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（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 30 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，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，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

内容提要

纵观 2016 全年 DDoS 威胁态势，DDoS 攻击次数和规模不断上升，攻击手段和策略也越来越复杂。2016 年单我国境内就发生 DDoS 攻击约 22 万次，与去年同期相比增长 18.6%，且大流量攻击事件较 2015 年有明显增多，攻击峰值在 50-100Gbps 的攻击总数在 2016 Q4 季度同比增长 172.6%，峰值大于 300Gbps 的攻击次数在 Q3 季度同比增长 522.2%。DDoS 攻击打击目标不再只是政府、金融、游戏，已经扩张到各行各业，DDoS 勒索事件频发；黑客攻击手段也越来越高明，不惜精心策划攻击策略，以套取更大利益。僵尸网络感染平台继续扩张，物联网设备大面积沦陷，DDoS 攻击规模屡创新高，造成的影响和破坏力越来越大，不断刷新人们对 DDoS 攻击的认知。面对不断升级的 DDoS 威胁，为了跟踪及呈现 DDoS 攻击的变化趋势，中国电信云堤联合绿盟科技发布《2016 DDoS 威胁报告》。

本报告从 DDoS 数据着手，通过攻击次数、峰值、时间、协议类型、攻击源、攻击目标、僵尸网络发展情况等多维度深入挖掘分析，展示 2016 年 DDoS 攻击变化情况；再结合 2016 年全球最具代表性的多个 DDoS 攻击事件分析，洞悉 2016 年 DDoS 发展方向，揭示 DDoS 防护趋势，为大家呈现 2016 年 DDoS 整体威胁趋势。进而帮助各组织及机构持续改善自己的 DDoS 防护技术及体系。

如果您需要了解更多信息，请手机扫码关注：

中国电信云堤官微

绿盟科技官微

特别声明

为避免合作伙伴及客户数据泄露，所有数据在进行分析前都已经过匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在本报告中。

执行摘要

多年来，绿盟科技致力于帮助客户实现业务的安全顺畅运行。每天，绿盟科技的 DDoS 威胁态势感知平台及相关防护产品都会发现数以千计的 DDoS（分布式拒绝服务）攻击危害客户的业务安全。为了跟踪及呈现 DDoS 攻击的相关情报，进而帮助各组织及机构持续改善自己的 DDoS 防护技术及体系，绿盟科技发布**《2016 DDoS 威胁报告》**。

数据来源

本次报告中涉及的所有数据，来源于绿盟科技的全球 DDoS 攻击态势感知平台、威胁情报系统、绿盟抗拒绝服务系统，以及两家合作伙伴所提供的数据，他们是中国电信云堤、金山安全。中国电信云堤提供了国内电信运营商的大网数据，便于更为全面的呈现大规模 DDoS 攻击流量及特性；金山安全提供了 Botnet 在全球及中国的分布数据，便于呈现其规模及其潜在的危害性。这两方面的数据结合绿盟科技的各平台的数据及分析，让本报告得以从全网大流量、Botnet 发展尤其是物联网 Botnet 的发展等角度立体化呈现 2016 年 DDoS 威胁的发展态势。

分析方法

本报告中流量数据分析基于 NetFlow 协议进行，是业界公认的一种统计方法，便于分析 DDoS 攻击流量构成、协议分布以及攻击行为。其中全局态势分析以中国国内攻击总流量统计数据为基础，进行多维度多层次关联分析；而与事件相关的流量区间及类型分析，则是按照攻击事件来进行统计而非流量大小进行计算的。

1. 2016 DDoS 态势概览

- 1. 2016 vs.2015 DDoS 攻击次数同比增长 18.6%
- 2. 2016 vs.2015 DDoS 攻击流量总值同比增长 25%
- 3. 2016 年 DDoS 攻击流量峰值大于 300Gbps 成为常态
- 4. 2016 DDoS 短时攻击增加，在 30 分钟以内结束的占 51.4%
- 5. 2016 攻击流量最大的 2 种攻击类型依然是 SYN 和 UDP Flood
- 6. 2016 反射攻击流行，NTP 和 SSDP Reflection Flood 猖獗
- 7. 2016 中国依然是受 DDoS 攻击最严重地区，其次是美国、法国、英国、德国
- 8. 越是互联网发达地区，DDoS 攻击越频繁，2016 国内发起 DDoS 攻击的源头主要来自广东、浙江、北京、江苏、上海
- 9. 2016 物联网僵尸网络规模迅速扩张
- 10. 2016 来自物联网的 DDoS 攻击增长明显，应用层 DDoS 的防护难度增大
- 11. 2016 各国开始推动 IoT 安全立法，治理 IoT 刻不容缓

中国电信·云堤 CHINA TELECOM

NSFOCUS

2016 DD
攻击者画

专注

攻击者不再是昼伏夜出，打 D 不再是兼职

- 一年当中 6-8 月份，是 DDoS 攻击者最忙碌的月份
- 攻击者在一天之中 11-16 点、17-21 点发起攻击最多（网络使用最频繁）
- 3 点 -7 点攻击较少（业务低谷期）

嗅探

为了更大流量和隐蔽，攻击者不断寻找更多可利用的资源

- 2016 年 BotMaster 主要分布在中国、俄罗斯、美国、巴西和土耳其
- 除了传统网络，僵尸网络已经渗透进入了物联网
- 甚至僵尸网络已经被用于黑产链中的牟利

攻击者不再是昼伏
不再是兼

为了更大流量和隐蔽，
更多可利用

攻击者也有自己的老板，

如果自己的能力不具备，D
资源整

黑产充满了邪恶，攻
厮杀

oS
像

夜出，打 D
职

攻击者不断寻找
的资源

也需要考虑投入产出比

DoS 攻击者也会进行
合

攻击者之间互相

精细

攻击者也有自己的老板，也需要考虑投入产出比

- 大流量攻击凶猛而短暂，百 G 以上的攻击大多 5 个小时就结束了
- 小流量攻击持续不断，甚至可以持续数天
- 反射型攻击，以其隐藏性高、成本低，相当多的攻击者都选择它

整合

如果自己的能力不具备，DDoS 攻击者也会进行资源整合

- DDoS 攻击者常常利用木马，控制更大规模及类型的僵尸网络
- 台风 DDoS 控制端，14% 的 C&C 都来自国内多家知名云
- 黑产者已经将 DDoS 攻击能力平台化，任何人都可以购买攻击服务

黑吃黑

黑产充满了邪恶，攻击者之间互相厮杀

- 僵尸网络的资源一旦聚集在某个组织手里，它就会成为撕咬的对象
- 黑产者甚至会攻击政府组织，攻击 CIA、FBI 的事件屡见不鲜
- 勒索软件等先进的攻击工具，也成为互相绑架的对象

2. 2016 DDoS 攻击趋势

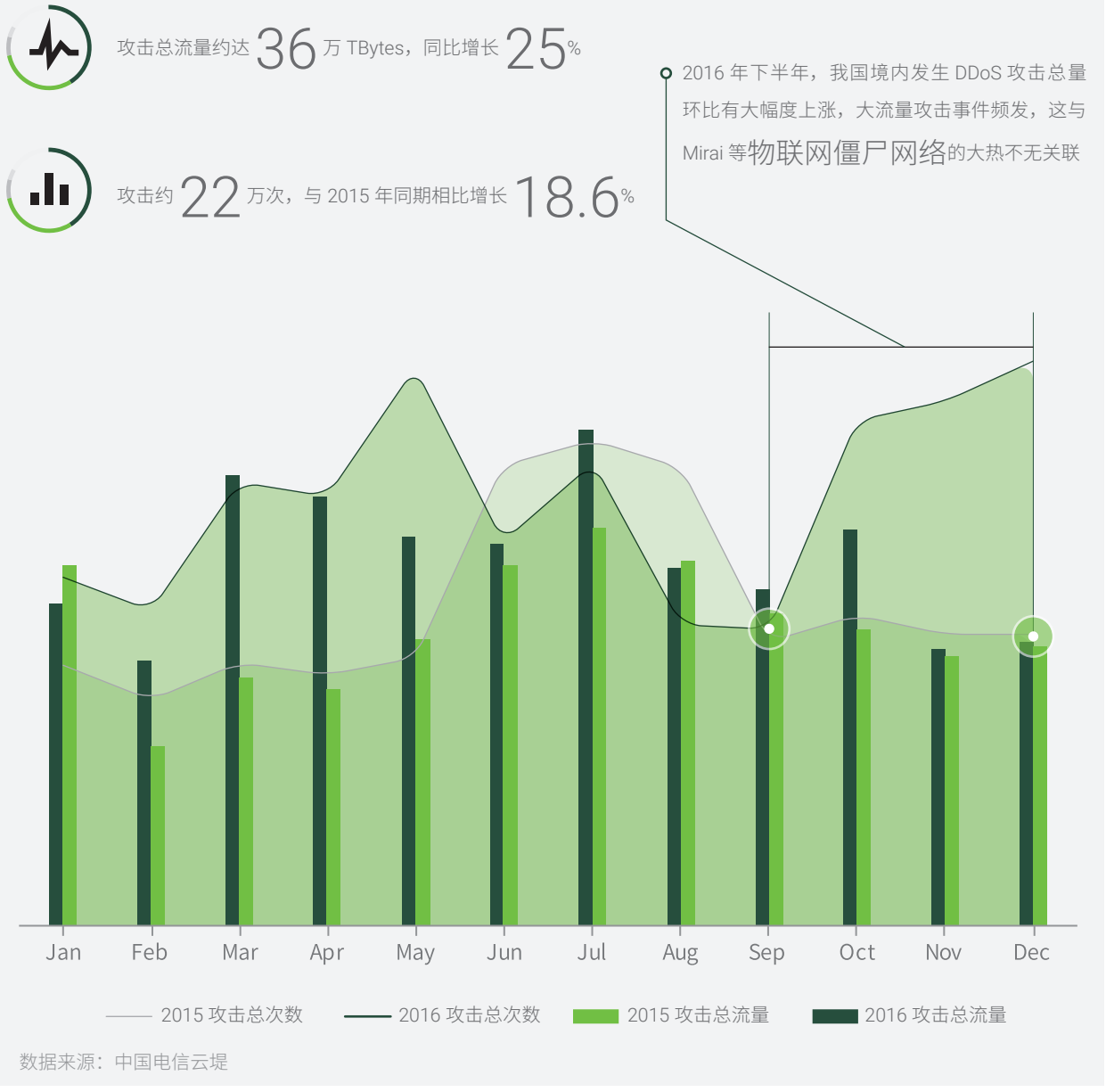
2.1 DDoS 攻击次数和流量峰值

2.1.1 DDoS 攻击次数和攻击流量

2016 年我国境内共发生 DDoS 攻击约 22 万次，与去年同期相比增长 18.6%，除了 1 月份外，其余各月份攻击次数均高于 15 年同期。攻击总流量约达 36 万 TBytes，同比增长 25%。

2016 年上半年，我国境内发生 DDoS 攻击呈现波动上升的趋势，下半年攻击总量环比有大幅度上涨，大流量攻击事件频发，这与 Mirai 等物联网僵尸网络的大热不无关联。

图 2.1 2016 vs. 2015 各月份 DDoS 攻击次数和流量趋势图



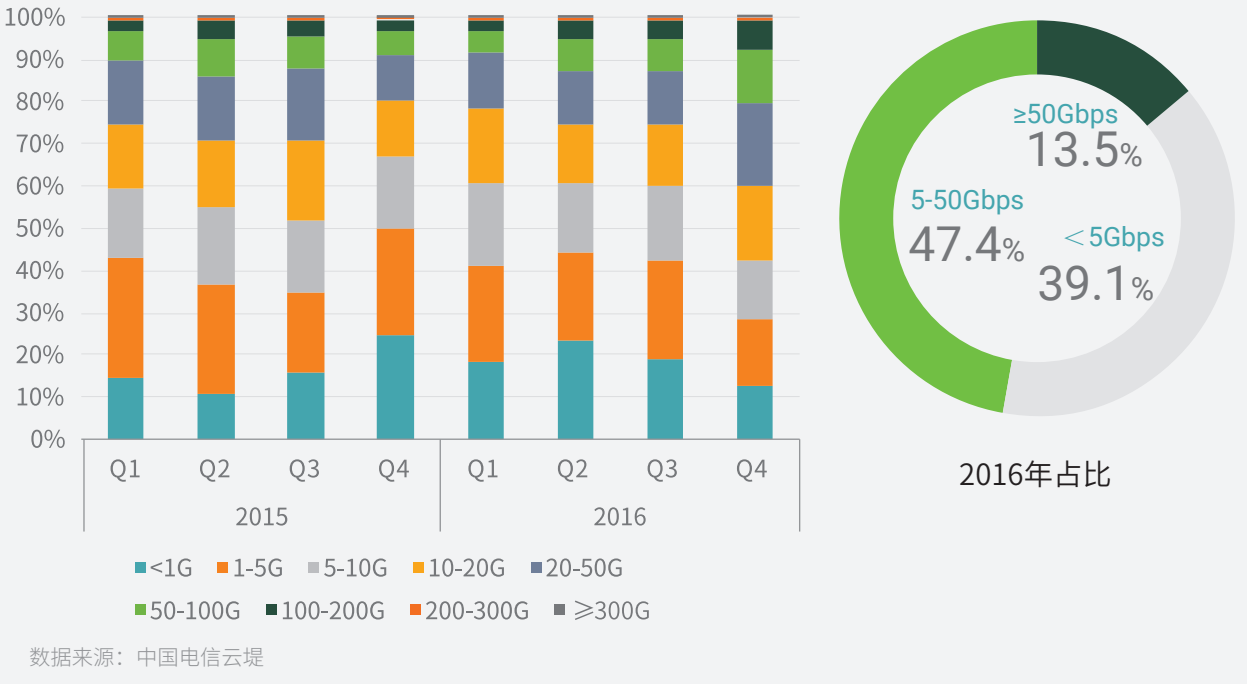
数据来源：中国电信云堤

2.1.2 攻击峰值各区间分布

2016 年攻击峰值各区间分布情况如下图所示，小于 5Gbps 的小流量攻击平均占 39.1%，同比去年下降 2 个百分点；5-50Gbps 流量的攻击平均占 47.4%，同比去年下降 0.2 个百分点；大于 50Gbps 的大流量攻击平均占 13.5%，同比去年上升 2.2 个百分点。

2016 年小流量攻击占比呈下降趋势，大流量攻击更为流行。

图 2.2 2016 vs. 2015 年各季度攻击峰值区间占比图



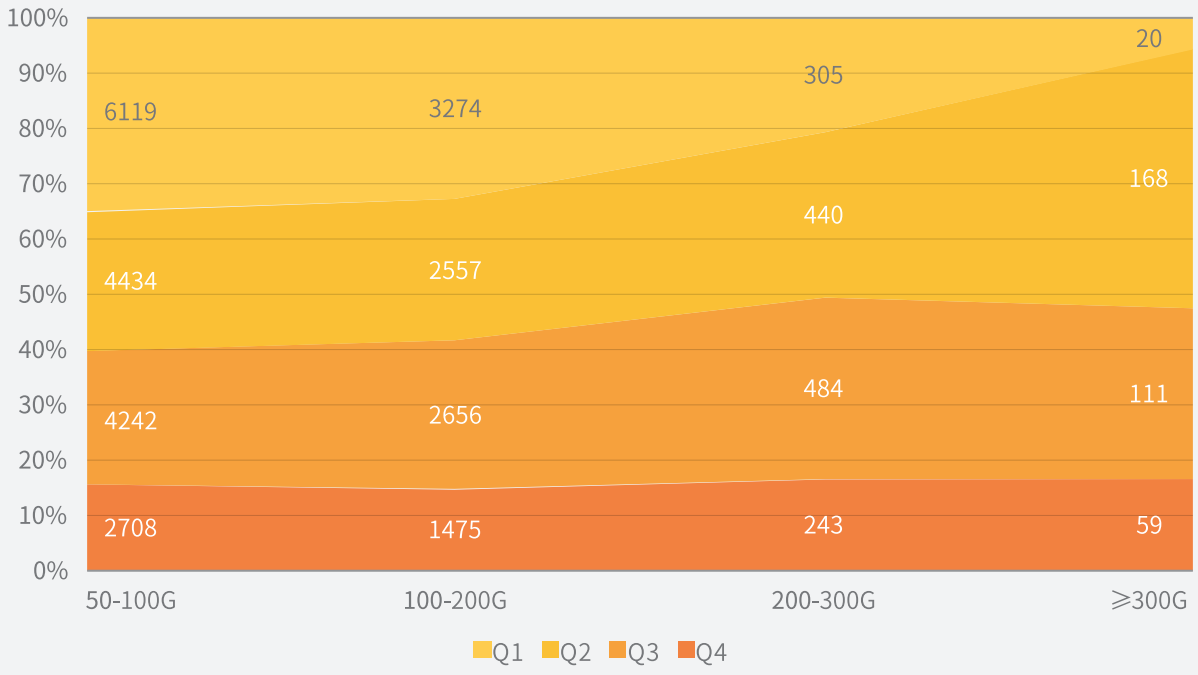
数据来源：中国电信云堤

2.1.3 大流量攻击事件频发

2016 年 Q4 季度，大于 50Gbps 的大流量攻击次数高达 9,718 次，其中峰值在 50-100Gbps 区间的攻击次数达 6,119 次，占 Q4 大流量攻击次数的 63%。全年峰值超过 300Gbps 以上超大流量攻击 358 次，其中 Q3 季度 168 次，占全年总数的 46.9%。

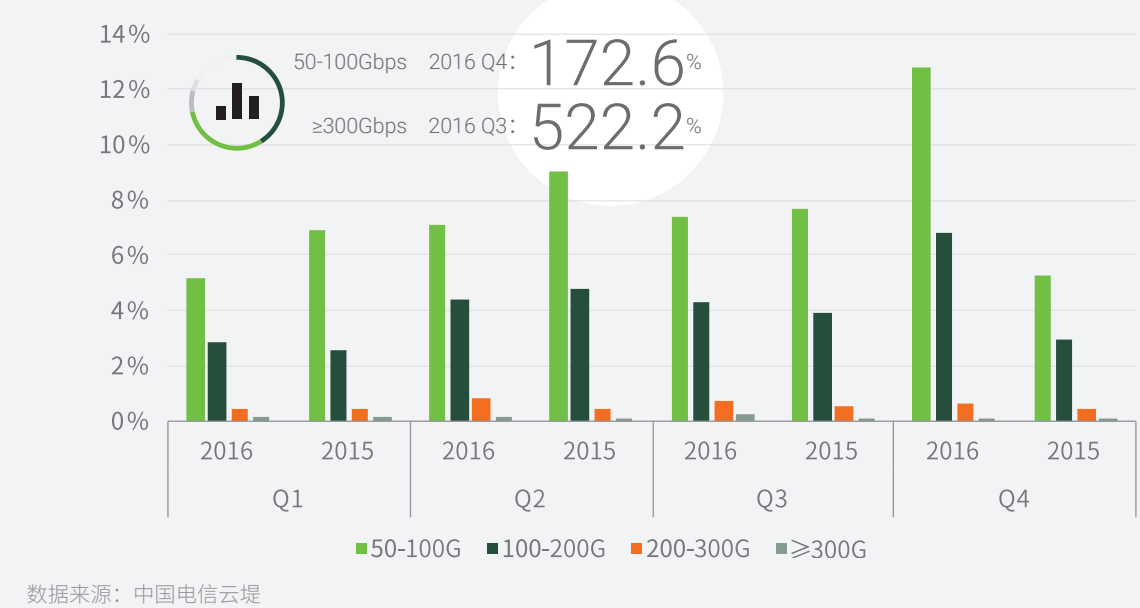
2016 年大流量攻击事件较 2015 年有明显增多，尤其在下半年。攻击峰值在 50-100Gbps 的攻击总数在 2016 Q4 季度同比增长 172.6%，峰值大于 300Gbps 的攻击次数在 Q3 季度同比增长 522.2%。

图 2.3 2016 年各季度大流量攻击次数图



数据来源：中国电信云堤　　单位：次数

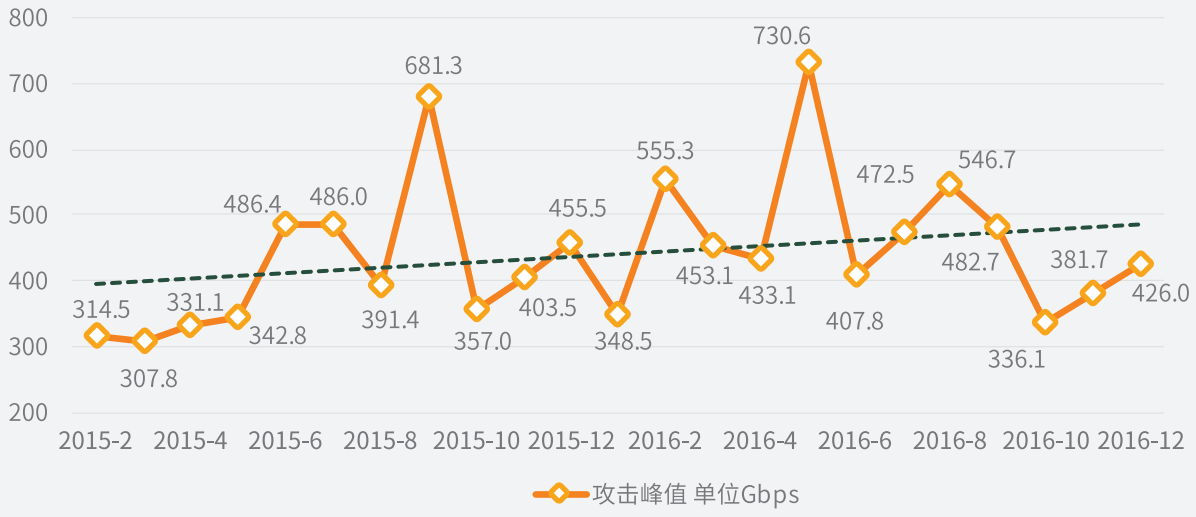
图 2.4 2016 vs. 2015 各季度大流量占比对比图



数据来源：中国电信云堤

从 2015 到 2016 年各月份我国国内发生攻击的最高攻击峰值看，整体趋势缓慢上升（注，除去 2015 年 1 月份的某公司的攻防演练峰值达 1Tbps 的攻击），且各月份最高峰值均已经高出 300Gbps，大流量攻击已成为常态，最高峰值不断刷新纪录。

图 2.5 2015-2016 年各月份攻击最高峰值趋势图



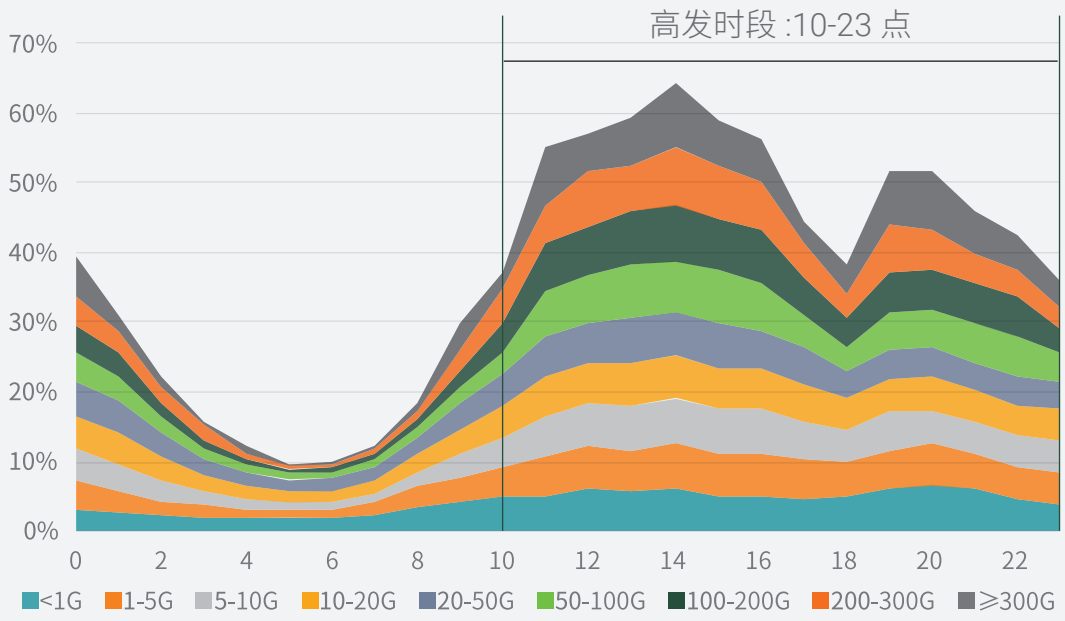
数据来源：中国电信云堤

2.2 DDoS 攻击发生和持续时间

2.2.1 DDoS 攻击发生时间

经我们的统计，2016 年的攻击多发生在 10-23 点这一时段，这通常也是互联网业务在线用户数量最多的时间段。

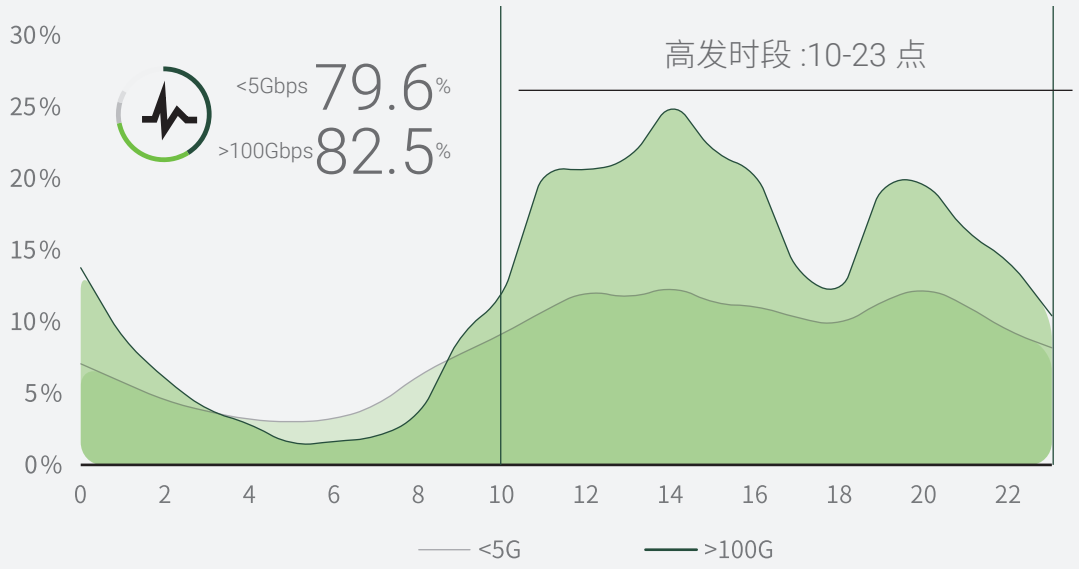
图 2.6 2016 年 DDoS 攻击峰值 / 时间堆积图



数据来源：中国电信云堤

从不同流量区间看，5Gbps 以下小流量攻击，发生在 10-23 点之间的攻击次数占总体攻击次数的 79.6%；大于 100Gbps 的大流量攻击，发生在 10-23 点之间的攻击次数占总体攻击次数的 82.5%，这一时段发生的大流量攻击曲线出现 2 个波峰，11-16 时为第一个波峰，该时段发生的大流量攻击次数占总体的 43.4%，14 点发生的大流量攻击最多，19-20 时为第二个波峰，该时段发生的大流量攻击次数占 13.3%。

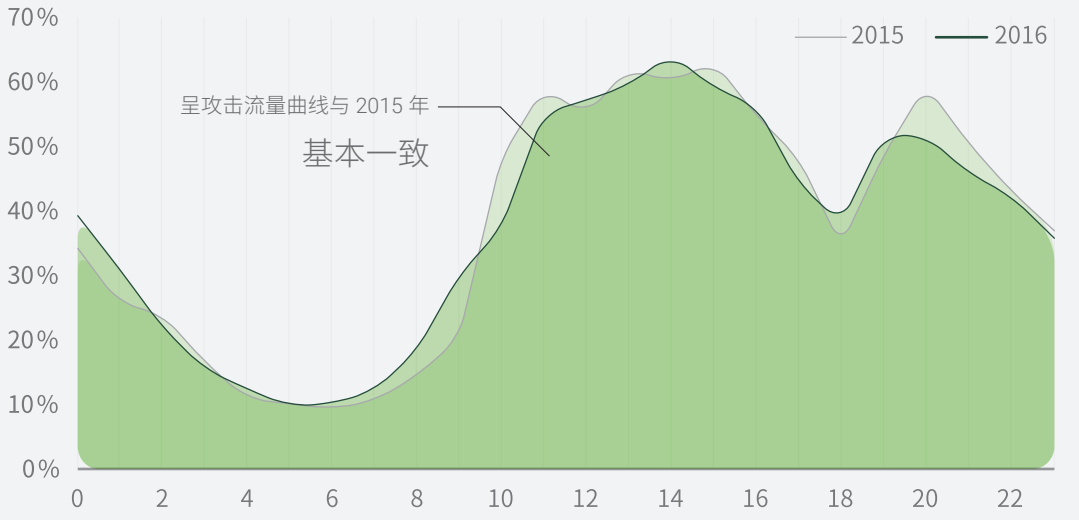
图 2.7 2016 年峰值 <5Gbps 和 >100Gbps 的 DDoS 攻击发生时间占比图



数据来源：中国电信云堤

有意思的是，2016 年攻击流量曲线与 2015 年基本一致。我们从这个统计数据来推测攻击者的意图：选在攻击目标业务使用高峰期发起攻击，往往会给被攻击目标带来巨大损失，反映了他们以期用有限的资源达到对目标的更精准的打击，使破坏力最大化。

图 2.8 2016 vs. 2015 年所有攻击发生时间占比对比图

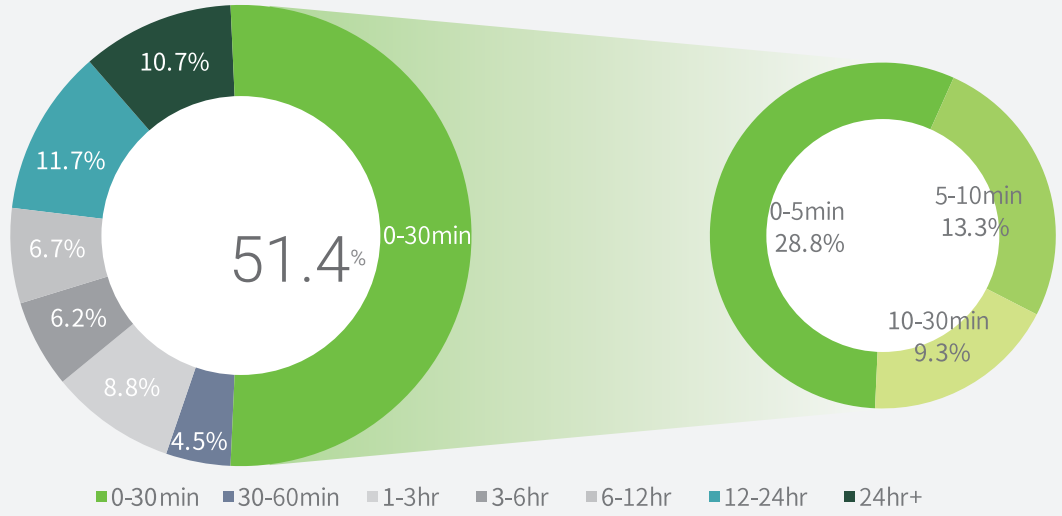


数据来源：中国电信云堤

2.2.2 DDoS 攻击持续时间

2016 年，攻击时长在 30 分钟以下的 DDoS 攻击占全部攻击的一半以上，达到 51.4%。而且大多是小于 5 分钟的短时攻击。

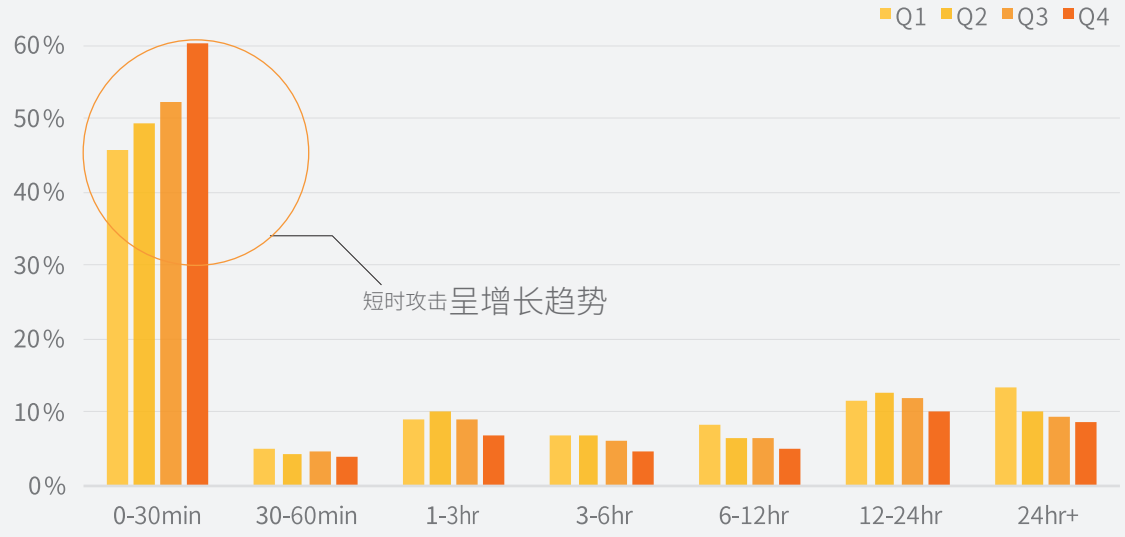
图 2.9 2016 年全年攻击持续时间占比图



数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

从 2016 年各季度 DDoS 攻击持续时间占比图可以看到，短时攻击呈增加的趋势。短时攻击，也叫瞬时攻击，特点是攻击时间极短，这对安全防护者的应急等能力是极大的考验，如果没有很好的应对经验和流程，很可能攻击已经打完了，安全团队还没开始应对。过多的短时攻击可能会牵制安全团队的大部分精力，使其无暇顾及网络中其他安全隐患。通常，大部分 DDoS 攻击背后都隐藏着入侵、数据窃取等其他安全事件。

图 2.10 2016 年各季度 DDoS 攻击持续时间占比图

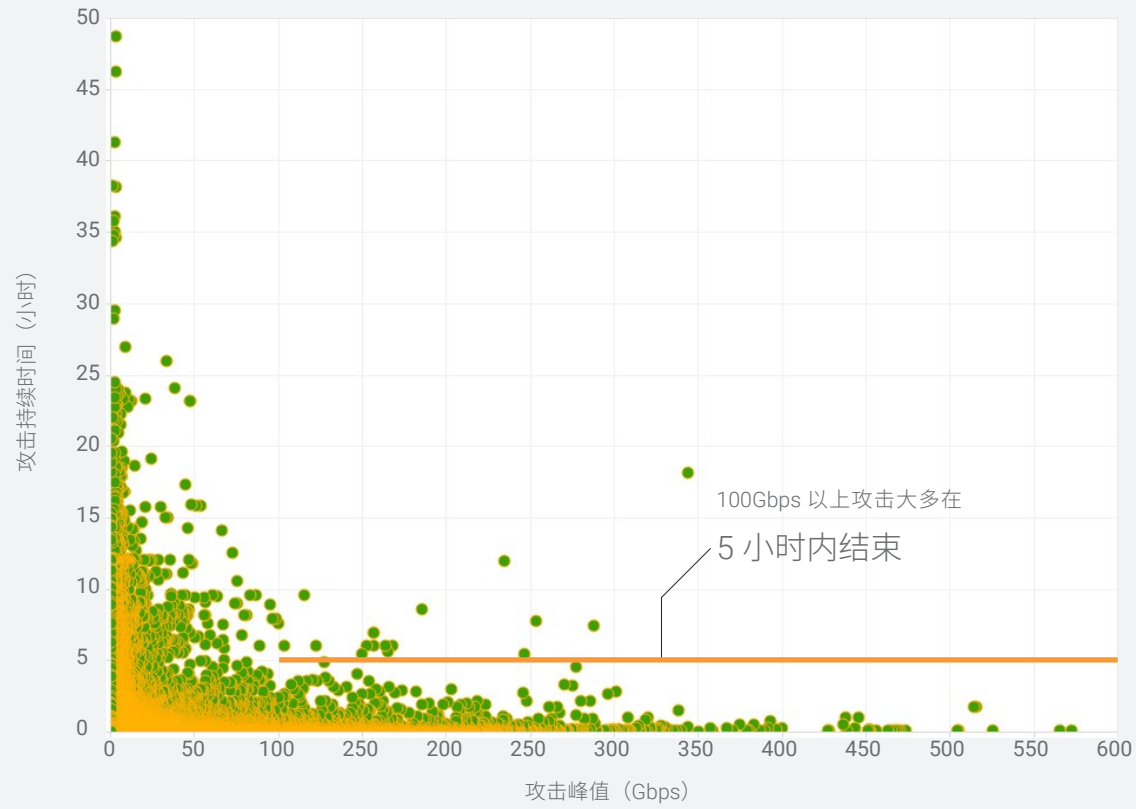


数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

2.2.3 DDoS 攻击峰值 vs. 攻击持续时长

我们对比分析了 2016 年所有攻击的攻击峰值及其攻击持续时长的关系，可以看到有如下规律：攻击流量越小，则攻击可持续的时间越长；反之，攻击流量越大，则攻击可持续的时间越短。100Gbps 以上攻击大多在 5 小时内结束，与去年相比，大流量的攻击持续时间变长。

图 2.11 2016 攻击峰值和攻击持续时间关系图



数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

2.3 DDoS 攻击类型分析

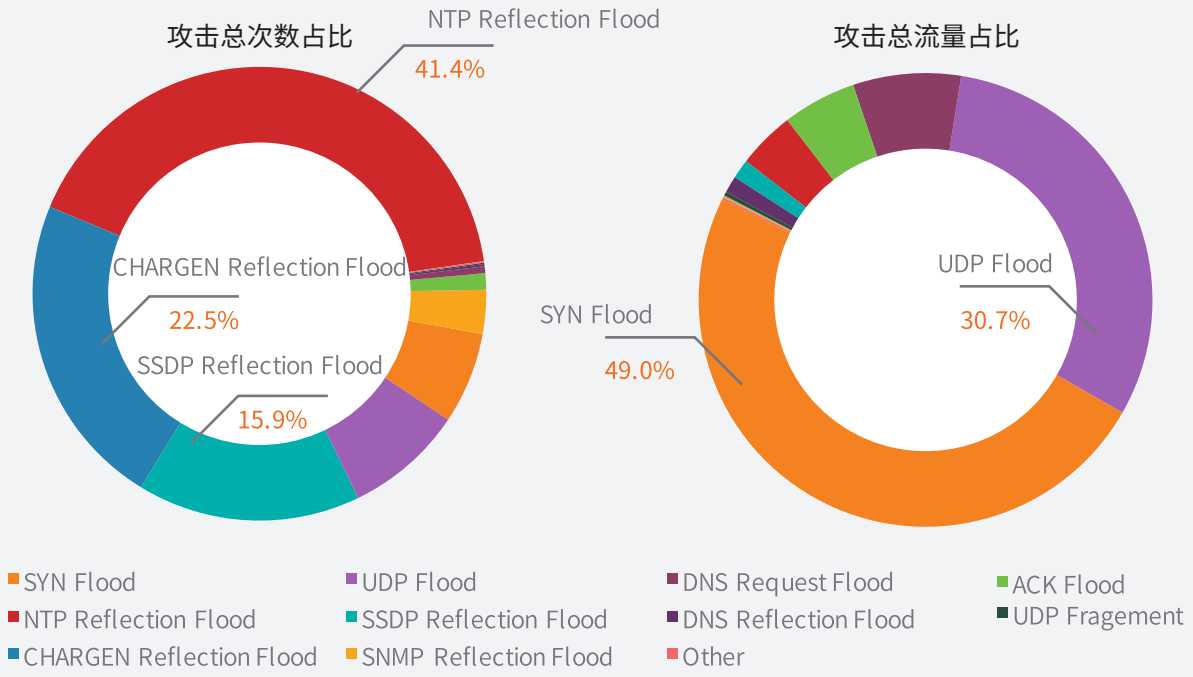
2.3.1 各攻击类型次数和流量占比

2016 年，全球 Top 3 的 DDoS 攻击均为反射攻击（按攻击次数统计），依次为 NTP、CHARGEN、SSDP 反射攻击，这三种攻击类型合计占比达 80%。

反射攻击的原理是攻击者伪造请求，将受害者 IP 地址作为请求源地址并将之发往互联网中存在漏洞的服务器，利用这些协议回应包远大于请求包的特点，达到反射放大流量的效果，构成对攻击目标的大流量 DDoS 攻击。发起反射攻击的成本远小于传统的 DDoS 攻击，近几年反射攻击已成为攻击者常用的攻击手段。运营商一直大力治理反射攻击，但可能仍有部分灰色地带无法监管，加之部分用户安全意识不高，导致可被利用的反射器依然数量庞大。

从统计的趋势来看，我们认为反射型 DDoS 攻击会存在较长时间。

图 2.12 按 DDoS 攻击总次数 / 总流量统计各类型占比图



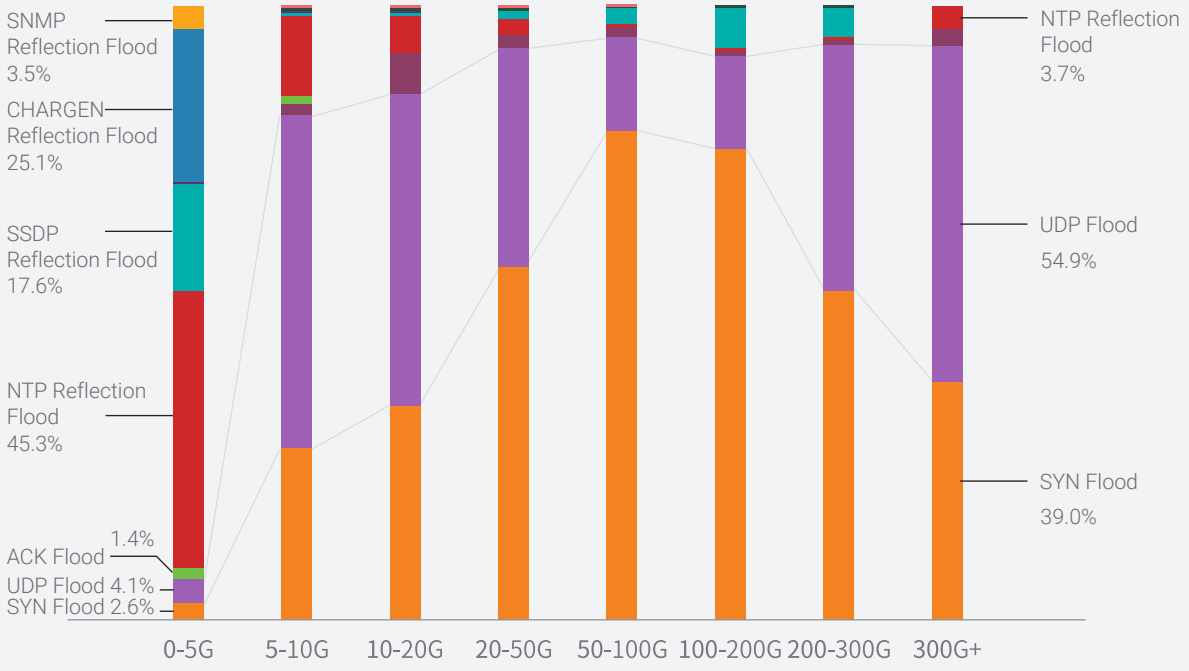
数据来源 : 绿盟科技全球 DDoS 态势感知系统 (ATM)

从各类攻击流量大小占比来看，SYN Flood 流量占比 49%，其次是 UDP Flood，流量占比 30.7%。我们观测到，近两年攻击者偏好使用 payload 经过填充的大包 SYN、UDP 进行 DDoS 攻击。SYN Flood、UDP Flood 依然是流量最大的两种攻击类型。

2.3.2 攻击类型各流量区间分布

2016 年攻击类型在各流量区间的分布呈现如下特点 : 小流量攻击多样化，大流量 UDP、SYN 作主角。这种现象和去年的分析保持一致，在低于 5Gbps 的小流量攻击中包含多种攻击类型，而在大于 5Gbps 的中型、大型、超大型流量攻击中，UDP Flood、SYN Flood 攻击交替占据主流攻击地位。攻击峰值在 50-300Gbps 的大型攻击中，SYN Flood 居多，5-20Gbps 的中型攻击和超过 300Gbps 的超大型攻击中，UDP Flood 居多。

图 2.13 DDoS 攻击类型各流量区间分布图



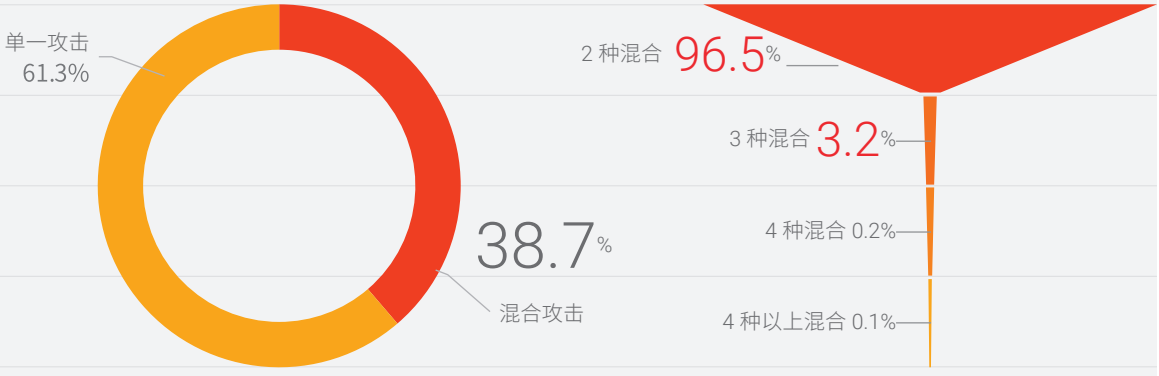
数据来源 : 绿盟科技全球 DDoS 态势感知系统 (ATM)

2.3.3 混合攻击分析

混合攻击相比单一攻击更难检测和防御，所有的攻击因素必须都进行精准检测和防护才能有效防御。有经验的攻击者经常使用混合攻击对目标进行攻击，2016 年混合攻击占全部攻击的 38.7%。

随着 DDoS-for-Hire 服务的不断发展完善，使得发起复杂攻击的门槛大大降低，恶意者只要愿意付一定的价钱，就能得到攻击规模更大、攻击种类更多、攻击持续时间更长的攻击服务。

图 2.14 2016 年混合和非混合 DDoS 攻击及混合种类数占比图

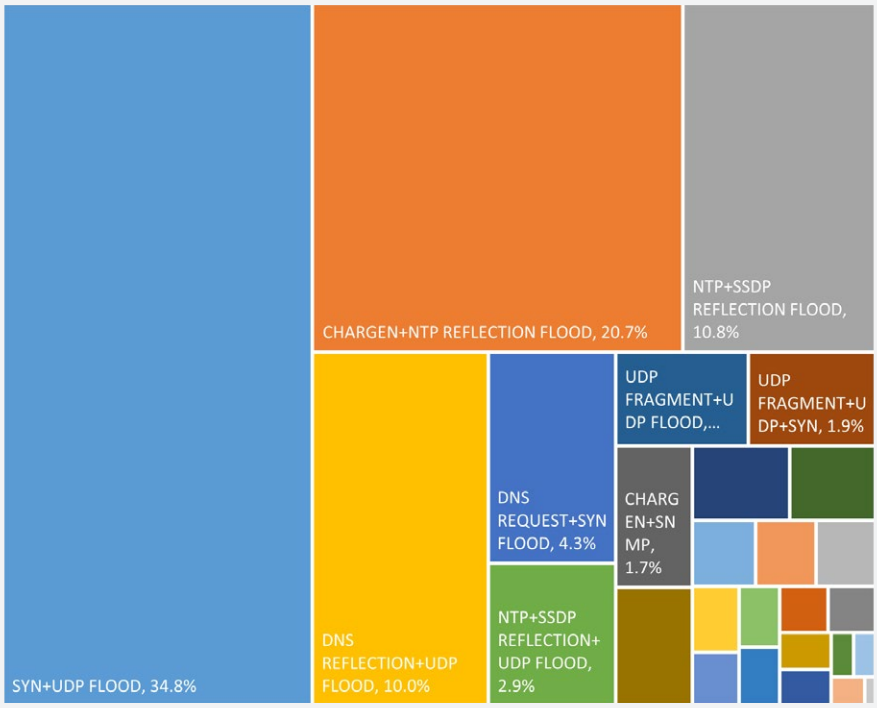


数据来源 : 绿盟科技全球 DDoS 态势感知系统 (ATM)

从攻击种类组成上来看，两种至三种攻击类型的组合最为常见，占据混合攻击的 99.7%。

攻击者最常使用的混合攻击组合见下图，其中 SYN Flood 和 UDP Flood 攻击组合占据全部混合攻击的 34.8%。其次，各类反射攻击的混合也是比较常见的混合方式，例如 CHARGEN 反射和 NTP 反射攻击混合，NTP 和 SSDP 反射攻击混合等。另外，UDP 攻击常混合有 UDP 碎片。

图 2.15 2016 年常见 DDoS 攻击混合类型图



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

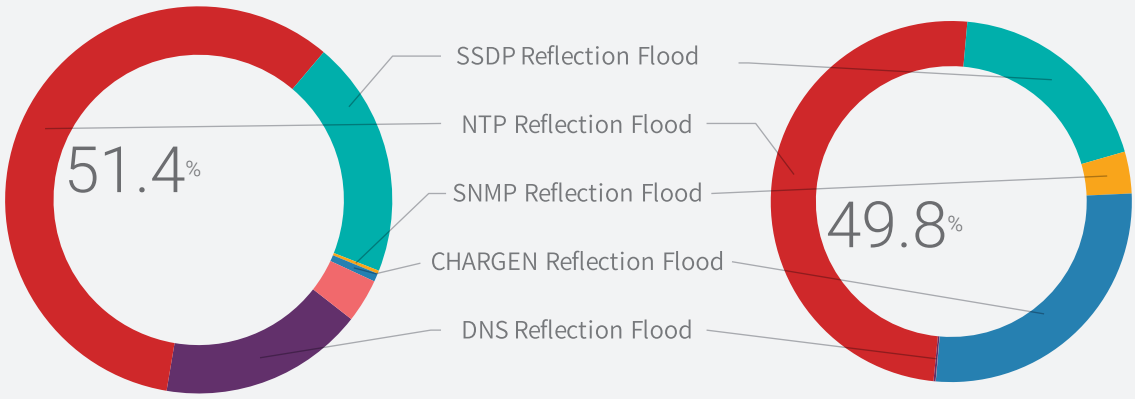
2.3.4 反射攻击类型分析

如 2.3.1 节所说的，2016 年反射类型攻击仍然比较活跃，全年反射类型攻击流量大小和次数占比情况如下图所示。NTP Reflection Flood 和 SSDP Reflection Flood 攻击类型占比均较大。

从攻击流量大小上来看，NTP Reflection Flood 攻击流量占比最多，占全部反射攻击流量的 58.5%，其次是 SSDP Reflection Flood 和 DNS Reflection Flood，分别占 19.8%、17.1%。

从攻击次数上来看，NTP Reflection Flood 仍占据首位，攻击次数占全部反射攻击次数的 49.8%，其次是，CHARGEN Reflection Flood 和 SSDP Reflection Flood，分别占 27.1%、19.1%。

图 2.16 各类反射攻击流量 / 次数占比图

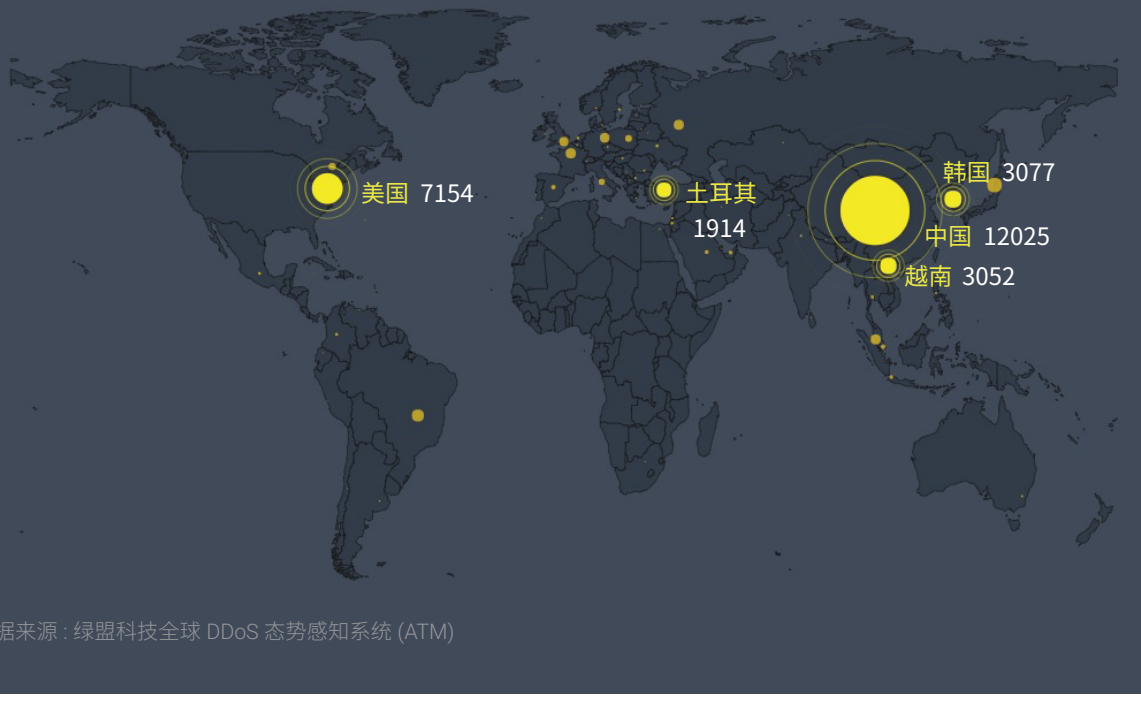


数据来源 : 绿盟科技全球 DDoS 态势感知系统 (ATM)

2016 年，我们检测到全球的活跃 NTP 反射器 (经常参与 DDoS 攻击的 NTP 服务器)52,396 个，全球分布情况如下图。

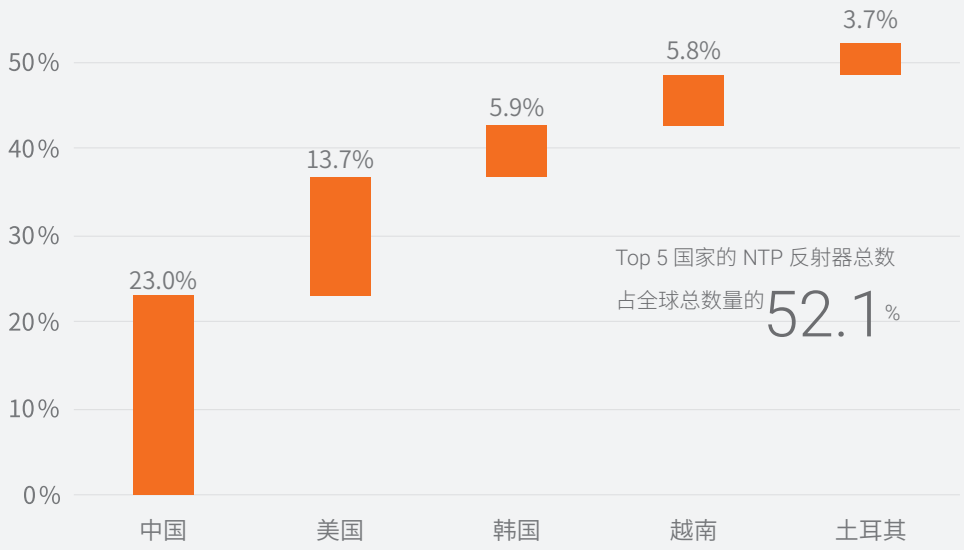
NTP 反射器个数排名前五位的国家分别为中国、美国、韩国、越南、土耳其，Top 5 国家的 NTP 反射器总数占全球总数量的 52.1%，其中中国的反射器个数占全球总数量的 23%。

图 2.17 活跃 NTP 反射器全球分布图



数据来源 : 绿盟科技全球 DDoS 态势感知系统 (ATM)

图 2.18 活跃 NTP 反射器 Top5 国家图

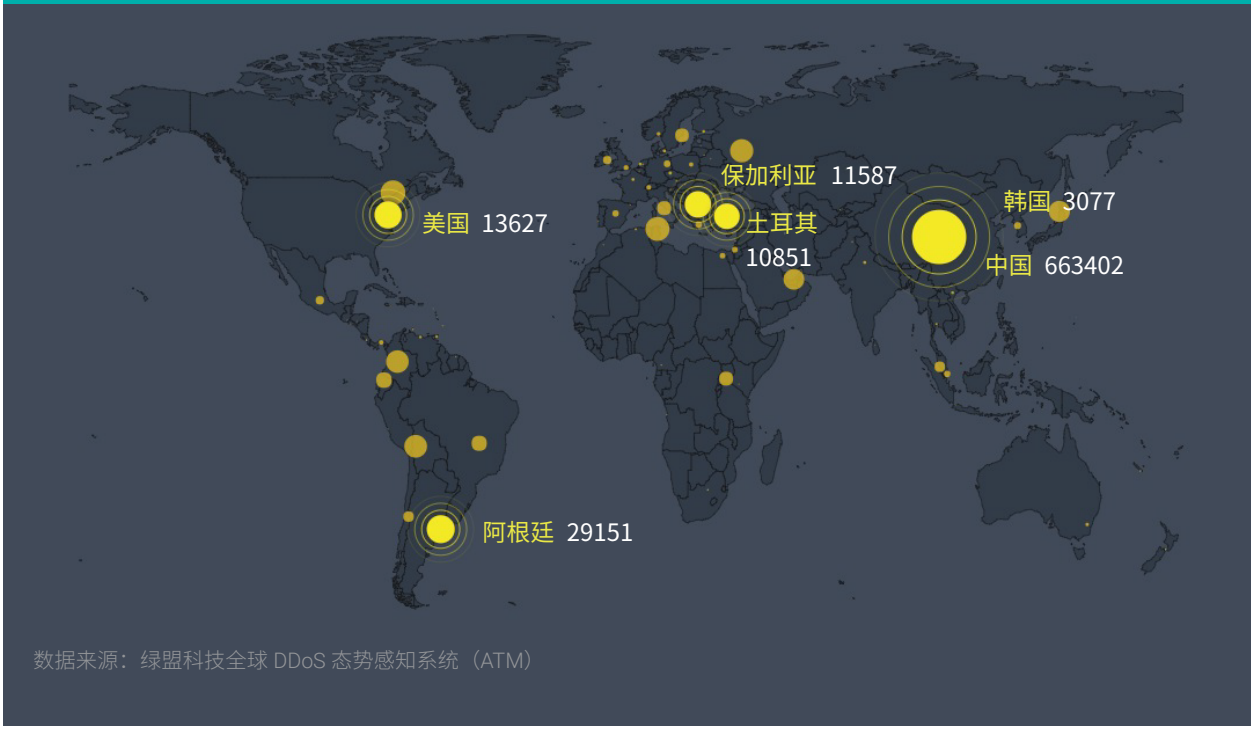


数据来源 : 绿盟科技全球 DDoS 态势感知系统 (ATM)

2016 年，我们检测到全球的活跃 SSDP 反射器 795,616 个，全球分布情况如下图。

其中，2016 年 Q4 季度活跃的 SSDP 反射器数量激增，中国的活跃 SSDP 反射器数量在各季度均占据首位。

图 2.19 活跃 SSDP 反射器全球分布图



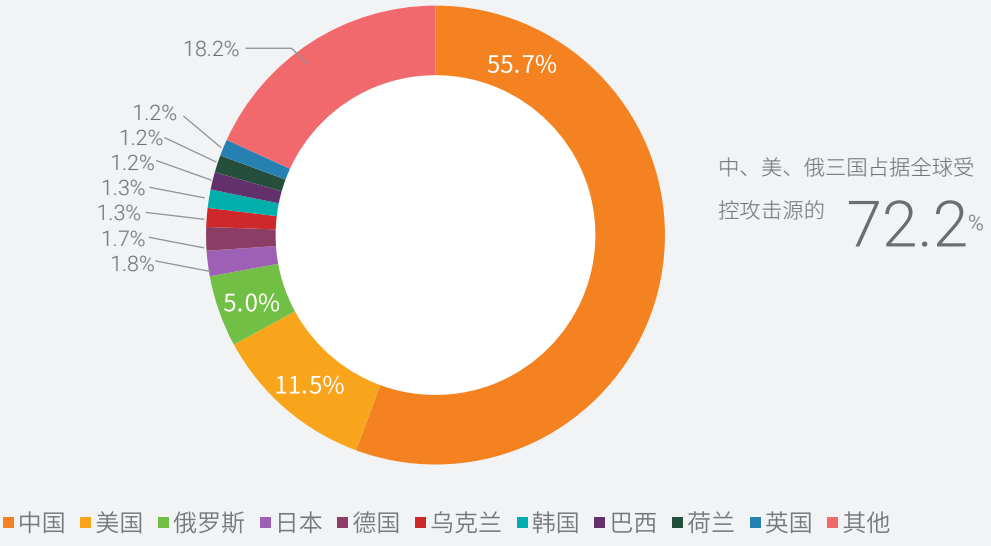
数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

2.4 DDoS 攻击分布情况

2.4.1 DDoS 攻击受控攻击源国家

中国依然是 DDoS 攻击受控攻击源最多的国家，其次是美、俄，三者占据全球受控攻击源的 72.2%。

图 2.20 2016 全球攻击源国家 Top 10 占比图

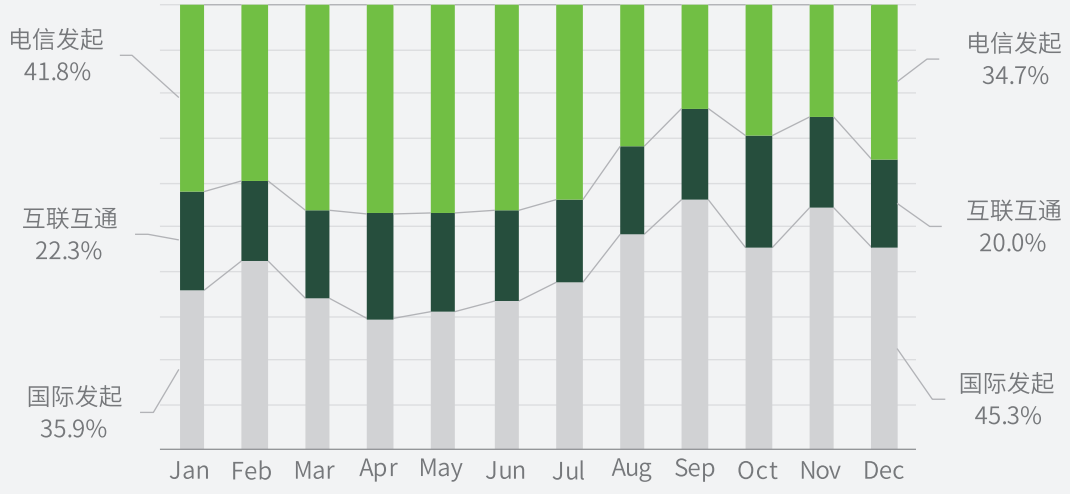


数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

2.4.2 DDoS 攻击来源发起网络

2016 年，由国际侧发起的 DDoS 攻击全年合计占 41.1%，互联互通发起的攻击全年合计占 20.9%，电信内发起的攻击全年合计占 38%。

图 2.21 2016 年攻击来源占比图



数据来源：中国电信云堤

与 2015 年相比，电信内发起攻击的占比有所减小，特别是 2016 年 6 月开始，每月电信内部发起的攻击占比同比减小 8-17 个百分点，这也与电信不断出台各种措施治理 DDoS 攻击密不可分。

国际下半年发起的攻击较多，11 月份来自国际的攻击占比高达 54.4%，同比增长 18.7 个百分点，2.4.1 章节分析了攻击源国家，除中国外，其它攻击源国家的合计占比达 44.3%，说明来自国际的威胁总体在上升。

图 2.22 2016 vs. 2015 电信发起攻击占比对比图

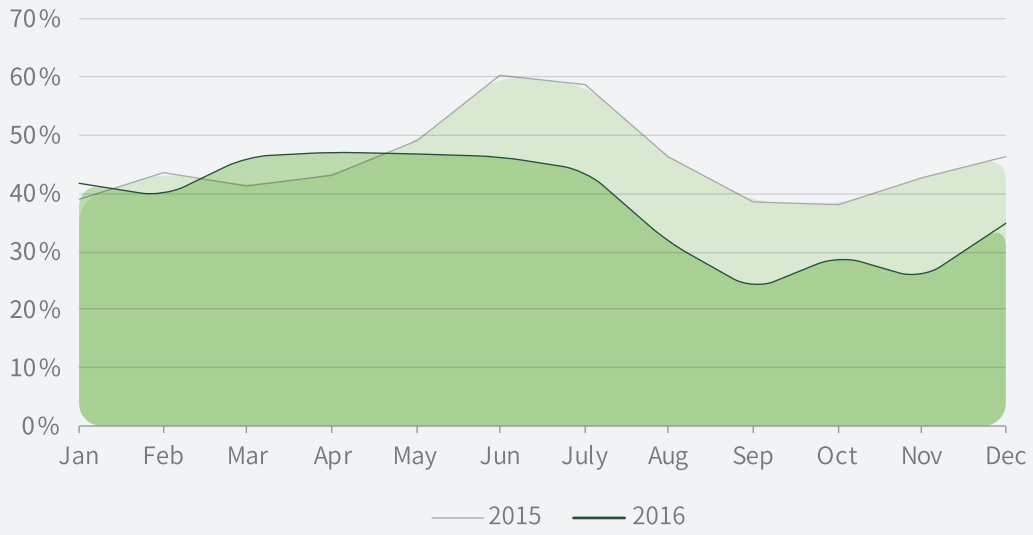
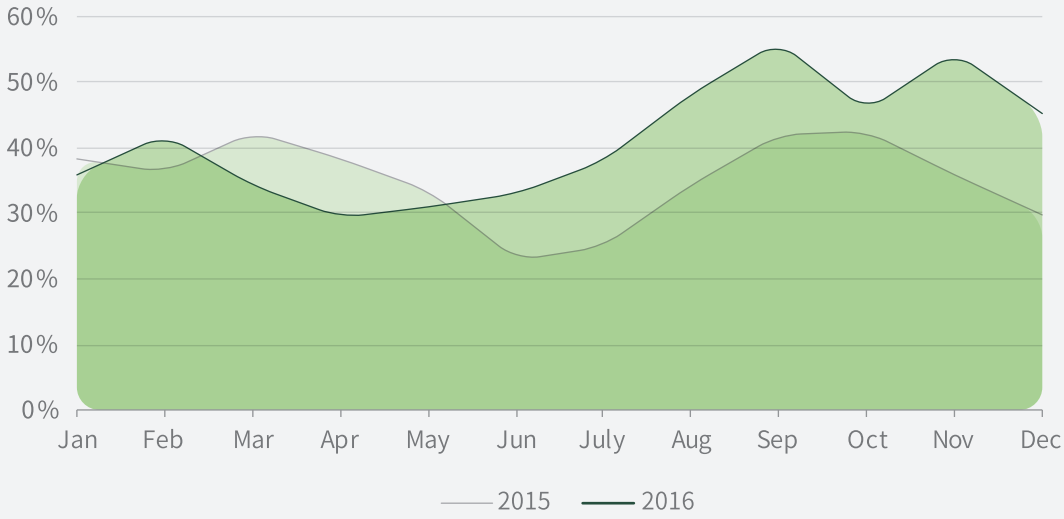


图 2.23 2016 vs. 2015 国际发起攻击占比图

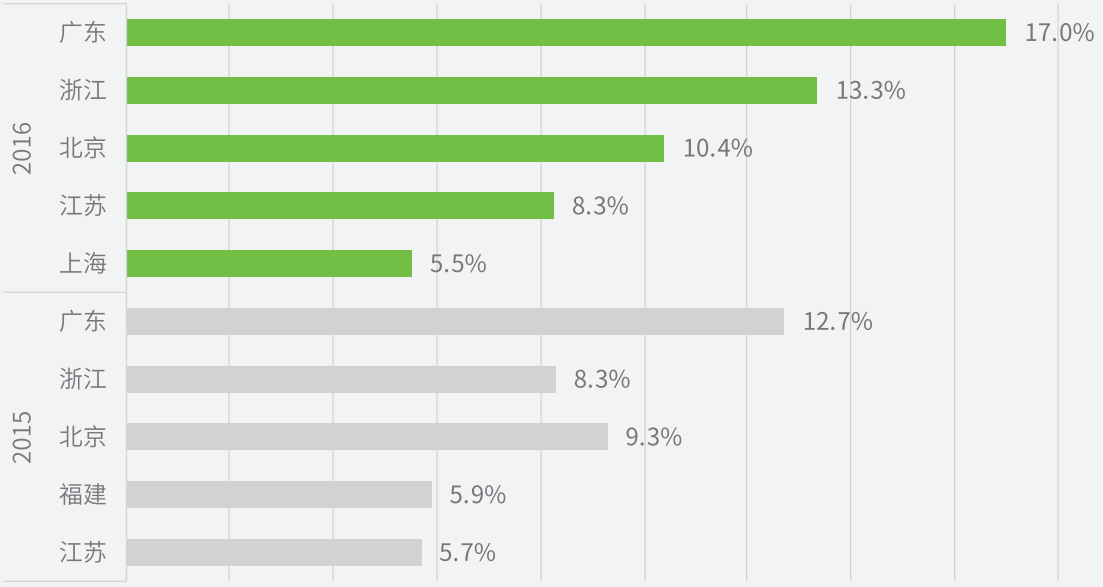


数据来源：中国电信云堤

2.4.3 中国各省份受控攻击源分析

国内发起 DDoS 攻击的源头主要来自广东、浙江、北京、江苏、上海 5 省市，合计占比达 54.5%。广东、浙江、北京仍占据前三位。

图 2.24 2016 vs. 2015 中国各省份攻击源 Top 5 占比图

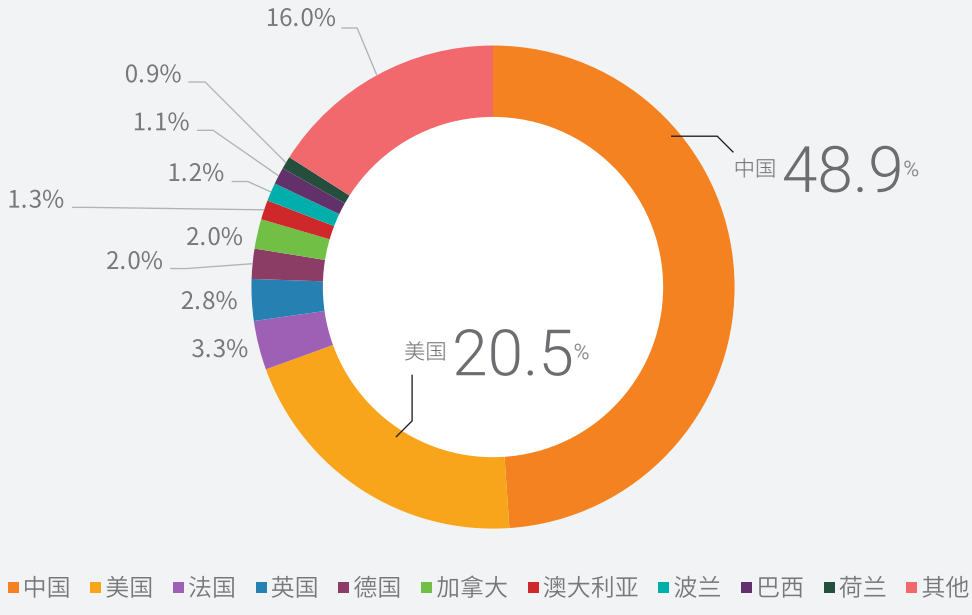


数据来源：中国电信云堤

2.4.4 全球 DDoS 攻击目标国家占比

受攻击最严重的国家是中国，攻击占全部被攻击国家的 48.9%，其次是美国，占 20.5%。

图 2.25 2016 全球被攻击国家 Top 10 占比图

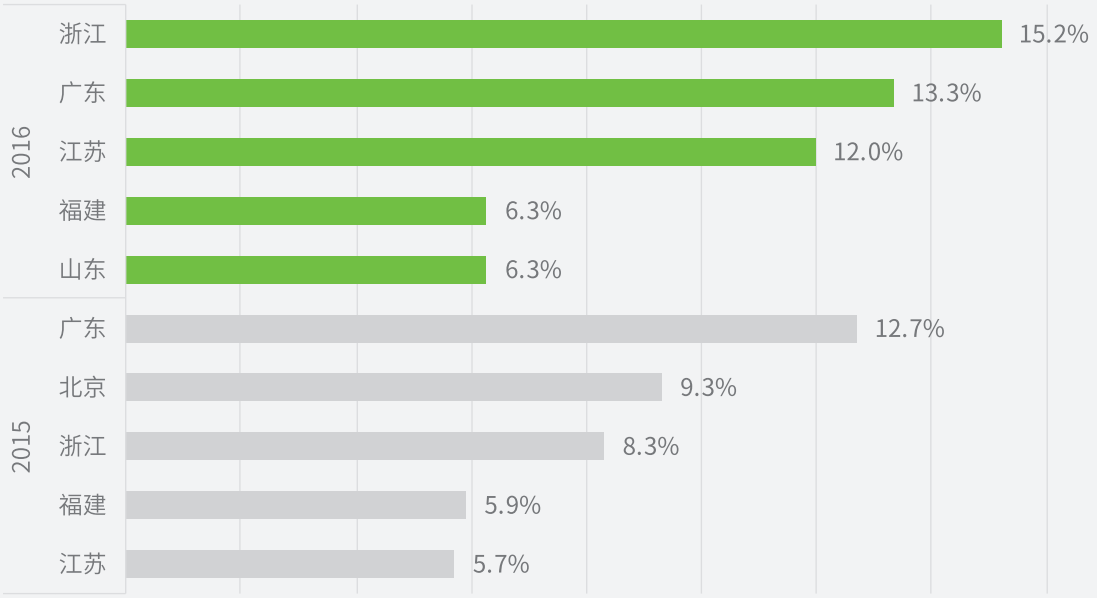


数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

2.4.5 中国 DDoS 攻击目标各省份占比

我国中东部沿海地区一直是 DDoS 攻击的高发地，浙江、广东、江苏、福建等地全年遭受攻击占全国总攻击数量的 53%。浙江省取代广东省成为今年遭受攻击最多的省份，山东省攻击数量明显上升，取代北京列入 DDoS 受灾 Top 5 省份。

图 2.26 2016 vs. 2015 中国受攻击各省份 Top 5 占比图



数据来源：中国电信云堤

3. 2016 僵尸网络发展情况

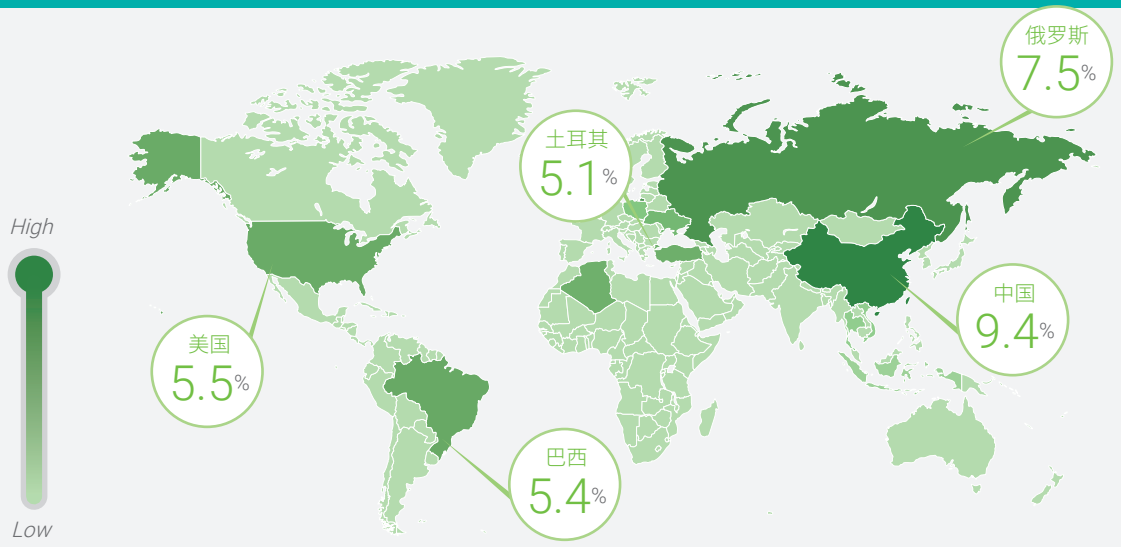
僵尸网络，即“Botnet”，通常由两部分组成，一部分是 Bot 端，作为被控端，俗称“肉鸡”，主要是互联网中大量感染了僵尸网络恶意程序的主机、服务器及其他联网设备等组成，用于执行控制端的各种命令；BotMaster 为控制端，负责一对多地管理 Bot 端，并向其下发各种指令。

僵尸网络（Botnet）已经成为当前网络犯罪的主要攻击载体。其广泛被用于 DDoS 攻击、垃圾邮件、欺骗、扫描等网络犯罪活动，根据我们的分析，目前几乎所有的僵尸网络都具备 DDoS 攻击的能力。除了反射攻击，大部分 DDoS 攻击均是由僵尸网络发起的。因此 Botnet 地理分布情况可以间接反应出不同地理位置上我们面临的威胁程度，其变化趋势也可以预知 DDoS 攻击源分布的变化情况。

3.1 BotMaster 全球分布

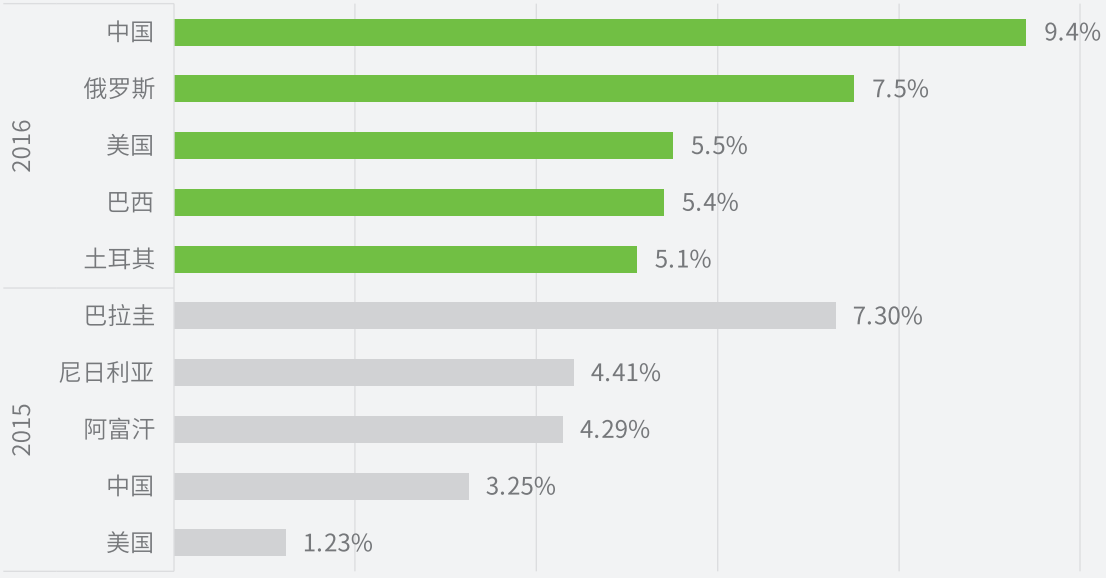
来自 2016 年金山安全的数据显示，BotMaster 全球分布广泛，涉及 120 多个国家和地区，其中中国、俄罗斯、美国、巴西、土耳其数量最多，这 Top 5 国家仅占据全球 BotMaster 数量的 27%。

图 3.1 2016 Botnet C&C 全球分布图



数据来源：金山安全

图 3.2 2016 vs. 2015 Botnet C&C 全球分布 Top 5 国家占比图

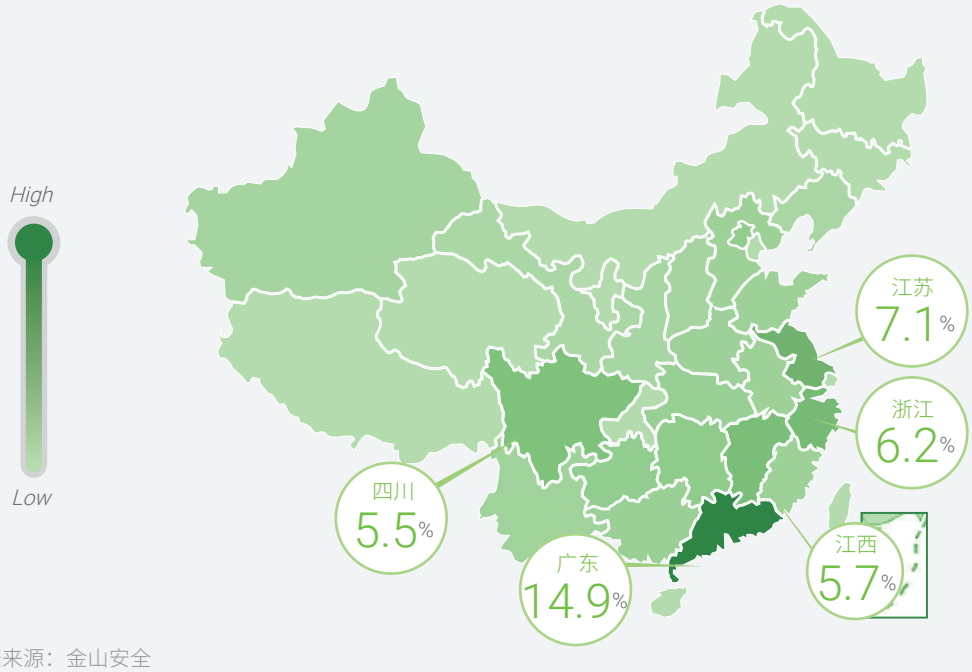


数据来源：金山安全

3.2 Bot 端国内分布

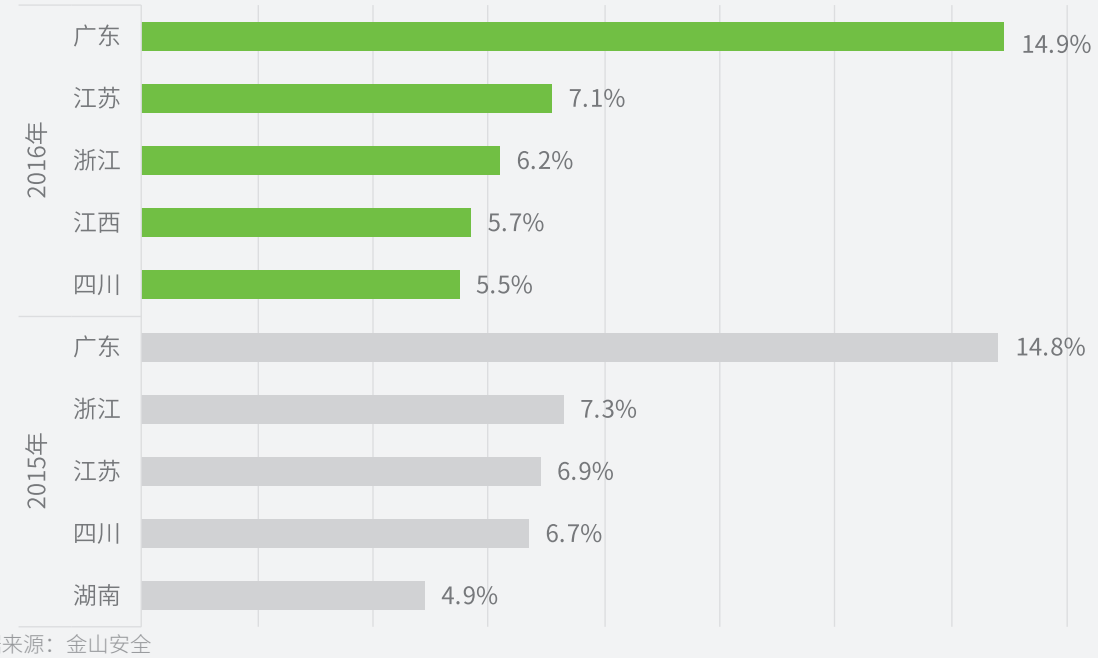
根据我们的统计，僵尸网络 Bot 端主要分布在我国的广东（14.9%）、江苏（7.1%）、浙江（6.2%）、江西（5.7%）、四川（5.5%）等省份。相比 2015 年，江苏省和江西省内 Bot 占比增多，湖南省占比下降。

图 3.3 2016 僵尸网络 Bot 端中国分布图



数据来源：金山安全

图 3.4 2016 vs. 2015 Botnet Bot 端中国省份分布 Top 5 对比图



数据来源：金山安全

3.3 物联网僵尸网络的扩张

物联网（Internet of Things，IoT）的很多应用已经渗透到我们生活的方方面面，其技术的发展，改变着人们的工作和生活方式，使我们更加方便、快捷的同时，也不可避免地带来了诸多安全问题。2016 年 10 月 12 日，绿盟科技发布了《绿盟科技网络视频监控系统安全报告》，报告中分析了网络摄像头这类物联网设备存在的安全隐患，如弱口令、后门、远程可执行漏洞等被黑客利用，使用户设备感染恶意僵尸网络程序 Lizardstresser、Mirai、Luabot 等，执行 DDoS 攻击、扫描、泄露隐私等犯罪活动。

物联网僵尸网络（IoT Botnet）与传统的僵尸网络（Botnet）相比最显著的特征就是其被感染和被控制的 Bot 端不再是传统的 PC 或 Server，而是物联网设备。由于全球这类物联网设备数量庞大，短期内其安全问题难以解决，且易感染、易控制，基于其的僵尸网络规模将不断扩大，拥有的破坏力也会更加惊人。2016 年 10 月发生的“北美大面积网络瘫痪”事件和 11 月发生的“德国大范围用户断网”事件就印证了我们的观点。物联网僵尸网络俨然已经成为黑客 DDoS 工具的新宠，其带来的安全问题给全球的网络安全防护都带来较大挑战。

3.3.1 Mirai 物联网僵尸网络

以 Mirai 为例，目前我们监测到的 Mirai 控制端就已经达到 57 个，如下表所示。从域名注册和更新时间看，基本都是 2016 年下半年开始活跃。

表 3.1 Mirai CC 列表

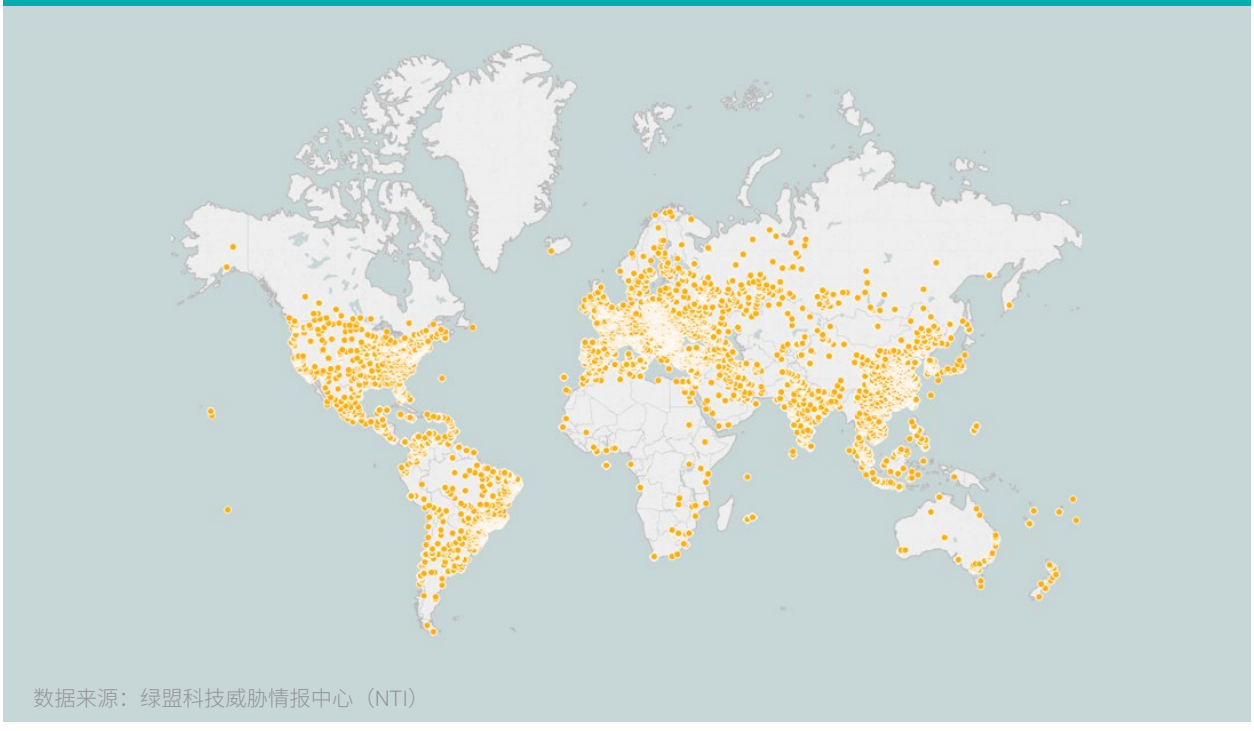
攻击指令服务器 - 地址	攻击指令服务器 - 端口	Report 服务器 - 地址	Report 服务器 - 端口	注册时间	更新时间
g[redacted]ng	23	re[redacted]icing	48101	2016/5/28	
fu[redacted]t.com	23	lu[redacted]m	48101	2016/7/26	
la[redacted].cf	23	re[redacted]ttenjoh.cf	48101	2015/11/16	
im[redacted]	1367	yc[redacted]	48202	2016/10/16	
lo[redacted]g	23	dc[redacted]cing	48101	2016/5/28	
sv[redacted]u	23	ne[redacted]me.ru	48101	2016/8/22	
sv[redacted]u	23	sv[redacted]u	48101	2016/8/22	
tv[redacted]	23	tv[redacted]	48101	2014/11/18	2016/6/13
fu[redacted]k.com	23	fu[redacted]com	53	2011/3/3	2016/4/14
ne[redacted]gcandycane.cx	23	re[redacted]candycane.cx	48101	2016/9/15	
he[redacted]	23	sh[redacted]	48202	2016/10/16	
hi[redacted]ub	666	re[redacted]ime.club	48101	2016/10/24	
ft[redacted]yz	23	lis[redacted]r.xyz	48101		
sc[redacted]	23	sc[redacted]	48101	2016/10/27	
cr[redacted]ng	23	re[redacted]cing	48101	2016/5/28	
ka[redacted]st.xyz	23	re[redacted]xyz	48101		
se[redacted]us	23	re[redacted]es.us	4810	2016/9/4	2016/9/4
lo[redacted]	23	r.l[redacted]	37065		
6[redacted]s.net	2047	e[redacted]s.net	20470	1999/4/22	2016/5/26
tir[redacted]	23	tir[redacted]	4810	2004/11/18	2016/10/27
m[redacted]e	23	re[redacted]e	48101	2015/11/14	
bo[redacted].xyz	23	ct[redacted]net.xyz	48101		
cr[redacted]com	23	lis[redacted]s.com	48101	2016/11/8	2016/11/12
cr[redacted]	23	re[redacted]ow	48202		
au[redacted]om	23	m[redacted]n	48202	2016/11/16	2016/11/16
si[redacted]	23	op[redacted]th.us	4810	2016/9/4	2016/12/11
cr[redacted]com	23	lo[redacted]om	48101	2016/12/12	2016/12/12
al[redacted]	23	tr[redacted]s	48110		
cr[redacted]	23	re[redacted]n	48101	2016/7/8	2016/7/26
cr[redacted]	23	re[redacted]net	48101	2001/6/29	2014/8/15
ur[redacted]	23	ur[redacted]	48101		

攻击指令服务器 - 地址	攻击指令服务器 - 端口	Report 服务器 - 地址	Report 服务器 - 端口	注册时间	更新时间
ov[redacted]s.org	23	ov[redacted]s.org	48101	1998/11/22	
cr[redacted]	23	re[redacted]	44110	2015/3/4	2016/2/3
u[redacted]	23	bo[redacted]	48101	2001/8/10	2013/4/19
cr[redacted]	16741	re[redacted]	36637		
cr[redacted]ce	23	re[redacted]e	48101		
do[redacted]	23	co[redacted]e.ru	48101	2017/1/10	
w[redacted]lesixtodeath.top	23	do[redacted]todeath.top	48101	2016/11/28	
cr[redacted]	23	so[redacted]	48101	2016/7/9	
c2[redacted]	23	ha[redacted]b	47202	2017/1/14	
q5[redacted]x9m4g.ru	23	xg[redacted]'gu55d.q5f2k0evy7go2rax9m4g.ru	48101	2016/10/28	
ne[redacted]	23	re[redacted]g	48101	2016/3/25	
w[redacted].org	23	w[redacted].org	4810	2016/9/20	
ou[redacted]	23	re[redacted]	48101	2016/8/19	
qb[redacted]	23	w[redacted]xyz	48101		
cr[redacted]	443	re[redacted]m	10184	2017/1/24	
ba[redacted]om	23	rp[redacted]n	8000	2016/6/29	
w[redacted]g.ru	28610	w[redacted]ru	56817		
ne[redacted]ir		ne[redacted]ir	48101		2017/2/4
fla[redacted]	23	fla[redacted]	48101	2016/12/22	
cr[redacted]z	23	re[redacted]xyz	48101		
tra[redacted]	23	co[redacted]ru	48101	2017/2/11	
c.[redacted]	23	r.c[redacted]	48101		
nu[redacted]	23	nu[redacted]	48101		
br[redacted]	23	br[redacted]	48101	2017/2/17	
ba[redacted]n	23	rp[redacted]	8000	2017/2/15	2017/2/15
kr[redacted]wang	443	rd[redacted]ng	48101	2017/2/4	

数据来源：绿盟科技 DDoS 攻防研究实验室

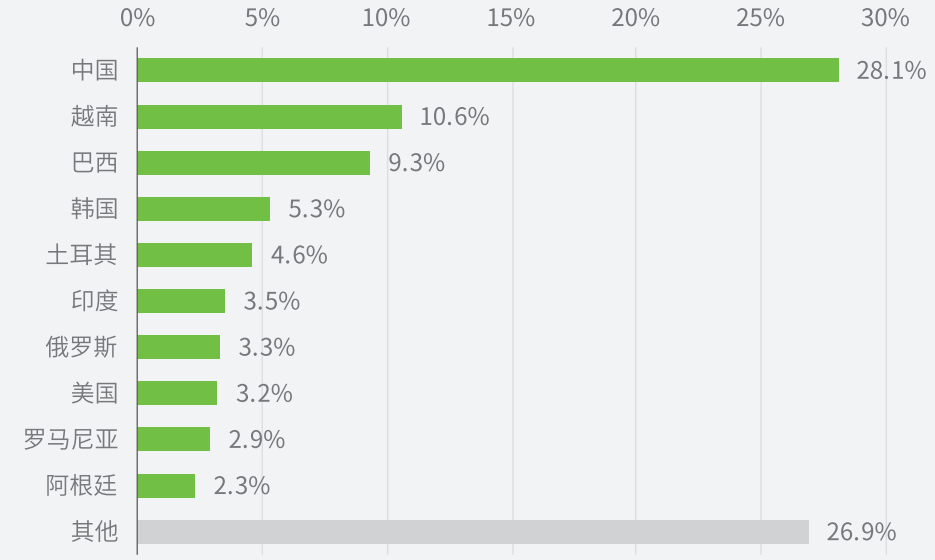
全球感染 Mirai 的物联网设备数量累计已经突破 200 万。Mirai 单个僵尸网络规模庞大，有些僵尸网络 Bot 端的数量多达几十万个。其全球分布情况及 Top 10 国家如下图所示。

图 3.5 Mirai Bot 端全球分布图



数据来源：绿盟科技威胁情报中心（NTI）

图 3.6 Mirai Bot 端全球分布 TOP10 国家占比图



数据来源：绿盟科技威胁情报中心（NTI）

我们截取了 2017 年初 1 个多月的 Mirai 扫描数据（其中包含使用最初 Mirai 版本扫描特征的 Bot 日扫描总次数，和未使用该特征的 Bot 日扫描总次数），如图 3.7 所示。

自从 Mirai 的源代码在 9 月份被公开后，各黑客组织就从未停止过对其功能的改造，Mirai 变种层出不穷。最初版本的 Mirai 使用 23 和 2323 端口进行新感染目标的扫描，且扫描时带有一些固定特征，到目前已经陆续出现新的扫描端口共 8 个，分别为 Port 7547、6789、5555、32、23231、3777、2222、19058。部分变种 Mirai 已经不再具备最初的特征。

图 3.7 Mirai Bot 端日扫描趋势图

数据来源：绿盟科技威胁情报中心（NTI）

另外，2017 年初，Mirai 日扫描次数相比 2016 年 Q3 季度平均 20 万次 / 日有较明显下降，我们推测有两方面原因：

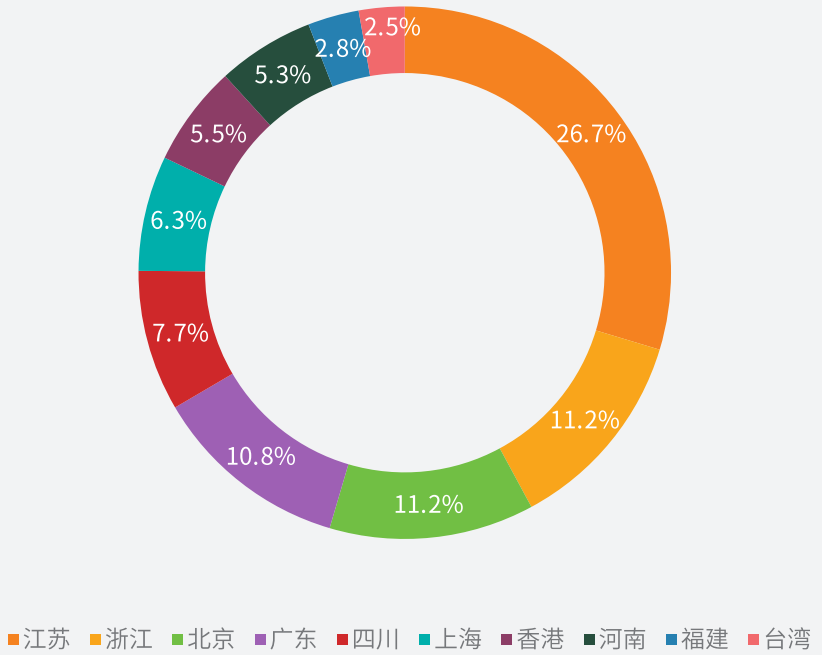
1. Mirai 僵尸网络在 2016 年下半年发起了多次破坏力和影响较大的攻击，已经引起了广泛的关注，相关部门和机构，以及设备厂商已经开始着手应对，也有部分用户开始注意自身的设备安全问题。
2. 除了 Mirai，其他基于物联网的恶意程序也在加紧抢占物联网资源。

3.3.2 台风 DDoS 物联网僵尸网络

基于物联网的僵尸网络恶意程序不仅 Mirai，还有 AES.DoS、Luabot、Hajime、台风 DDoS 等。这类基于物联网设备的僵尸网络恶意程序，只是较少曝光于公众视野。

根据我们的数据显示，台风 DDoS（tfddos）这款主要针对中国地区的基于物联网设备的僵尸网络，其 C&C 主控制端已经将近 1000 个，76% 都分布在中国，也有少部分在美国、土耳其等国家。而中国地区江苏、浙江、北京、广东等地分布最密集。

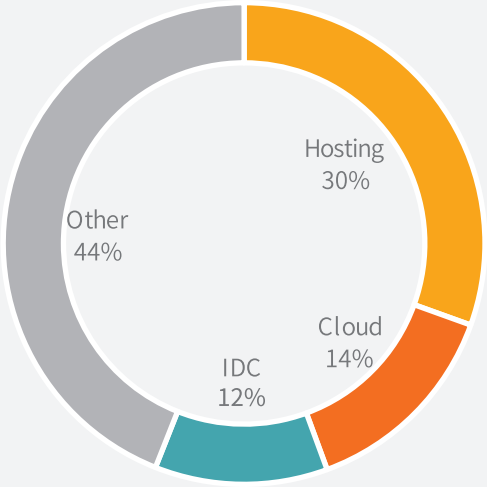
图 3.8 台风 DDoS C&C 主控端中国各省份 TOP10 占比图



数据来源：绿盟科技 DDoS 攻防研究实验室

对台风 DDoS 的 C&C 控制端地址进行溯源显示，14% 的 C&C 控制端都位于云端主机上，包括国内多家知名云；30% 位于提供托管服务或服务器租赁的托管公司的主机上，有意思的是，很多这类托管公司都提供 DDoS 清洗服务。

图 3.9 台风 DDoS C&C 控制端宿主机类型占比



数据来源：绿盟科技 DDoS 攻防研究实验室

3.3.3 物联网僵尸网络资源的争夺

在分析过程中我们发现很多物联网设备，同时被多种恶意软件感染。也发现不同种类的物联网僵尸网络在互相攻击。由于数量庞大、易控制、易感染等特点，物联网设备很自然地成为黑产争夺的对象，不同黑客组织间正在加速抢占物联网僵尸网络资源以为其谋利。

图 3.10 LuaBot 与 Mirai 对抗

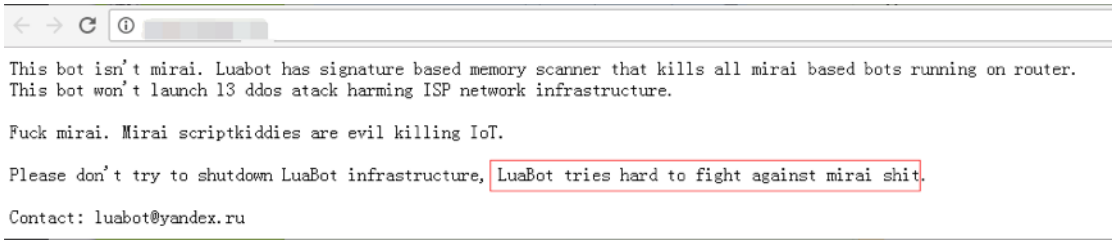


图 3.11 同一物联网设备同时被 Mirai 和 Luabot 感染

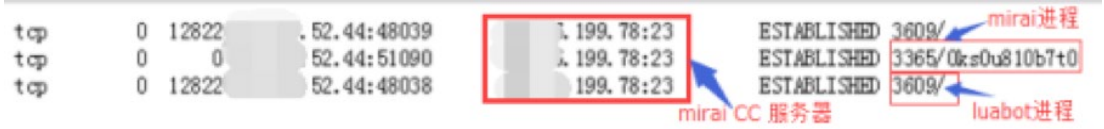
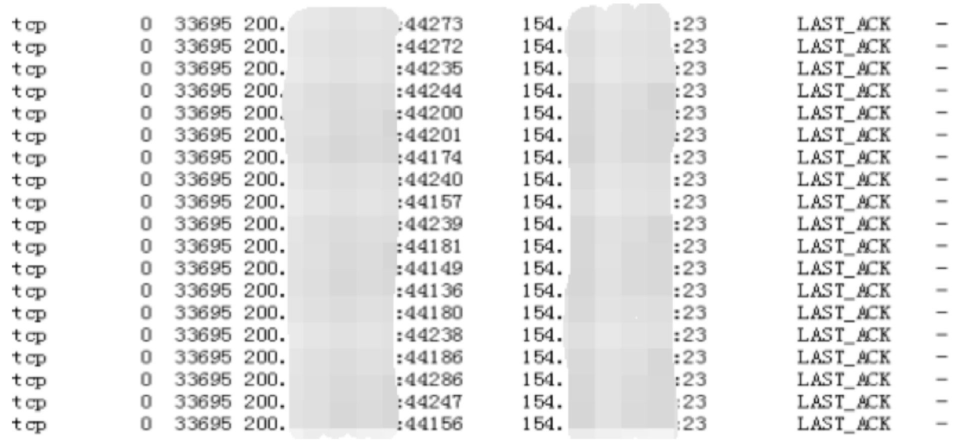
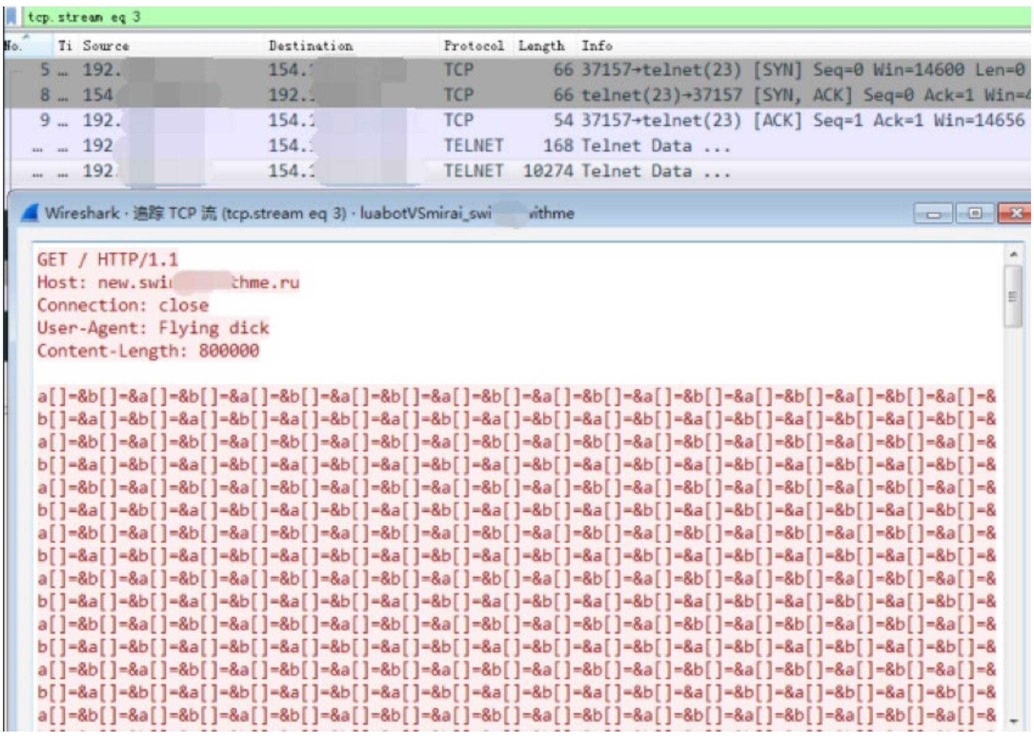


图 3.12 某 Luabot 的 Bot 端在攻击 Mirai 某 C&C 控制服务器





数据来源：绿盟科技 DDoS 攻防研究实验室

3.4 物联网的治理

据 Gartner Inc. 预测，2016 年新的物联网设备将以每天 550 万的速度接入互联网，到 2020 年这个数字将会到达 208 亿。要治理物联网的安全乱象，还需要国家相关主管机构、标准组织、设备生产商、安全厂商等联合协作制定符合物联网行业实情的法律法规、行业安全标准等，以规范物联网的设备生产、管理、运营，构建绿色的网络空间。

我们看到，目前国内外很多相关组织和管理机构开始重视并计划着手应对物联网安全威胁。

2016 年，国内外相关组织开始针对物联网安全发布的规范指南和框架，主旨在规范物联网系统内的相关参与者的义务和准则，包括物联网服务提供商、设备开发商以及研发人员，以确保物联网的健康发展。我们的相关整理如下：

1. 2016 年 2 月，GSM 协会（GSMA, Group Special Mobile Association）发布《物联网（IoT）安全指南》；
2. 2016 年 2 月，云安全联盟（CSA, Cloud Security Alliance）发布 Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products；
3. 2016 年 5 月，开放式 Web 应用程序安全项目（OWASP, Open Web Application Security Project）发布《物联网安全指南》；
4. 2016 年 11 月，宽带互联网技术咨询小组（BITAG, Broadband Internet Technical Advisory Group）发布 Internet of Things (IoT) Broadband Internet Technical Advisory Group；
5. 2016 年 12 月，IoT 安全基金会（IoTs, IoT Security Foundation）发布 IoT Security Compliance Framework 1.0；
6. 2016 年 12 月，绿盟科技发布《物联网安全白皮书》。

各国政府机构推动的物联网安全相关法律规范：

1. 2016 年 10 月，欧盟委员会宣布将制定新物联网设备安全规范，希望通过制定该新法规，强制企业遵守安全标准，确保物联网隐私安全，消除安全威胁；
2. 2016 年 11 月，美国国土安全部（DHS）发布《保障物联网安全的战略原则》，明确表示物联网制造商必须在产品设计阶段构建安全，否则可能会被起诉；
3. 2016 年 3 月，我国国家“十三五”规划指出，要实施网络强国战略，加快构建高速、移动、安全、泛在的新一代信息基础设施。支持智慧城市的建设，提高网络安全等方面风险防控能力；
4. 2016 年 11 月，我国发布了《中华人民共和国网络安全法》，明确指出网络产品和服务提供者，网络安全运营者的安全义务，提出进一步完善个人信息保护规则，加强建立了关键信息基础设施安全保护制度。

4. DDoS 热点攻击事件

2016 年对于网络空间这个没有硝烟的战场来说战事异常猛烈。作为当前网络安全首要威胁之一的 DDoS 攻击，其打击目标不再只是政府、金融、游戏，已经扩张到各行各业，DDoS 勒索事件频发；黑客攻击手段也越来越高明，不惜精心策划攻击策略，以套取更大利益。僵尸网络感染平台继续扩张，物联网设备大面积沦陷，DDoS 攻击规模屡创新高，造成的影响和破坏力越来越大，不断刷新人们对 DDoS 攻击的认知。我们面临的 DDoS 威胁依然严峻。

4.1 万物互联时代，物联网成僵尸网络新宠

2016 年 9 月 20 日，专门从事曝光网络犯罪的网站 KrebsonSecurity.com 遭遇基于物联网设备的僵尸网络 Mirai 的攻击，攻击峰值最高达 620Gbps。该网站之前曝光了付费 DDoS 租赁服务 vDOS，在 Krebs 曝光之后，vDOS 的两位创建者都被逮捕，这次攻击很可能就是为了报复 Krebs 网站的曝光。

紧接着，9 月 21 日，OVH 的 CTO Octave Klaba 在 Twitter 上称他们遭受了一起由 145,607 个网络视频监控设备发起的峰值最高达 1Tbps 的 DDoS 攻击。预计该僵尸网络有能力发动峰值超过 1.5Tbps 的 DDoS 攻击。据推测，针对 Krebs 和 OVH 的攻击很可能来自于同一个 Mirai 僵尸网络。针对 OVH 的这次攻击，创史上最高攻击峰值记录。

10 月 21 日，美国 DNS 服务商 DYN 遭受攻击，大半个国家的网络陷入瘫痪。这起事件缘由是提供动态 DNS 服务的 DynDNS 遭到了大规模 DDoS 攻击，攻击源部分是由感染了恶意程序 Mirai 的物联网设备发起的。导致许多使用 DynDNS 服务的网站一度瘫痪，其中包括 GitHub，Twitter，Airbnb，Reddit 等。此次攻击所带来的影响远远比攻击者所期望的要更加严重，攻击波及到其他使用 DYN 服务的网络站点，这些网站又是北美地区主要的网站，所以造成了北美地区网络全面瘫痪的假象，此次事件堪称史上“最具破坏力的攻击”。

11 月，德国电信路由器被僵尸网络利用，90 多万台路由器出现严重的连接问题，2000 万用户遭遇网络访问受限。德国电信对此次事件进一步确认，是由于路由设备的维护界面被暴露在互联网上，黑客利用这些路由器发起有针对性的网络攻击，导致了此次大范围的故障。

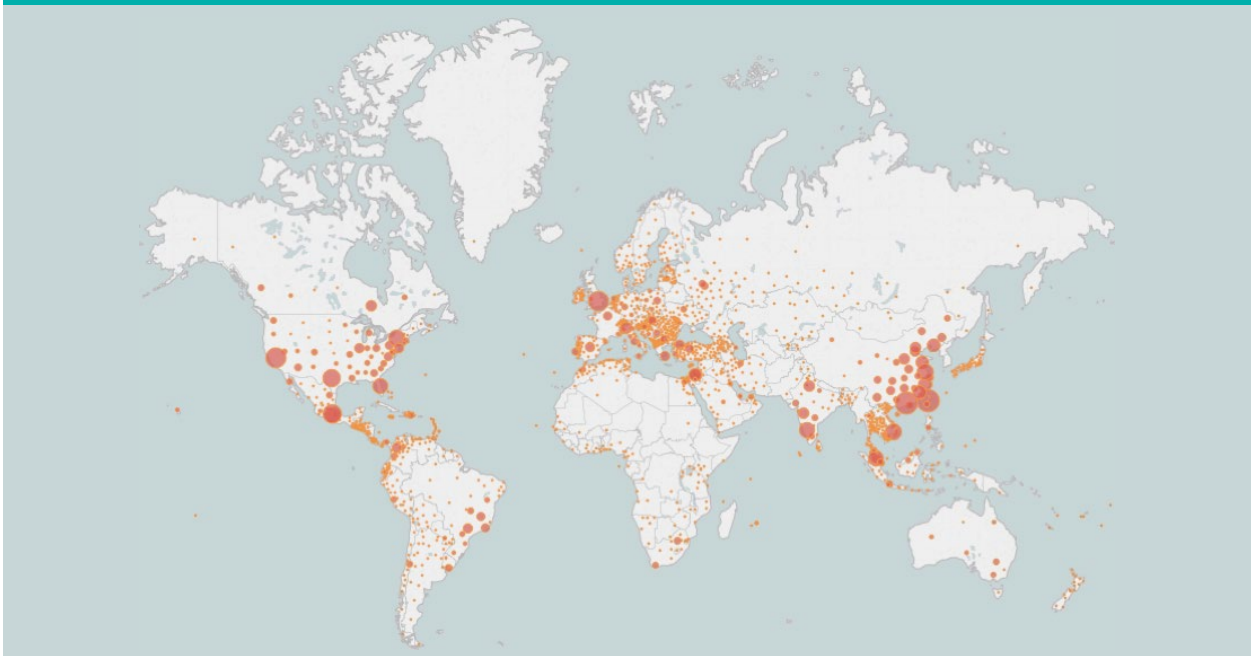
物联网相关 DDoS 攻击事件频发，在 2016 年《绿盟科技 2016 年 Q3 季度 DDoS 态势报告》中曾提到，2016 年 Q3 季度攻击峰值超过 300Gbp 的超大流量攻击事件中，除了几起攻击使用的是反射攻击外，其余的非反射攻击大都有网络摄像头、家庭路由器这些物联网设备的参与，且大部分流量的攻击特征符合基于物联网的僵尸网络特点。

在另外一份 2016 年我们发布的《绿盟科技网络视频监控系统安全报告》中，我们提到，随着安防监控设备在各行各业的普及，以及传统安防行业与互联网的深度融合，网络视频监控系统的这类物联网设备的安全现状如不加以控制和改变，基于其的僵尸网络就会以惊人的速度扩张，对全球的网络安全防护带来很大的挑战。

据我们的统计，2016 年全球范围内存在安全隐患的网络视频监控系统的数量就已经超过 2,500,000 个。这些存安全隐患的网络视频监控系统数量最多的国家是中国，占全部的 21.4%，其次是美国，占 15.9%，剩余国家分别是墨西哥、印度、马拉西亚、泰国、韩国、英国、巴西、越南。

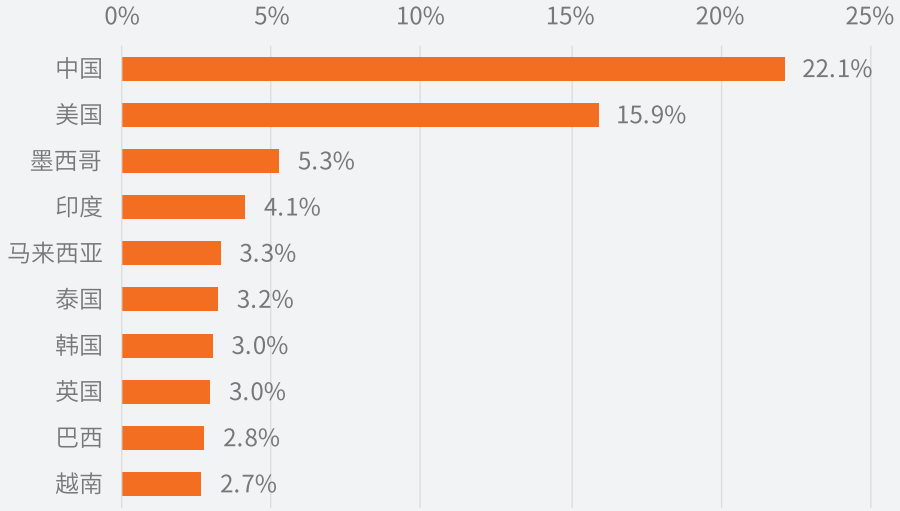
Top10 国家的存安全隐患的网络视频监控系统的数量占全球总数的 65.3%，其余 34.7% 的系统分散于其他 204 个国家和地区内。

图 4.1 存安全隐患的网络视频监控系统全球分布图



数据来源：绿盟科技威胁情报中心（NTI）

图 4.2 全球存安全隐患的网络视频监控系统分布国家 TOP10 占比

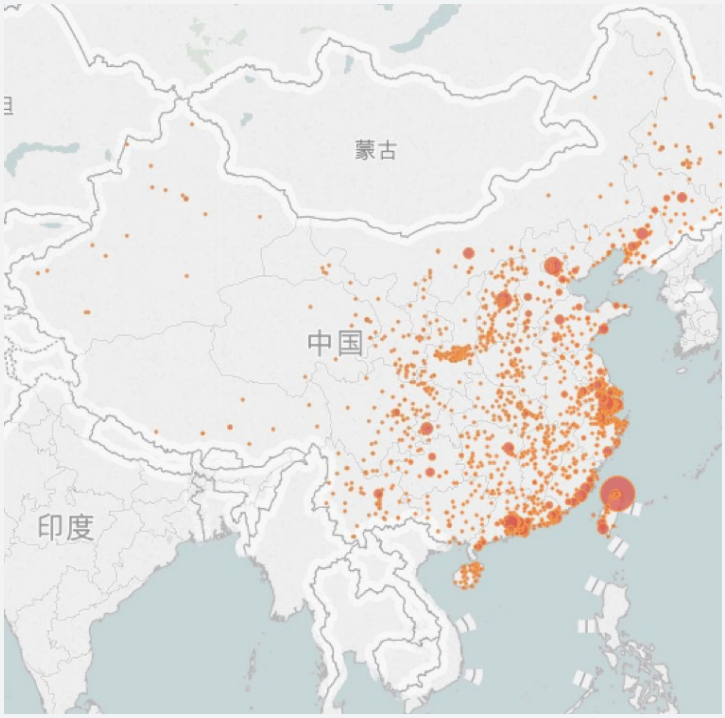


数据来源：绿盟科技威胁情报中心（NTI）

同时，2016 年中国各省份及地区分布的存安全隐患的网络视频监控系统总数量达 50 万以上。其中台湾地区所占数量最多，占 16.1%，其次是广东、福建、浙江等地区。

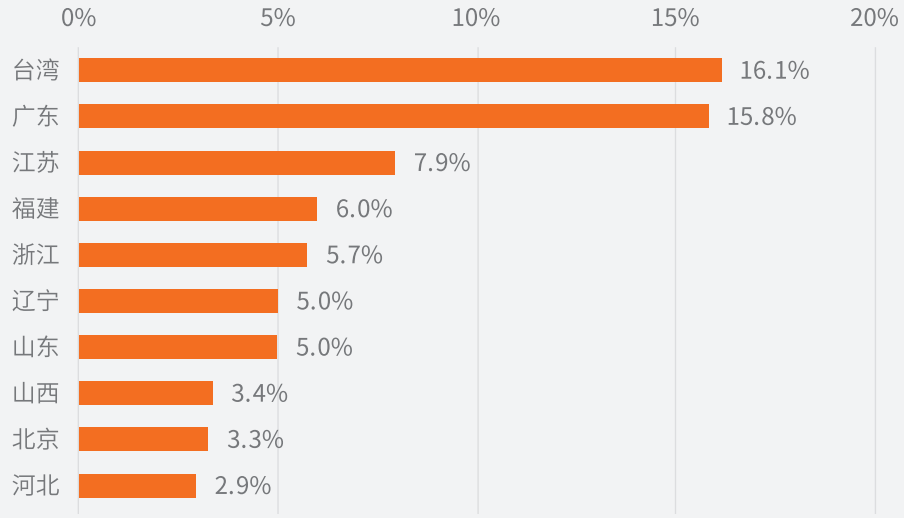
TOP10 省份的存安全隐患的网络视频监控系统的数量占中国总数的 71.2%，其余 28.8% 的数量分散于其他 17 个省份或地区内。可见大部分均分布在东南沿海等商业较发达的地区，这跟网络视频监控系统的市场分布也是相匹配的。

图 4.3 存安全隐患的网络视频监控系统中国各省份及地区分布图



数据来源：绿盟科技威胁情报中心（NTI）

图 4.4 存安全隐患的网络视频监控系统中国 TOP10 省份占比排名



数据来源：绿盟科技威胁情报中心（NTI）

这些分布在世界各地，且数据量巨大的网络视频监控系统，普遍都存在各种安全问题，如弱口令、 系统后门和远程代码可执行漏洞等。由于这类设备的管理特殊性，如使用者安全意识不强、设备久不升级、设备固件升级缓慢等，导致这类设备的漏洞短时间内难以修复，且大量的这些设备并没有安全防护，直接

暴露于互联网中。与此同时，针对这些系统的僵尸网络恶意程序越来越多，其传播手段也不断更新，这些处于完全开放或半开放状态的视频监控系统，沦为黑客的僵尸网络无非只是时间问题，对这些安全隐患设备的治理刻不容缓。

4.2 勒索软件整合 DDoS 攻击能力，进一步挖掘黑产利益

DDoS 勒索比特币（DDoS-For-Bitcoin）类似于勒索软件（Ransomeware）勒索比特币（Ransomware-for-Bitcoin），都是黑客套利的手段，通常要求受害者支付比特币，不然就会遭到 DDoS 攻击。最初是名为 DD4BC 的黑客组织，据记录，其使用这种方式曾经对 140 家公司进行过勒索。DD4BC 通常要求受害者支付 10~200 比特币，如果受害者延迟支付，他们会提高赎金。后来这种方式开始流行起来，同期涌现了很多模仿这种勒索方式的黑客组织，如 Armada Collective 组织，因为 Bitcoin 的方式比其他支付方式更能隐藏勒索者的身份。初期 DDoS 勒索对象通常是一些有能力支付赎金的大公司，后来随着大量勒索组织的出现，各种规模的网站和企业负责人都会收到这样的勒索邮件，受害者数目也呈指数型增长。

2016 年 3 月初，有数百家公司收到了“Armada Collective”组织的勒索信，宣称要么支付 10~50 比特币（约 4600~2.3 万美元）的保护费，要么就等着面对 1Tbps 以上的 DDoS 攻击。大部分公司不予理会，但有些公司认怂了。该团伙的比特币钱包地址显示，入账高达 10 万美元，但那些拒绝支付保护费的公司至今尚未遭到攻击。

并不是所有的 DDoS-for-Bitcoin 都是虚张声势，很多勒索组织已经兑现了自己的威胁，有些甚至支付赎金后仍然被攻击。如 Armada Collective 组织勒索 Proton Mail 供应商花 20 个比特币，终止针对他们的大型 DDoS 攻击。但当 Proton Mail 支付赎金后，攻击仍然持续了较长时间才停止。

2017 年新年伊始，台湾十多家券商就遭到假冒 Armada Collective 名义的勒索组织的 DDoS 攻击，其勒索信宣称要求券商支付 7~10 个比特币（市值约 20-30 万台币），如不付款就会在 2 月 7 日发动 Tb 级更大规模的 DDoS 攻击，在这之前有至少 5 家券商的网站已经遭受了长达 15 分钟的 DDoS 攻击，更多的券商在第二波 DDoS 攻击中受影响，虽然攻击峰值并不如黑客宣称的那样大，但此次攻击导致很多券商的业务下线至少半小时。2016 年我国国内也发生多起针对银行等行业的 DDoS 勒索事件。

Ransomware-as-a-service 导致 Ransomware-for-Bitcoin 横行。同样，DDoS-as-a-service（或 DDoS-for-Hire）也促使了 DDoS-for-BitcoinRxr 的泛滥。2016 年被称为“勒索软件之年”，黑客将在利益的驱使下，寻求整合更多的攻击能力为其谋利。我们也看到，FireCrypt 等勒索软件就同时带有加密文件和 DDoS 功能，虽然其 DDoS 功能并未完善，但不排除后面的变种会升级该功能。就在本报告即将截稿之日，就爆出 Necurs 恶意软件除了发送垃圾邮件传递 Locky 勒索软件外，还整合了 DDoS 攻击能力，由于 Necurs 僵尸网络规模庞大，即使是最基本的技术也足以发起巨大破坏力的攻击。

4.3 攻击者使用 DDoS 攻击作为其他犯罪活动的烟雾弹

我们发现，现在使用 DDoS 作为其他网络犯罪活动掩护的情况越来越多。首先使用 DDoS 攻击吸引安全维护团队的全部精力，同时暗地里进行窃取数据、感染、欺骗等其他形式的犯罪活动，这样安全团队可能就无暇顾及其他安全威胁而使黑客更容易得手。据一份调查报告显示，在遭受 DDoS 攻击的企业中，有 25% 的企业会同时丢失数据。另外一份研究表明，有 30% 的美国金融从业者反馈他们遭受 DDoS 攻击后发现系统被感染恶意软件或者病毒。

巴西里约奥运会期间（2016 年 8 月 5 日 -21 日）Anonymous 组织发起 OlympicHacking 活动，号召其它黑客对巴西政府、奥委会及相关网站进行网络攻击，以抗议巴西政府不投入资金解决国内民生、教育、健康问题，却投入大量物力财力举办里约奥运会。据记录，这期间相关网站遭受的 DDoS 攻击最高峰值达 540Gbps，日均峰值均高于 500Gbps。Anonymous 专门制作了 DDoS 攻击工具 opolympddos，包含专门的 Windows 操作界面，并使用 LizardStresser 构建僵尸网络，该恶意程序专门感染物联网设备，比 Mirai 早些出现在公众视野中，可以进行 DNS、NTP、CHARGEN、SSDP 和 GRE Flood 等 DDoS 攻击。此次攻击，不但利用 DDoS 攻击使相关网站的访问受限，也借此为其窃取数据做掩护，因为黑客在第二阶段的攻击中，曝光了相关网站大量注册用户的信息。

我们预计，未来这种攻击模式会被更多有经验的黑客采用。我们有必要提醒，企业一旦发现正在遭受 DDoS 攻击，务必要了解全面的威胁情况，并随时准备好处理多种类型的网络攻击，否则很有可能遭受更大的损失。

图 4.5 Anonymous 在网上发起 OlympicHackin 活动

4.4 政府、金融、游戏行业依然是 DDoS 攻击重灾区

黑客为了谋利通常会将高利润产业如金融、游戏等行业作为 DDoS 攻击和勒索的重点目标。还有些黑客组织为了提高自身的知名度，在政治热点事件、国际上的重大活动等期间打着某种正义的旗号对一些国家政府、机构等高调宣扬其攻击行为。因此，政府、金融、游戏一直都是 DDoS 攻击的重灾区。如下列中

的事件（1）-（5）。

随着黑产利益链的不断成熟，DDoS-for-Hire 的产业化，任何恶意者都可以通过购买 DDoS 攻击服务发起恶意攻击，除了勒索获利，恶意竞争，还有些只是出于愤怒或者是无聊。DDoS 威胁的不再是个别重点行业，各行各业都面临该威胁。

（1）黑客组织轮番攻击特朗普和克林顿的竞选网站干扰美国大选

黑客组织 Anonymous 在 4 月 1 日扬言要令特朗普的竞选网站大规模宕机，破坏总统候选人特朗普的竞选活动，特朗普拥有的酒店网站 trumptowerny.com 遭受了 12 小时的 DDoS 攻击，Anonymous 宣称对此负责。11 月初，不同黑客组织先后利用 Mirai 僵尸网络对特朗普和希拉里克林顿的竞选网站发起了持续 30s 的 HTTP layer7 攻击。

（2）11 月份非洲国家利比里亚频遭 IoT 僵尸网络攻击几乎导致全国断网

在 Mirai 僵尸网络 DDoS 攻击导致大半个美国网络中断后不久，利比里亚一些网络供应商接二连三地遭受 DDoS 攻击，攻击流量最高峰值超过 500Gbps，几乎导致利比里亚全国断网，有证据显示，攻击源头仍然是 Mirai 僵尸网络。有安全研究人员猜测，攻击一个鲜为人知的小国，可能对 Mirai 僵尸网络而言是测试网络武器的“最佳地点”，以备后期开展更大规模的攻击活动。

（3）全球范围内多家银行被 DDoS 攻击，导致多个国家央行网络系统瘫痪甚至被迫关闭

2016 年 5 月，Anonymous 麾下的 BannedOffline、GhostSquadHackers 幽灵黑客小队等组织，针对全球范围内的多家银行网站，发动了 DDoS 攻击，导致约旦、韩国以及摩纳哥等央行网络系统陷入了半小时的瘫痪状态，而黑山国家银行网络系统则被迫关闭，停止服务，攻击给这些国家带来了巨大的经济损失。

（4）俄罗斯 5 家大型银行遭遇大范围僵尸网络 DDoS 攻击

2016 年 11 月，俄罗斯 5 家主流大型银行遭遇了持续两天的 DDoS 攻击。每波攻击持续至少 1 个小时，最长不间断持续超过 12 个小时，攻击类型包括 SYN Flood，HTTP/HTTPS Flood 攻击，以每秒约 66 万次请求攻击银行的 web 网站，随后利用 web 漏洞对其远程管理系统发起应用层攻击。有证据显示攻击来自多个 Mirai 僵尸网络，这些物联网设备遍布 30 多个国家，大部分位于美国、印度、台湾和以色列。这一系列事件给全球银行安全系统敲响警钟。

（5）暴雪公司遭受多次 DDoS 攻击，黑客扬言推特转发超 2000 次就停手

2016 年 4 月，Lizard Squad 黑客组织对暴雪战网和旗下游戏发起持续的 DDoS 攻击，包括《魔兽世界》、《星际争霸》、《暗黑破坏神》等多个重要游戏离线宕机，玩家无法登陆。“Poodle Corp”黑客组织也针对暴雪发起过多次 DDoS 攻击，8 月份有 3 起，9 月份有 1 起，攻击均导致服务器离线，多款游戏受到影响。黑客扬言只要游戏用户转发推文超过 2000 次就停止攻击。

（6） 国内某互联网金融平台遭受大流量 DDoS 攻击勒索

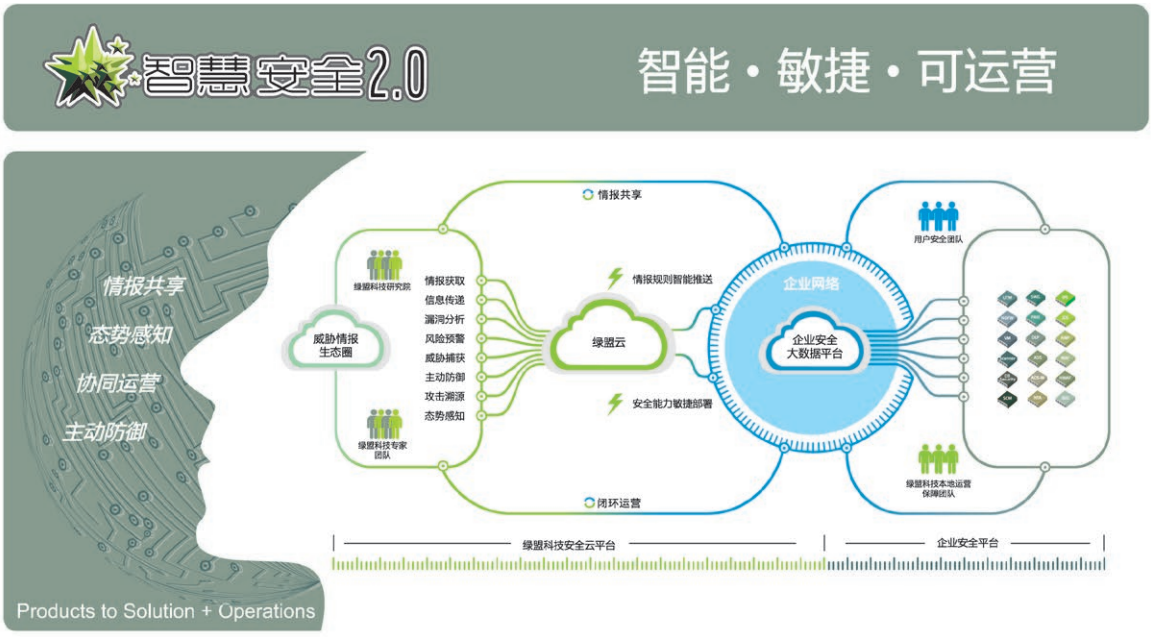
2016 年 12 月，我国某互联网金融平台遭受 DDoS 攻击，攻击峰值最高达 325.9Gbps。最开始的 DDoS 攻击峰值在 10Gbps 左右，黑客要求支付每月 3 万元才停止攻击，第二天攻击就升级到 325.9Gbps，攻击一直持续到当天晚上 19 点。

5. DDoS 防护趋势

5.1 智能、敏捷、可运营

2015 年，绿盟科技发布了以智能、敏捷、可运营为核心理念的，包括“绿盟云”安全服务平台、安全态势感知解决方案、云计算安全解决方案，以及下一代威胁防御解决方案的智慧安全 2.0 战略。

图 5.1 绿盟科技智慧安全 2.0



绿盟抗 D 云清洗解决方案，正是围绕以上理念展开。绿盟科技在 2016 年发布了云清洗运营平台：

图 5.2 绿盟科技云清洗运营平台大屏展示界面

绿盟科技云清洗运营平台具备如下特性：

智能	敏捷	可运营
• 绿盟云端威胁情报资源整合 • 绿盟云端专家策略库整合 • 产品端安全业务学习能力	• 主动感知用户业务状态 • 防护策略智能决策 • 产品端快速执行能力	• 用户自助化安全配置服务 • 自动化告警推送服务 • 清洗资源自动调度 • 客户资源管理系统 • 计费系统 • 产品端完备的 API 接口 • IOS/Android 客户端支持

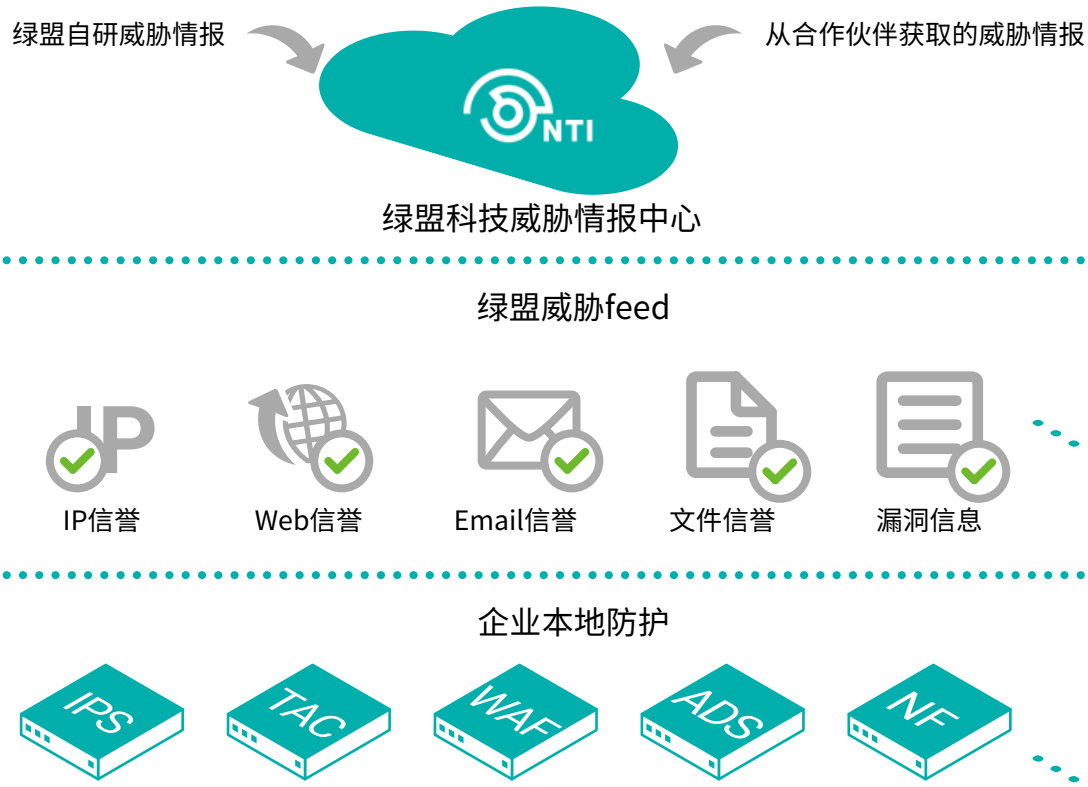
基于绿盟科技云清洗运营平台，可帮助用户更好、更快的对抗 DDoS 攻击，保护用户业务。

5.2 基于威胁情报的 DDoS 防护

近年来，越来越多的攻击者利用僵尸网络进行攻击，一方面僵尸主机数量巨大，尤其是物联网设备，成为黑客僵尸网络资源的新宠，这些设备在全球范围内数量庞大，且普遍存在安全漏洞，短期内难以解决，易于感染和利用，能发起 Tbps 级别的超大流量攻击；另一方面，僵尸工具越来越智能化，很多已经可以绕过部分防护算法，如常用的 302 跳转、JS 等防护机制；因此，僵尸网络的防护成为一个难题。

绿盟科技产品引入了基于情报的 DDoS 防护机制，抗 D 产品可与绿盟云端的威胁情报中心 NTI 连接，获取 IP 信誉数据（包括各种类型 Botnet IP 地址等精确信息），直接对这些 Bot 流量进行阻断或限速。购买绿盟科技 ADS 产品的用户，将得益于大数据分析为其带来的更便捷和准确的防护，从而体会到接入云端的价值。

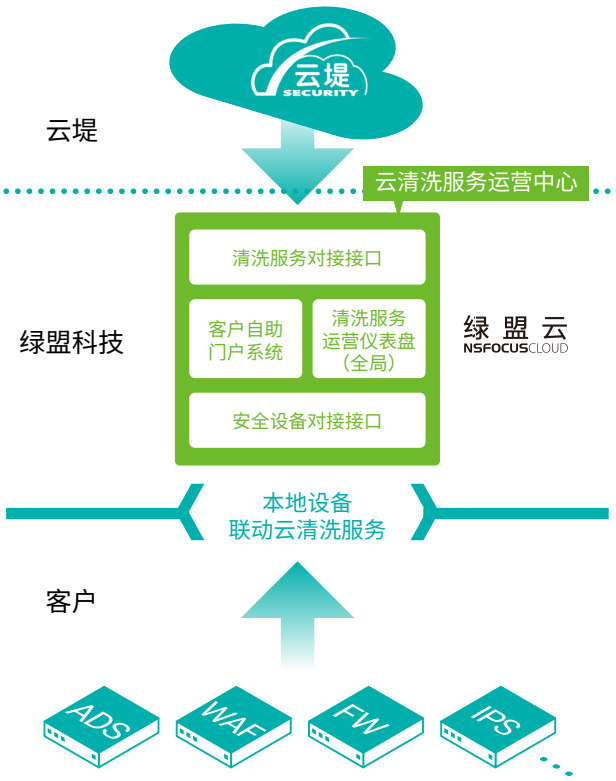
图 5.3 绿盟科技威胁情报中心（NTI）



5.3 本地 + 云端的混合清洗方案

随着 DDoS 攻击流量增大、频次增高、复杂化、产业化的趋势，DDoS 防护也面临挑战。通常硬件防护设备在本地部署，用于近目的清洗，防护策略可根据客户实际业务做调整，但面临接入带宽资源消耗问题，无法抵御大流量攻击，不少客户面临带宽被打满，缺乏专业的 IT 安全人员的情况，很难对 DDoS 攻击做出及时有效的响应或防御。因此，各大运营商 / 厂商开始提供云清洗服务，如中国电信的“云堤”，“云堤”提供的流量清洗是突破性的近源清洗，利用电信全网资源在近攻击源处完成流量清洗，解决接入带宽消耗问题。绿盟科技与中国电信“云堤”合作，可创新性实现本地 + 云端混合清洗技术，达到优势互补，明显提升防护清洗效果。

图 5.4 云清洗场景



混合云清洗场景：

1. 用户有绿盟安全设备，购买了绿盟的云清洗服务；
2. 云清洗服务开通时，提供自服务账号给用户，用户自行配置与本地设备联动的相关配置后，用户本地设备将 DDoS 攻击流量信息上传至绿盟云。如果用户处的攻击流量超过设定阈值，将自动联动云清洗服务或短信通知用户当前攻击超阈值的情况，请其自行决定是否联动云清洗服务，如需要联动，可以做到一键联动云清洗服务；或自动触发云清洗服务；
3. 用户可以通过自服务页面实时查看清洗情况（云清洗和本地清洗报表），绿盟运维工程师运维在运营界面密切关注客户 DDoS 攻击清洗情况。

云清洗可解决大流量攻击的带宽问题，但购买云清洗的带宽费用昂贵，并且很难针对客户业务特点做精准防护，用户陷入两难选择。为了解决用户这一问题，我们提出了抗 D 本地 + 云端混合清洗的防护方案，80% 的攻击由本地防护设备清洗，小于 20% 的大流量攻击联动云端清洗服务进行远程清洗，为用户打造了立体抗 D 混合清洗方案。

图 5.5 混合防护方案

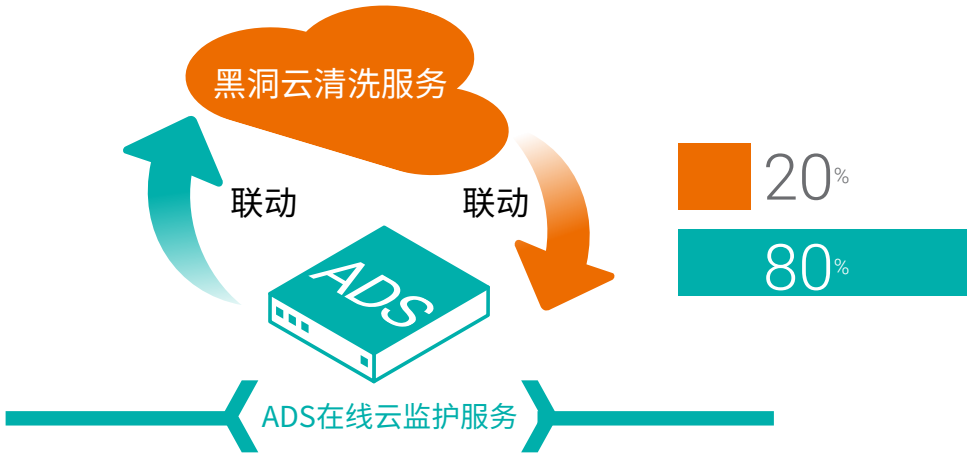
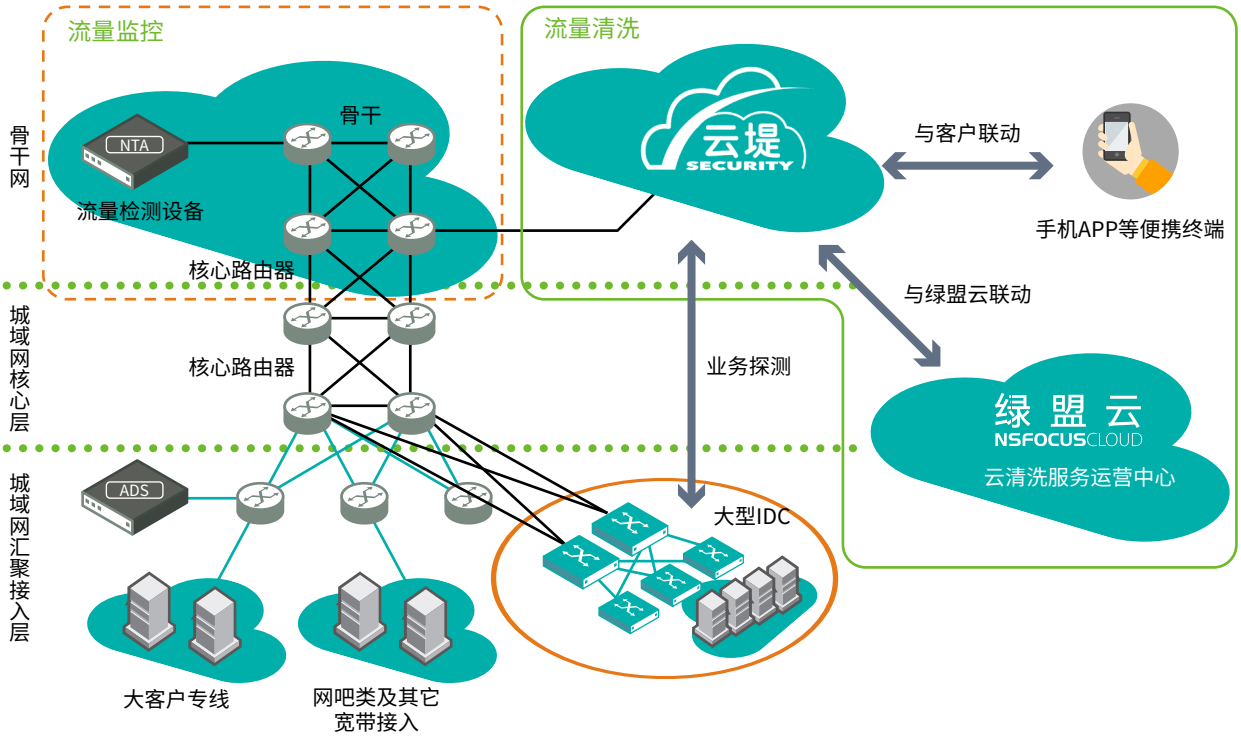


图 5.6 混合防护方案部署



抗 D 混合清洗方案的价值在于：

1. 攻击快速响应；
2. 防御能力强；
3. 业务私密性强，只有大流量攻击时才牵引，大部分时间流量只过本地；
4. 性价比高，花费少量成本即可建立本地 + 云端的立体抗 D 防护体系；
5. 防御带宽大，可防护超 300Gbps 的 DDoS 攻击。

抗 D 混合防护方案，可有效应对大流量和应用层复杂攻击，目前绿盟科技在国内、国外多地分布有云清洗中心。

图 5.7 绿盟国际云清洗中心分布图

结束语

本报告通过对 DDoS 攻击数据及僵尸网络数据进行多维度解读，以及对 2016 年多个有代表性的攻击事件进行总结分析，揭示了 2016 年 DDoS 攻击的威胁和整体变化趋势。

物联网、云计算等技术的普及已深刻影响着 DDoS 攻防形势，我们面临的安全防护形势更加严峻。DDoS 攻击从最初基于 PC 机的僵尸网络攻击，到近两年盛行的反射放大攻击，再到现在越来越多的基于云主机、物联网设备的僵尸网络攻击，我们看到 DDoS 攻击规模不断扩大，攻击算法更加智能。各种攻击服务的产业化，也使得发起复杂、大规模攻击的门槛大大降低，近年多起破坏力巨大的 DDoS 攻击事件已经给互联网安全敲响了警钟。

不断变化的业务环境，以及不断升级的安全威胁，给传统 DDoS 防护模式带来巨大挑战。在新威胁形势下，如何基于大数据分析、威胁情报共享、多方协同联动等，构建好智能、敏捷、可运营的 DDoS 防护体系，为客户做好 DDoS 防护工作，需要我们安全从业人员不断思考、落地。

作者

中国电信云堤　张敏　常力元　刘紫千　刘长波　陈林

绿盟科技　潘文欣　何坤　孙叶　杨旭　王洋

编辑　**绿盟科技**　郝明　黄柱（平面设计）

DDoS 威胁报告

SECURITY

DDoS（分布式拒绝服务）作为网络安全威胁中的典型攻击手段，从诞生的那天起就从未停止，而网络安全威胁也正在变得日益复杂，各类攻击目标、手段就来源始终在不断的发生着变化，随之企业及各类组织需要不断关注这些发展趋势，以便能够理解与预测未来可能遭遇到的恶意攻击，进而让应对复杂变化所带来的挑战。

本次报告即为 2016 全年的 DDoS 威胁报告，帮助大家：

- 持续了解及掌握 DDoS 威胁发展态势
- 在遭遇到攻击后，可以快速理解及检测可能的伤害程度
- 不断强化网络安全意识，完善解决方案

2016 DDoS Threat Report