方面需要从恶意样本入手，分析攻击手段，从攻击链的各环节加强防护措施；另一方面，需要更强化的主动防御策略，监控僵尸网络动向，对 DDoS 攻击进行早期检测、预警以及溯源。比如，通过蜜罐、蜜网技术，主动获取恶意样本、捕获恶意流量行为，通过关联分析，识别攻击者的攻击意图，破解其攻击手段，打破其攻击链条。

4.4 流量可视化

要做好 DDoS 的防护和治理，具备可见能力尤为重要。

随着人们日益增长的网络使用需求，以及 IPv6、5G 等技术的快速发展，网络带宽迅速增加。传统的流量可视化技术已跟不上大流量网络可视化的发展，比如，DPI 技术有着高昂的建设成本，传统 DFI 技术的应用分析能力不足。这给流量可视化成本 (ROI) 带来极大挑战。

在当前网络流量中，热点流量、是否恶意、恶意类型、流量流向、区域位置、国家信息、公司名称、设备类型、应用名称、CDN 识别等这些都是重要的流量可视化信息，管理者只有全局掌控各方面信息，才能快速监控和处置异常事件。换句话说，流量可视化能力是衡量管理者防护和治理 DDoS 能力的一大指标。

5

总结

总结

获利是攻击者永恒的诉求，DDoS 始终是攻击者手中的利剑之一。

DDoS 攻击有着见效快和获利便捷等优势，将会长期受到攻击者的青睐。产业和技术的变革，意味着 DDoS 攻击会以更多的形态出现在攻防的战场上。

DDoS 的防护，同样也不能因循守旧，要充分利用大数据和人工智能技术，提供更有效的预警和检测方案，充分利用云清洗服务和威胁情报，在监管机构和安全厂商之间共享威胁信息，协同防御，合作共赢。

作者

中国电信　云堤

绿盟科技　天枢实验室　伏影实验室

编辑

绿盟科技　鄢君 (平面设计)

中国电信·云堤 CHINA TELECOM

NSFOCUS

2018 DDoS攻击态势报告

中国电信云堤官方微信

绿盟科技官方微信