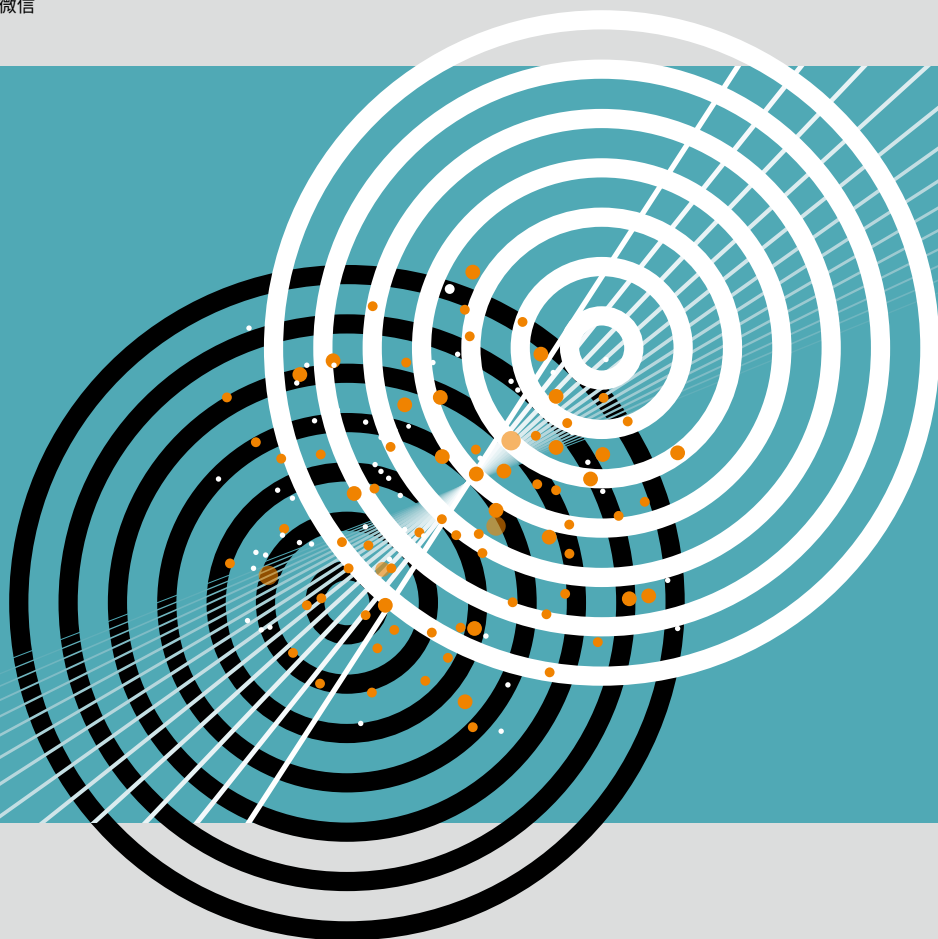




中国电信云堤官方微信



绿盟科技官方微信



2017 DDoS 与 Web 应用攻击 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。

1. 前言	1
2. 2017 年 DDoS 攻击态势概览	2
1. 2017 vs. 2016	2
2. 2017 H2 vs. 2017 H1	2
3. 重要观点	3
3. 2017 年物联网僵尸网络趋势概览	4
4. 2017 年 Web 应用攻击态势概览	5
5. 2017 年 DDoS 攻击趋势	6
5.1 DDoS 攻击次数和流量峰值情况	7
5.1.1 DDoS 攻击次数和攻击流量	7
5.1.2 攻击峰值各区间分布	9
5.1.3 单次攻击最高 / 平均峰值	11
5.2 攻击源特征分析	12
5.2.1 各攻击规模攻击源主机类型分布	12
5.2.2 物联网 IoT 类攻击源具体类型分析	13
5.2.3 各季度参与 DDoS 攻击的攻击源数量和类型统计	15
5.2.4 DDoS 攻击源主机攻击广度及其 IP 信誉	16
5.3 DDoS 攻击类型分析	17
5.3.1 各攻击类型次数和流量占比	17
5.3.2 攻击类型各流量区间分布	18
5.4 反射攻击	19
5.4.1 以 NTP 为代表的传统类型反射攻击活动放缓	19
5.4.2 新型 Memcached 反射攻击来势汹汹, 1.35Tbps 峰值创新高	22
5.5 DDoS 攻击持续时间	26
5.5.1 DDoS 攻击持续时间占比	26
5.5.2 DDoS 攻击持续时间变化趋势	27
5.5.3 被攻击频次与攻击时长	28
5.6 DDoS 攻击时间画像	29
5.6.1 一天 24 小时 DDoS 攻击活动分布	29
5.6.2 一周 7 天 DDoS 攻击活动分布	29
5.7 DDoS 攻击地域分布	30
5.7.1 DDoS 攻击源地域分布	30
5.7.2 DDoS 被攻击目标地域分布	31

6. 物联网僵尸网络发展趋势	32
6.1 物联网僵尸网络发展趋势	33
6.1.1 感染方式升级：从弱口令破解到 Oday 漏洞利用	33
6.1.2 感染平台进一步扩张：具备跨平台传播能力	33
6.1.3 隐蔽性增强：使用更隐蔽的扫描方式和沙箱技术	35
6.1.4 攻击武器库不断升级：集成反射攻击能力	35
6.1.5 黑产继续加紧争夺 IoT Botnet 资源	35
6.1.6 来自物联网设备的威胁将继续扩大	37
6.2 热点 IoT Botnet 对比分析	38
6.2.1 热点 IoT Botnet 概述	38
6.2.2 寄宿平台对比分析	38
6.2.3 传播手法对比分析	39
6.2.4 潜在威胁对比分析	40
7. 2017 年 Web 应用攻击态势	41
7.1 被攻击目标站点	42
7.2 被攻击目标行业	43
7.3 Web 应用攻击类型	43
7.3.1 Web 应用攻击类型	43
7.3.2 注入类攻击常见 Payload 注入位置	44
7.3.3 SQL 注入攻击常见 Payload	45
7.4 利用 Web 服务器已知漏洞的攻击	46
7.4.1 受攻击的目标服务器类型	46
7.4.2 攻击利用 Web 服务器已知漏洞的类型	46
7.4.3 利用 Web 服务器已知漏洞攻击 Top10	47
7.5 利用 Web 框架或应用已知漏洞的攻击	47
7.5.1 受攻击的 Web 框架或应用类型	47
7.5.2 利用 Web 框架或应用已知漏洞 TOP10	48
7.6 Web 攻击源 IP 攻击广度与其 IP 信誉	49
7.7 Web 应用攻击时间分布	50
7.8 Web 应用攻击地域分布	52
7.8.1 攻击源主机地理分布	52
7.8.2 攻击目标地理分布	52
7.9 热点漏洞分析	53
7.9.1 Apache Struts 2 REST 插件安全漏洞 (CVE-2017-9805)	53
7.9.2 WebLogic XMLDecoder 反序列化漏洞 (CVE-2017-10271)	53
8. DDoS 和 Web 应用攻击防护	55
8.1 DDoS 攻击防护	56
8.2 Web 应用攻击防护	58


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。



内容提要

本报告在第 5 章通过攻击流量、频次、攻击规模的变化情况，结合攻击源分析，攻击类型分析，攻击持续时间、攻击地域分布等多个维度力求全面呈现 2017 年 DDoS 攻击变化趋势。报告第 7 章主要介绍 2017 年 Web 应用攻击态势，包括被攻击站点情况、被攻击行业情况，结合 Web 应用攻击类型，攻击源分析、攻击时间、攻击地域分布等方面的分析。鉴于物联网僵尸网络的重要性，本报告单独成立第 6 章进行介绍，总结了 2017 年物联网僵尸网络的 6 个发展趋势，并从寄宿平台、传播手法、潜在威胁等三方面对 2017 年热点物联网僵尸网络进行对比分析。第 8 章，结合当前 DDoS 和 Web 应用攻击的威胁形式，给出了绿盟科技基于多年来在安全防护方面的经验积累和持续创新总结出的安全防护解决方案。报告第 2、3、4 章分别是 2017 年 DDoS 攻击趋势、物联网僵尸网络发展趋势、Web 应用攻击态势的重要观点和趋势的提炼，以便帮助读者更好的理解报告内容。



DDoS 攻击和 Web 应用攻击是当今互联网面临的较为突出的**两大安全威胁**。

DDoS 攻击特性

上升

- 攻击总流量 64 万 TBytes, 比 2016 年增长 **79.4%**
- 单次攻击平均攻击峰值 14.1Gbps, 比 2016 年增长 **39.1%**
- 单次攻击最高攻击峰值 1.4Tbps, 是 2016 年的近 **2** 倍

主导

- SYN Flood** 攻击总流量占主导地位 61.6%
- 攻击时长 **≤30 分钟** 的 DDoS 攻击占全部攻击的近一半
- Linux/Unix** 类主机或服务器成 DDoS 稳定攻击源 (55%)
- IoT** 类设备更多地参与到小型攻击中 (29.8%)
- IoT 类攻击源中, **家用路由器** 占比高达 69.7%

下降

- 攻击总次数** 20.7 万次, 相比 2016 年下降 5.8%
- 2017 下半年比上半年 **总攻击流量** 下降 27.2%
- 2017 上半年 **平均攻击峰值** 从 16.9Gbps 下降到 11.2Gbps

Web 应用 攻击特性



近 **3/4** 站点遭受过任意类型的 Web 应用攻击

92.2% 的 Web 应用攻击是针对 **互联网企业** 的

最常利用的攻击方式 **XSS 跨站脚本攻击** 占 37.7%、注入类攻击 20.7%

有 56% 的利用服务器漏洞的攻击都会导致 **关键信息的泄露**

已知框架或应用漏洞攻击中, **Apache Struts2** 的漏洞是最频繁被利用的漏洞



- 传统反射攻击活动放缓, 新型 Memcached 反射 T 级攻击来势汹汹
- 基于物联网 IoT 设备的 Botnet 不断升级换代, 威胁不容小觑

1. 前言

基于互联网衍生出来的云计算、大数据、物联网、移动计算等新技术与新模式，深刻地影响着网络世界的变革。在这样的大背景下，网络安全面临的威胁也在不断变化与升级。

其中，DDoS 攻击和 Web 应用攻击是当今互联网面临的较为突出的两大安全威胁。从攻击手段和攻击目的来看，二者截然不同，但二者往往不是相互独立的，而是紧密联系的，可以简单认为 DDoS 攻击和 Web 应用攻击分别处于攻击链中的不同环节，而僵尸网络（Botnet）就是二者联系的“桥梁”。从单个的 Web 应用攻击事件来看，针对某一 Web 站点的扫描、注入、利用已知漏洞渗透等一系列的攻击行为，可能是攻击者为了获取该站点的权限，并进一步获取机密数据，又或者作为攻击企业网络中其他重要基础设施的跳板。但很多攻击者并不仅满足于此，他们常常在获取服务器权限后，种下 Botnet 恶意程序，构建属于自己的僵尸网络大军。僵尸网络作为黑客进一步谋利的工具，经常被用于进行 DDoS 攻击，挖矿，扫描，点击欺诈，发送垃圾邮件等活动。针对某些服务器或 Web 应用漏洞的扫描又是感染并控制主机的第一步，攻击者经常利用已经被感染的设备在网络中发起扫描以发现更多待感染目标。

DDoS 攻击、挖矿活动是攻击者能够直接谋利的活动，通常是处于攻击链的最后一个环节。2017 年 10 月份爆发的 WebLogic XMLDecoder 反序列化漏洞（CVE-2017-10271），在爆出不久后就有黑客利用该漏洞在 Weblogic 主机间传播感染僵尸程序用于挖矿¹。又如，2017 年爆出的物联网僵尸网络变种 IoT_reaper²，利用了多个物联网相关的漏洞构建僵尸网络，其中之一就是某些网络摄像头存在的 Goahead Web Server 漏洞（CVE-2017-8221 到 CVE-2017-82215）³。而 IoT_reaper 僵尸网络的一个重要功能就是 DDoS 攻击。

本报告将 DDoS 攻击和 Web 应用攻击态势一同发布，力求给网络安全相关从业人员一些参考，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 <http://toutiao.secjia.com/weblogic-host-mining>

2 <https://research.checkpoint.com/new-iot-botnet-storm-coming/>

3 <https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html>



2017 年 DDoS 攻击规模增大，
攻击峰值突破新高，企业面临的
DDoS 攻击威胁扩大

2. 2017 年 DDoS 攻击态势概览

1. 2017 vs. 2016

- 2017 vs. 2016 攻击总次数 20.7 万次，下降 5.8%
- 2017 vs. 2016 攻击总流量 64 万 TBytes，增长 79.4%
- 2017 vs. 2016 单次攻击平均攻击峰值从 10.1Gbps 增长到 14.1Gbps，增长 39.1%。
- 2017 vs. 2016 单次攻击最高攻击峰值 1.4Tbps，是 2016 年（738Gbps）的近 2 倍
- 2017 vs. 2016 平均攻击时长为 12 小时，相比 2016 年的 8.8 小时增长 36%
- 2017 vs. 2016 最长一次 DDoS 攻击持续了 16 天 2 小时（386 小时），相比 2016 年的 36 天 16 小时（880 小时）下降一半
- 2017 vs. 2016 SYN Flood 流量增长明显，在峰值超过 300Gbps 的超大规模攻击中占比 88.7%，相比 2016 年的 39% 翻了 1 倍

2. 2017 H2 vs. 2017 H1

- 2017H2 vs. 2017 H1 总攻击流量下降 27.2%
- 2017H2 vs. 2017 H1 平均攻击峰值从 16.9Gbps 下降到 11.2Gbps，下降 33.7%
- 2017H2 vs. 2017 H1 最高攻击峰值 1.4Tbps vs. 713Gbps
- 2017H2 vs. 2017 H1 平均攻击时长 8.8 小时 vs. 15.6 小时

3. 重要观点

观点 1: 2017 年 DDoS 攻击规模不断增大，攻击峰值不断突破新高。

一方面，DDoS 攻击服务化、产业化；另外一方面，由于物联网的加入，可利用的攻击源种类越来越多，针对物联网的 Botnet 也在不断升级换代。使得攻击成本越来越低，攻击规模会继续增大。从趋势看，企业面临的 DDoS 攻击威胁逐年在扩大。

观点 2: DDoS 攻击活动受政策监管和利益驱动的影响明显。

2017 年上半年攻击势头强劲，下半年攻击势头减弱。2017 年下半年总流量比上半年减少 27.2%，单次攻击平均攻击峰值下降 33.7%。以对比明显的中型攻击为例，在 Q4 季度参与中型攻击的攻击源相比 Q2 下降了 314%。通过攻击源分析，发现下半年基于 Windows 和 Linux/Unix 的主机类型的攻击源明显减少，而常用于小规模攻击的物联网设备攻击源显著增多，前者明显计算性能更高。面对国家政策的威慑和监管的强力整治，黑产将掌握的“高性能” Botnet 资源从犯罪成本较高的 DDoS 攻击活动转而投向了犯罪成本相对较低但收益更高的挖矿活动中，反映了黑产对攻击资源的投入受政策监管和利益驱动的影响明显。

观点 3: Linux/Unix 类主机和服务器构成稳固的 DDoS 攻击源（55%），IoT 类设备参与小型攻击更多（小型攻击中占比 29.8%，大型攻击中占比 10.3%），相比之下大型攻击 Windows Server 类设备更常见。

观点 4: 物联网（IoT）攻击源中，以家用路由器或调制解调器类设备占比最高（69.7%），虽然 IoT 较多被用于小型 DDoS 攻击，但 IoT 安全问题突出（漏洞多、修复难度大），种类多数量巨大，且针对其的恶意程序不断在升级换代，我们不能轻易对来自 IoT Botnet 的威胁放松警惕。

观点 5: DDoS 攻击多发于业务使用高峰期，以实现对目标的精准打击。一天中工作时段和前半夜休闲时间（10-22 点）发生的攻击占 75.7%，一周中多发生在工作日。

观点 6: 以 NTP 为代表的传统类型反射攻击趋势放缓，新型 Memcached 反射攻击来势汹汹，1.35Tbps 峰值破新高。

观点 7: 中国为受控攻击源最多的国家，占比约为全球的 1/2，山东、新疆首次列入国内 TOP5。

观点 8: 中国也是受 DDoS 攻击最严重的国家，60% 的攻击瞄准中国，国内浙江依然最多，福建排入 TOP3。



3. 2017 年物联网僵尸网络趋势概览

来自物联网僵尸网络的威胁将继续扩大。虽然从攻击溯源数据看，物联网设备更多地被用于小型 DDoS 攻击中，但我们不能就此放松对物联网设备的警惕。据绿盟科技《2017 物联网安全研究报告》的数据显示，2017 年全球暴露的物联网设备约 6200 万，其中路由器设备最多，总数约 4900 万台，国内暴露的路由器设备约 1092 万台。如果假设这部分暴露的设备被感染的概率仅为 1%，那么仅国内被感染的路由器设备就能轻松打出 T 级别的 DDoS 攻击。按照当前物联网设备令人堪忧的安全状况和修复情况看，暴露在网络中的这些设备被感染的概率要远高于 1%，这些资源一旦掌握在不法分子手中，威胁将不可估量。与此同时，针对物联网的僵尸网络变种不断出现，能力不断升级。

物联网僵尸网络的发展趋势：

趋势一：感染方式升级：从弱口令破解到 0day 漏洞利用

趋势二：感染平台进一步扩张：具备跨平台传播能力

趋势三：隐蔽性增强：使用更隐蔽的扫描方式和沙箱技术

趋势四：攻击武器库不断升级：集成反射攻击能力

趋势五：黑产继续加紧争夺 IoT Botnet 资源

趋势六：由于物联网数量庞大，再加上本身安全问题突出（漏洞多，修复难度大），可以轻易被感染和控制，因此来自物联网设备的威胁将继续扩大



2017 年监控到 73.6% 的 Web 站点遭受过任意类型的 Web 应用攻击，92.2% 针对互联网行业

4. 2017 年 Web 应用攻击态势概览

1. 有 73.6% 的 Web 站点曾遭受过任意类型的 Web 应用攻击。
2. 有 65.9% 的站点曾遭受利用已知 Web 漏洞的攻击（包括针对已知 Web 服务器漏洞和 Web 框架漏洞的攻击）。
3. 92.2% 的 Web 攻击是针对互联网企业的，但各行各业都应该重视 Web 类的攻击，Web 攻击往往是打开企业内网的第一道大门。
4. XSS 跨站脚本攻击占 37.7%，其风险虽然从 A3 下调至 A7，但其仍然是黑客进行 Web 攻击时最常利用的攻击方式。
5. 注入类攻击占比为 20.7%，在 2017 年重构的《OWASP Top10》中此类攻击风险定义为 A1 级别。
6. 已知服务器漏洞攻击中，攻击较多的是 Microsoft IIS（39%）、Nginx（30%）、Apache Tomcat（28%）三种服务器类型。
7. 有 56% 的利用服务器漏洞的攻击都会导致关键信息的泄露，且大部分都是一些比较古老的服务器漏洞。
8. 已知框架或应用漏洞攻击中，有 94.3% 的攻击针对对框架类程序，Apache Struts2 的漏洞是最频繁被利用的漏洞，其中针对 Apache Struts 2 REST 插件安全漏洞（CVE-2017-9805）攻击最高达 335,776 次 / 日。
9. 大部分 Web 应用的攻击同样发生在一天中 Web 业务使用高峰期 9 点 -18 点，占 53.6%，而利用已知 Web 漏洞的攻击较多发生在凌晨或周末，这与其攻击方式和攻击目的密切相关。
10. 北京、浙江两省稳坐 Web 攻击源和被攻击目标的 Top3。
11. WebLogic XMLDecoder 反序列化漏洞（CVE-2017-10271）在爆出不久后就有黑客利用其对 Weblogic 主机进行挖矿恶意程序的感染，利用该漏洞攻击者能够同时攻击 Windows 及 Linux 主机。

2017 年我国境内共发生攻击
20.7 万次，攻击总流量 64 万
TBytes，DDoS 攻击受政策和
利益驱动影响明显



5. 2017 年 DDoS 攻击趋势

- 5.1 DDoS 攻击次数和流量峰值情况 7
- 5.2 攻击源特征分析 12
- 5.3 DDoS 攻击类型分析 17
- 5.4 反射攻击 19
- 5.5 DDoS 攻击持续时间 26
- 5.6 DDoS 攻击时间画像 29
- 5.7 DDoS 攻击地域分布 30

5.1 DDoS 攻击次数和流量峰值情况

5.1.1 DDoS 攻击次数和攻击流量

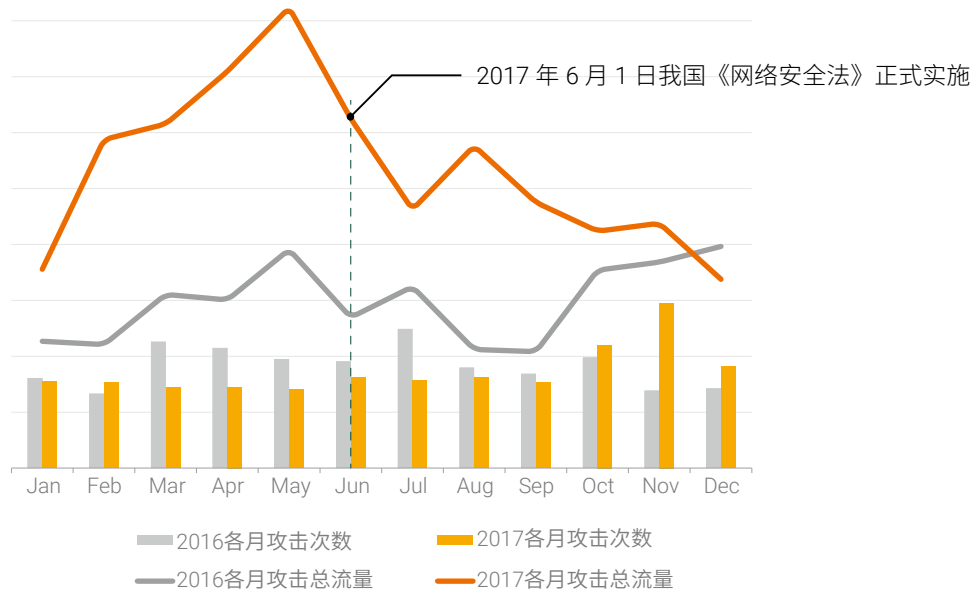
2017 年我国境内共发生 DDoS 攻击 20.7 万次，与 2016 年相比下降 5.8%。攻击总流量达 64 万 TBytes，相比 2016 年增长 79.4%。2017 年全年 DDoS 攻击次数虽有所下降，但攻击总流量较 2016 年明显增长。这主要因为 2017 年 DDoS 攻击规模整体偏大，即 2017 年中、大型规模的攻击明显增多，小规模攻击显著下降，具体详见 5.1.2 节。

单从 2017 年全年看，DDoS 攻击总流量在上半年的前两个季度处于持续增长阶段，到 Q2 的 5 月份达到全年最高峰，此后从 6 月份开始（除了 8 月份有小幅波动外）几乎一直处于下降趋势，Q4 达到最低。2017 年下半年攻击总流量比上半年下降 27.2%。虽然 Q4 季度的 DDoS 攻击次数高于前三个季度，但进入 Q4 季度后，小流量攻击增多，中、大型规模攻击大幅减少（详见 5.1.2 节），致使总攻击流量大幅下降。Q4 季度攻击的平均攻击峰值明显低于前三个季度也能说明这一点（详见 5.1.3 节）。我们认为有两方面主要因素，影响了 DDoS 攻击的这一趋势。

一方面，2017 年 6 月 1 日《网络安全法》和《网络产品和服务安全审查办法（试行）》开始实施，明确了国家机关、企业和个人在网络安全方面的法律责任和义务，在“法律责任”中则提高了违法行为的处罚标准，加大了处罚力度，增加了网络犯罪的成本，对网络犯罪构成了强有力的震慑力。而且，国家有关部门联合开展各类网络安全专项整治行动，净化网络空间，整治效果显著。

另一方面，2017 年下半年以比特币为代表的虚拟货币开始暴涨。在国家政策的威慑和监管的强力整治下，我们推测，黑产开始将掌握的“优质”Botnet 资源从犯罪成本较高的 DDoS 攻击活动转而投向了犯罪成本相对较低但收益更高的挖矿活动中。这也反映了黑产对攻击资源的投入受利益驱动明显。

图 5.1 2017 年 vs.2016 年各月份攻击次数和流量图



数据来源：中国电信云堤

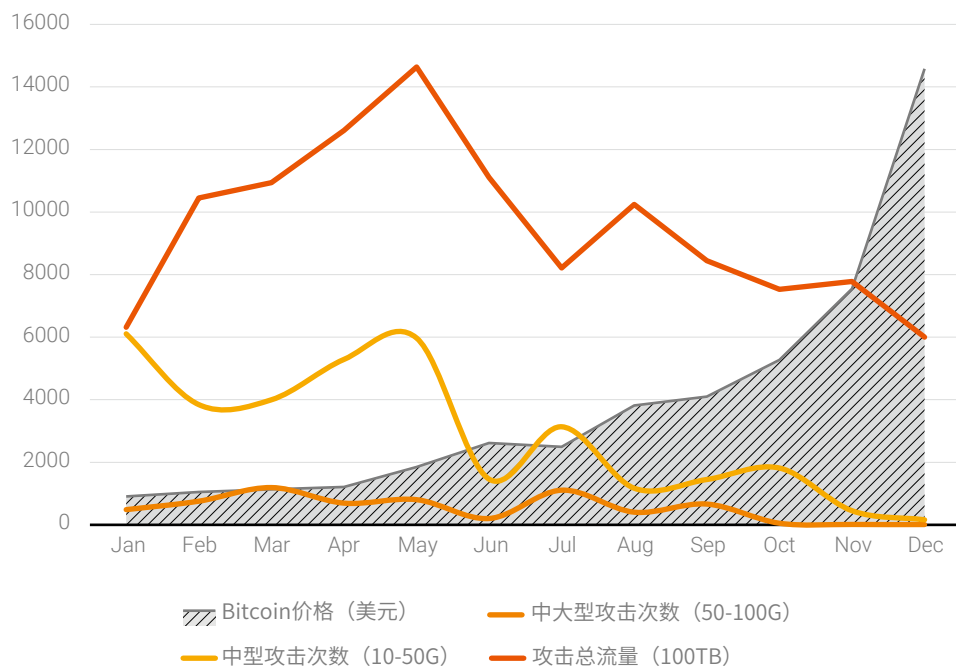
图 5.2 2017 年比特币价格趋势



数据来源: Bitcoin.com

我们将 2017 年各月份比特币价格趋势（取月平均值）与 DDoS 攻击总流量趋势做比较，有一个比较有趣的发现：DDoS 攻击总流量与比特币价格走势呈现负相关，相关指数为 -0.56；从攻击规模看，中型攻击，与比特币价格走势负相关指数最高，为 -0.73。从这一关系中我们推测，黑产有可能将从事 DDoS 攻击的 Botnet 资源转而投向了犯罪成本相对较低利润更加有吸引力的挖矿活动中。

图 5.3 2017 年各月份比特币价格走势与 DDoS 攻击趋势图



数据来源: 中国电信云堤

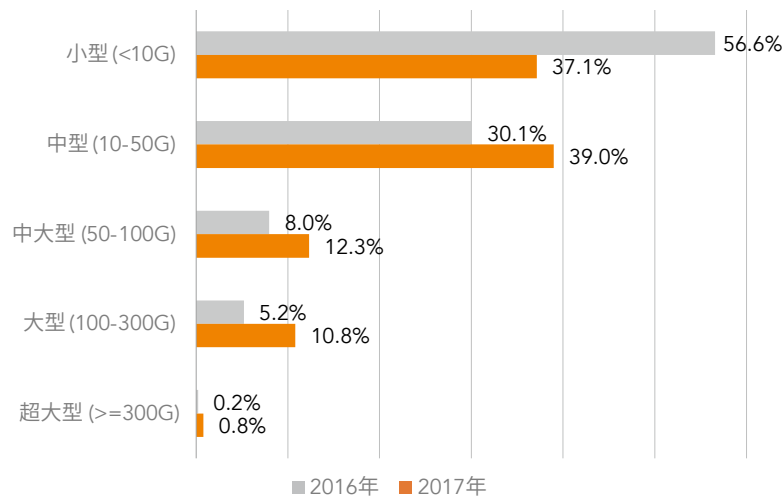
接下来，我们以 DDoS 中型攻击为例，分析其各季度攻击源及类型变化情况。具体内容请参见 5.2.3 节。

5.1.2 攻击峰值各区间分布

与 2016 年相比，2017 年 DDoS 攻击规模整体偏大。2017 年的大、中型 DDoS 攻击明显增多，小规模攻击相对减少。其中，涨幅最明显的为攻击峰值在 300Gbps 及以上的超大型攻击，相比 2016 此类攻击增长了 379%。中、大型的攻击也都在增长。唯独攻击峰值在 10Gbps 以下的小型攻击，相比 2016 年攻击减少 38%。2016 年小型攻击占全部攻击总数的一半之多（56.6%），而 2017 年这部分攻击占比为 37.1%，相比去年下降了 19.5 个百分点。

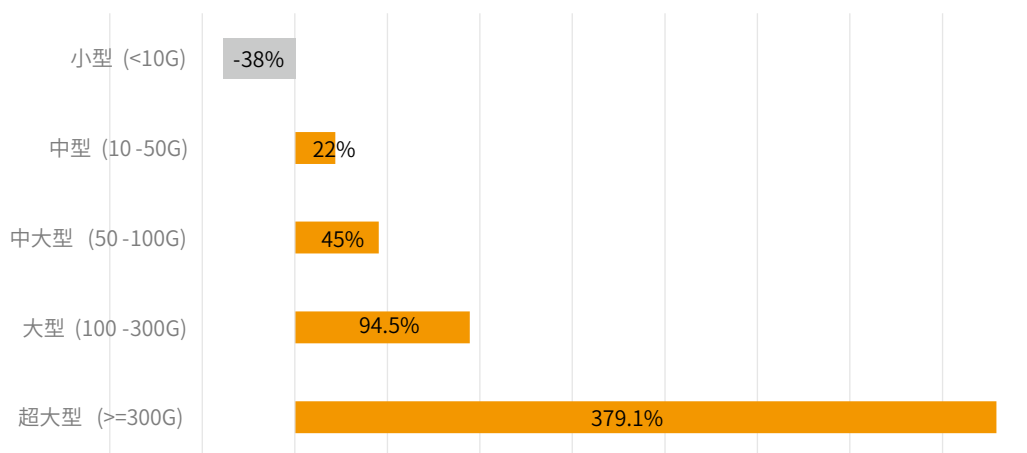
注 我们对 DDoS 攻击按照攻击规模进行分组，将攻击峰值在 10Gbps 以下的攻击归为小型攻击，峰值在 10-50Gbps 的攻击归为中型攻击，峰值在 50-100Gbps 的归为中大型攻击，峰值在 100-300Gbps 的归为大型攻击，最后，峰值在 300Gbps 以上的归为超大型攻击。

图 5.4 2017 年 vs.2016 年各类规模的攻击次数占比



数据来源：中国电信云堤

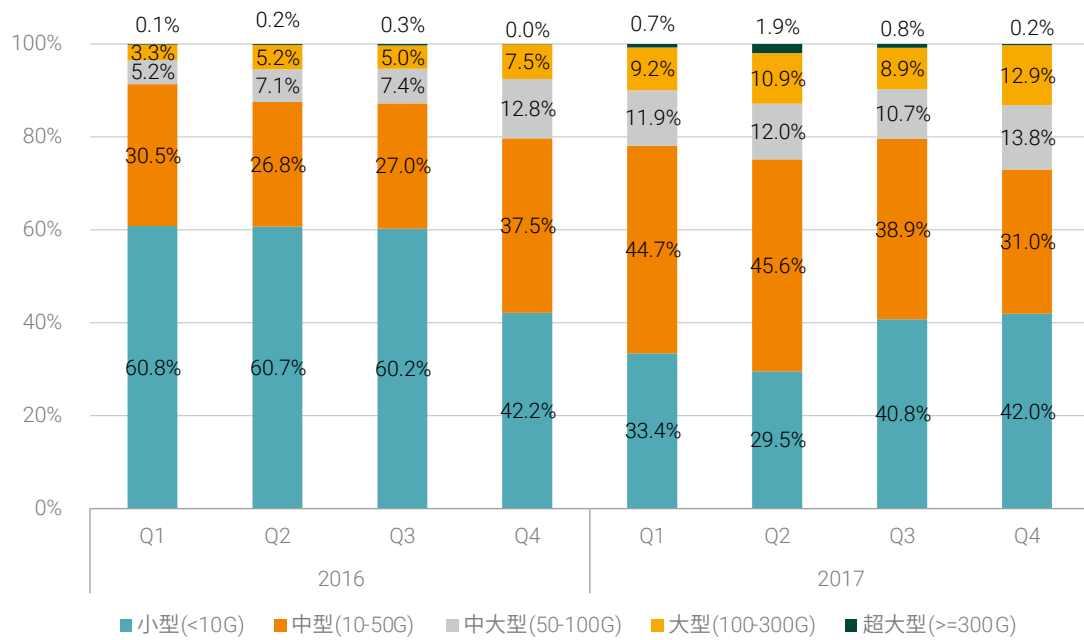
图 5.5 2017 年 vs.2016 年各类规模的攻击增长（减少）率



数据来源：中国电信云堤

从 2017 年各季度看，上半年攻击规模持续增大，下半年攻击势头逐渐下降。2017 前两个季度，中、大型攻击占比持续走高，攻击势头强劲。进入 Q3 季度后，中型、超大型 DDoS 攻击占比减少，小规模攻击显著增加。对比最明显的是 Q4 和 Q2 季度，中型攻击 Q4 相比 Q2 下降 14.6 个百分点，超大型攻击下降 89.5 个百分点，小型攻击 Q4 相比 Q2 增长 21.5 个百分点。关于这一变化趋势的原因分析，请详见 5.2.3 节。

图 5.6 2017 年 vs.2016 年各季度各类规模攻击次数占比



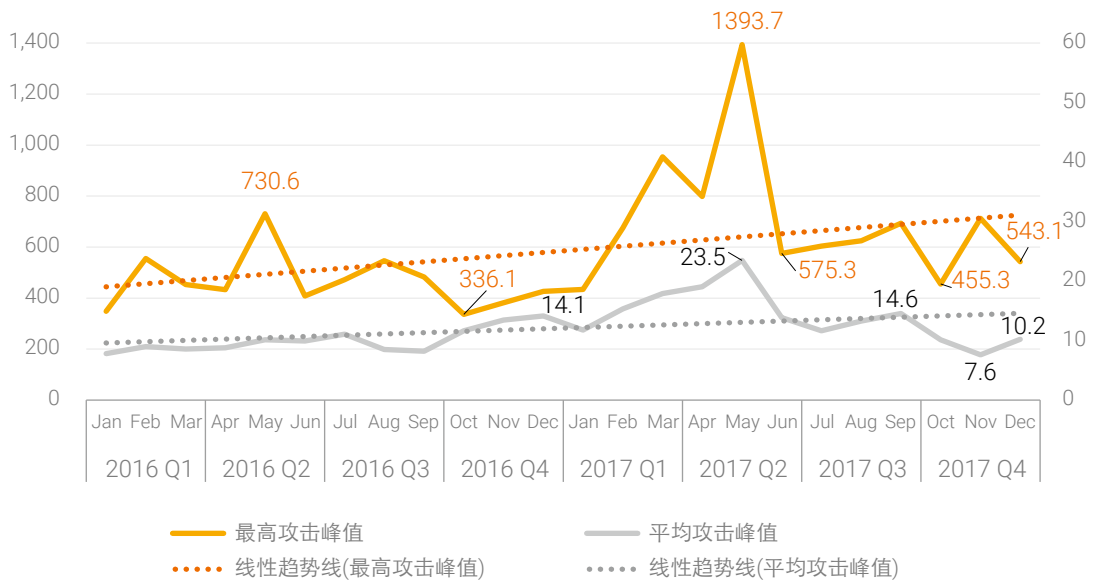
数据来源：中国电信云堤

5.1.3 单次攻击最高 / 平均峰值

2016年至2017年单次攻击平均攻击峰值和最高攻击峰值均呈整体上升趋势。2017年全年平均DDoS攻击峰值为14.1Gbps，比2016年增长39.1%。单次DDoS攻击规模最大的一次发生在2017年5月份，峰值达1.4Tbps，当月平均攻击峰值也达到全年最高值为23.5Gbps。

经过2016年至2017年前两个季度的持续增长，2017年下半年平均攻击峰值与最高攻击峰值有回降的趋势，2017年下半年单次攻击平均峰值比上半年下降33.7%。这与5.1.2节中分析的小规模DDoS攻击占比增多，中型、超大型攻击占比大幅减少直接相关。

图 5.7 各月份单次攻击峰值及平均攻击峰值趋势图（单位：Gbps）



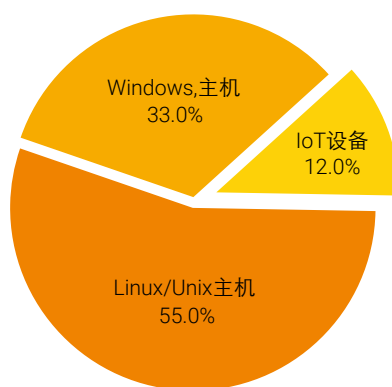
数据来源：中国电信云堤

5.2 攻击源特征分析

5.2.1 各攻击规模攻击源主机类型分布

我们将 2017 年参与过 DDoS 攻击的源进行溯源，利用绿盟科技威胁情报 NTI 对这些攻击源 IP 的类型进行识别，发现基于⁴Linux/Unix 的主机或服务器占比 55%，其次是 Window 类的主机或服务器占比 33%，其次是物联网 IoT 设备，占比 12%。

图 5.8 DDoS 攻击源设备类型分布



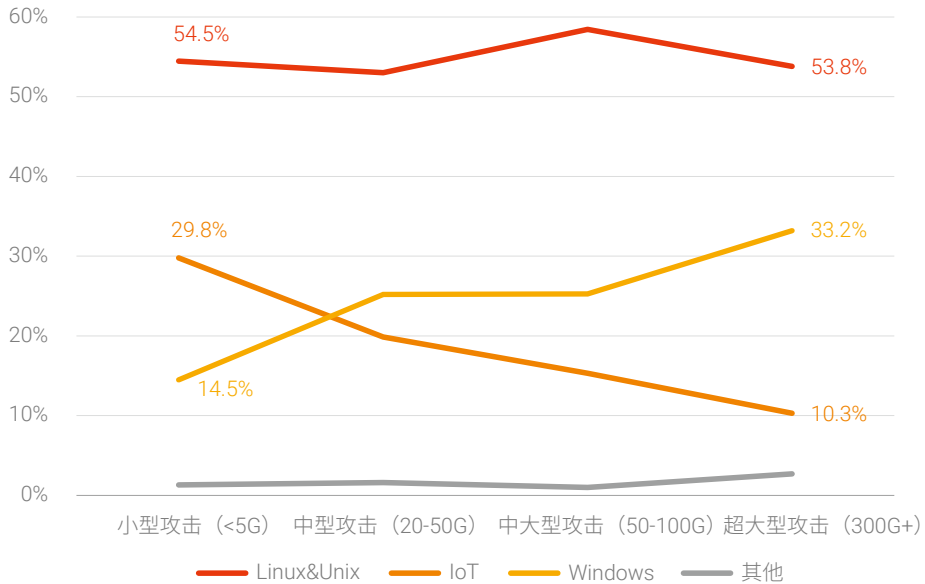
数据来源：绿盟科技威胁情报中心（NTI）

我们将这些攻击源按照参与攻击的规模进行分组，发现攻击源设备类型会随参与攻击规模的不同而发生变化。并且这一变化反映在物联网（IoT,Internet of thing）和 Windows 类型的攻击源上表现尤为明显：小型攻击中，IoT 类设备明显多于 Windows 类设备；从中型攻击开始，参与攻击的 IoT 类设备占比开始下降，Windows 类设备占比升高。其中，Windows 类的主机中，有 2/3 为 Windows Server 服务器。总体看，Linux/Unix 类设备类型⁵参与攻击最多，占比均在一半以上，在各攻击规模下其占比变化不大，成为较稳定的攻击源“贡献者”。

⁴ 这里主要指以 Linux/Unix 为系统的主机或服务器，不包含基于嵌入式 Linux 的物联网设备。

⁵ 这里的 Linux/Unix 类设备指基于 Linux/Unix 系统的 PC 或服务器，不包含物联网嵌入式系统

图 5.9 DDoS 攻击源类型分布随攻击规模的变化趋势



数据来源：绿盟科技威胁情报中心 (NTI)

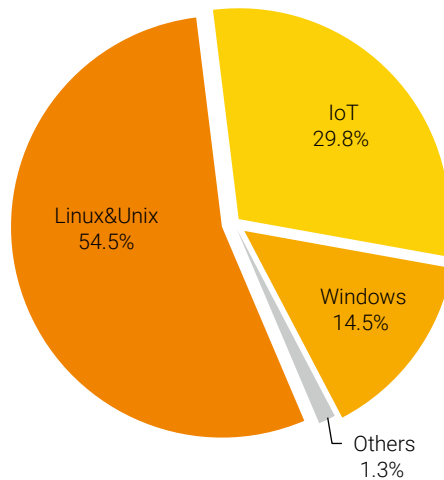
2017 年参与超大型 DDoS 攻击的独立 IP 约 15 万个。这些攻击源中 Linux/Unix 类主机占比 53.8%，其次是 Windows 主机占比 33.2%。IoT 设备在超大流量攻击源中仅占比 10.3%。且 Linux/Unix 和 Windows 类主机大部分为服务器，这其中有近一半的是 Web 服务器，也发现有较多的文件存储服务器、数据库服务器等。我们发现，其中部分设备使用了 VMware ESXi server，这类系统主要用于云端主机资源的虚拟化，以实现云端用户服务器资源的灵活分配。这一现象也再次印证了我们在《绿盟科技 2017 上半年 DDoS 和 Web 应用攻击态势报告》中提到的观点：攻击者通常会瞄准那些性能高、带宽大的服务器资源以寻求创造更强大、更高效的僵尸网络。

我们也看到，参与各规模攻击的攻击源类型的变化，与黑产控制的 Botnet 资源投入到 DDoS 活动的情况密切相关。例如，大型 DDoS 攻击一般用于精准打击某个目标，迫使其业务受到严重影响而不可用，这类攻击如果目的达成通常会给黑产带来很可观的收益，因此黑产更愿意调动带宽资源和性能更强的 Windows、Linux 类僵尸主机进行攻击以达成预期的目的。这类设备相比 IoT 类设备，由于在攻击过程中需要占用较高资源，很容易被管理员发现，导致 Botnet 的“掉鸡”，因此这类僵尸肉鸡资源，攻击者更愿意较多的投入到收益更高的攻击活动中去。

5.2.2 物联网 IoT 类攻击源具体类型分析

2017 年参与小型 DDoS 攻击的攻击源约有 130 万个独立 IP。从攻击源类型看，仍然是 Linux/Unix 类设备占比最高，达 54.5%，其次是 IoT 类设备，占比为 29.8%。这与超大型攻击源溯统计结果有着明显的差别，小型 DDoS 攻击的 IoT 设备的源占比大型攻击的占比高出了约 19.5 个百分点，物联网设备更多地参与到小规模 DDoS 攻击中。

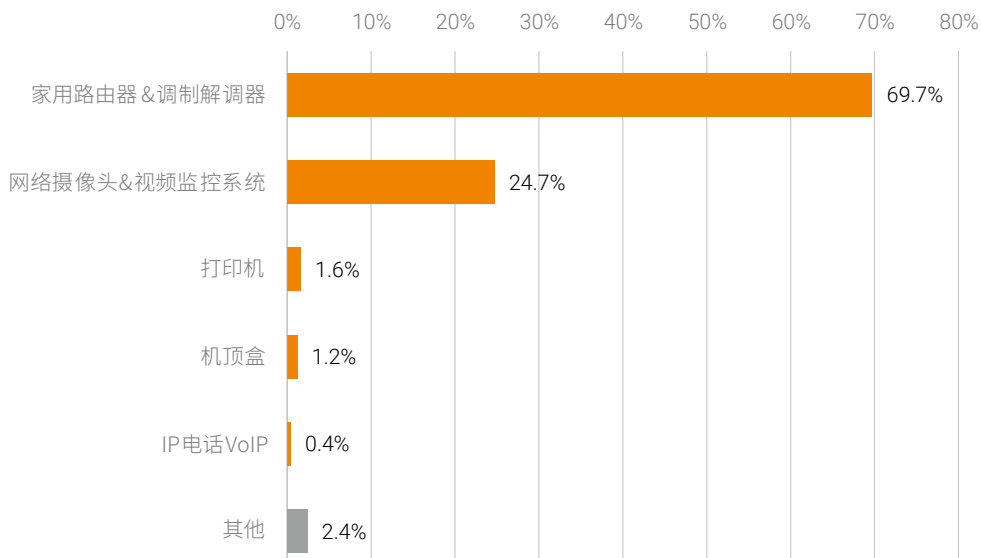
图 5.10 小规模 DDoS 攻击源各类型设备占比



数据来源：绿盟科技威胁情报中心 (NTI)

我们对参与小型攻击的 IoT 类设备的具体类型进行更深入的挖掘，发现家用路由器和调制解调器类设备占比高达 69.7%，视频监控设备占比 24.7%。其他包括打印机、机顶盒、IP 网络电话等物联网设备也均在列。

图 5.11 DDoS 攻击源 IoT 类设备具体类型分布



数据来源：绿盟科技威胁情报中心 (NTI)

我们对参与攻击的家用路由器类设备进一步分析，发现国内一些知名厂商的家用路由器和调制解调器类设备均在列，且占比较高。分析中发现，很大一部分无线路由器或调制解调器设备曾开放过 7547 端口⁶。这一端口正是 TR-069 (CPE WAN Management Protocol) 或 TR-064 协议 (LAN-Side CPE Configuration) 默认使用的端口。TR-069 协议和 TR-064 协议分别用于 WAN 侧和 LAN 侧对客户终端接入设备 (CPE) 如家用路由器、调制解调器等

⁶ http://www.theregister.co.uk/2016/11/28/router_flaw_exploited_in_massive_attack/

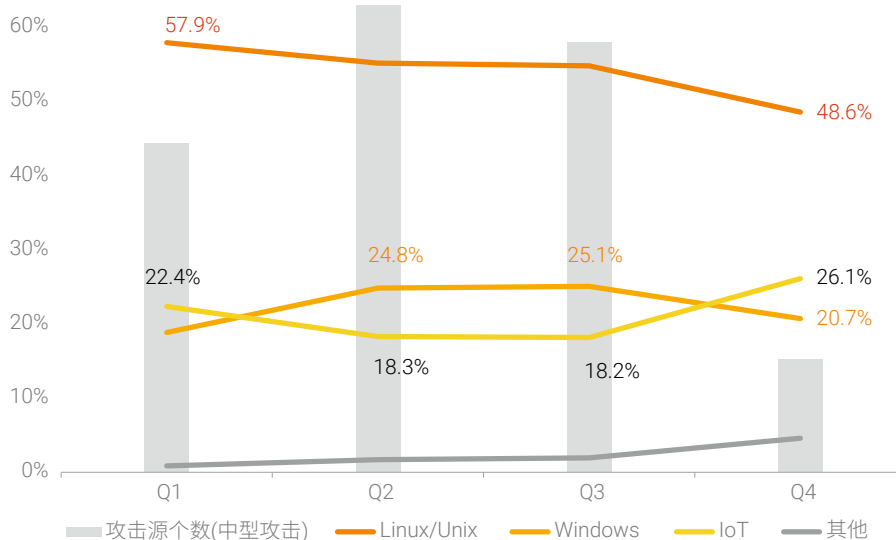
进行配置和管理。然而很多这类设备，并未限制 WAN 侧对 TR-064 协议的使用。这意味着，只要该端口向互联网开放，任何人都能够利用这一系列的安全漏洞连接这些家用路由器或调制解调器等 CPE 设备。更不幸的是，该协议在进行 NTP Server 配置时存在命令注入漏洞⁷。这样一来，恶意者利用如上漏洞对全球大量家用路由器进行控制也不足为奇。2016 年 11 月底，德国电信 Telekom 约 90 万客户断网事件正是由于 Mirai 变种利用了该协议的漏洞对大量家用路由器进行扫描导致的，据称有 4%-5% 的 Zyxel 路由器出现故障⁸。随后，陆续受到影响的还有英国 Kcom 公司、英国 TalkTalk 公司（36 万客户）⁹、英国 Post Office Broadband（10 万客户）以及爱尔兰电信 Eir 等¹⁰。

然而，这仅仅是我们看到的冰山一角，2017 年越来越多的基于物联网设备（IoT）的僵尸网络恶意程序出现，有些是基于 2016 年 Mirai 的变种，有些是传统 Linux 和 Windows 平台的僵尸网络扩展了 IoT 平台感染控制能力，这些恶意程序在感染、传播、攻击能力、隐蔽性等各方面都较之前的 Botnet 恶意程序有了较大的提升，具体详见第 6 章介绍。

5.2.3 各季度参与 DDoS 攻击的攻击源数量和类型统计

结合 5.1.1 和 5.1.3 节的分析结果，我们以 2017 年各季度攻击占比变化较明显的中型攻击为例，对其各季度参与攻击的攻击源进行分析。对比最明显的是 Q4 和 Q2 季度，Q4 季度攻击源数量相比 Q2 下降了 314%，主要是 Linux/Unix¹¹ 和 Window 类的攻击源下降比较明显。挖矿僵尸网络恶意程序通常会把目标锁定在 Window 或 Linux 类服务器或主机，如 Bondnet 挖矿僵尸主要锁定 Windows Server 主机¹²，因为这类设备的计算资源通常会高于一些小型家用设备，虽然也发现有少量挖矿 Botnet 使用物联网设备。在以比特币为代表的虚拟货币价格高涨时期，抽调这部分“优质”资源进行挖矿活动也正好符合黑产的趋利性。

图 5.12 中型规模 DDoS 攻击源数量及其类型



数据来源：绿盟科技威胁情报中心（NTI）

7 <https://www.exploit-db.com/exploits/40740/>

8 <http://toutiao.secjia.com/new-mirai-attack-germany-telecom>

9 <https://www.incapsula.com/blog/new-variant-mirai-embeds-talktalk-home-routers.htm>

10 https://motherboard.vice.com/en_us/article/nz7ky7/hackers-say-knocking-thousands-of-brits-offline-was-an-accident-mirai

11 这里主要指以 Linux/Unix 为系统的主机或服务器，不包含基于嵌入式 Linux 的物联网设备。

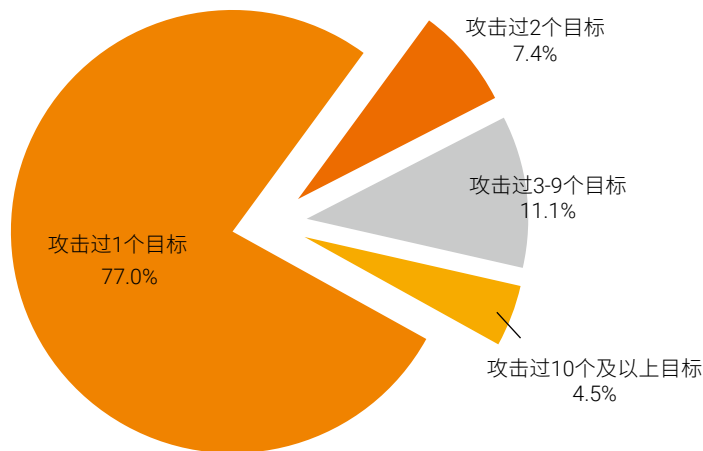
12 <http://safe.zol.com.cn/638/6388907.html>

5.2.4 DDoS 攻击源主机攻击广度及其 IP 信誉

2017 年参与 DDoS 攻击的攻击源中，有 23% 攻击过 2 个或以上目标。

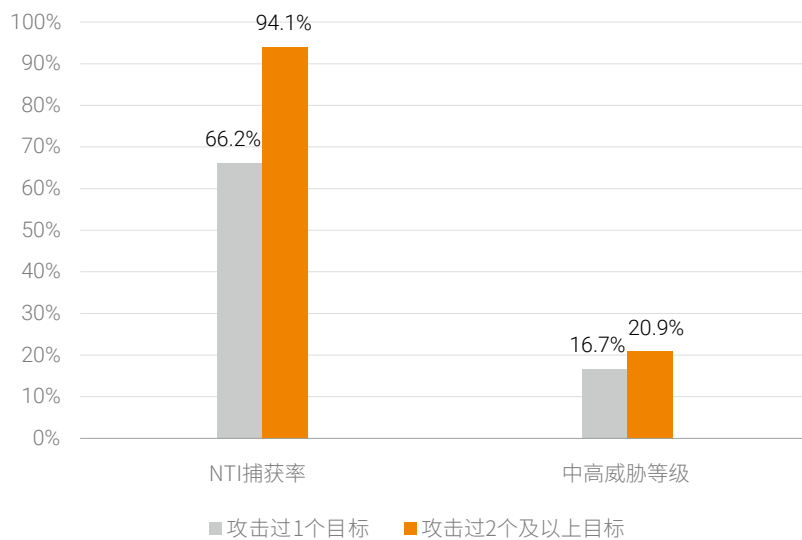
源 IP 攻击过的目标数量越多，代表这个 IP 活动越频繁，其威胁程度也就越高。攻击过 2 个目标或以上的源 IP 其在威胁情报中心的捕获率为 94.1%，这部分 IP 中有 20.9% 被标识为中、高等级威胁。我们在 7.6 节中，对参与过 Web 应用攻击的攻击源同样做了分析，与 DDoS 攻击源在捕获率和威胁等级上会存在差别，具体分析详见该节。

图 5.13 攻击源主机攻击目的 IP 数量占比



数据来源：绿盟科技威胁情报中心 (NTI)

图 5.14 DDoS 攻击源 IP 攻击过的目标数量与 IP 信誉情况



数据来源：绿盟科技威胁情报中心 (NTI)

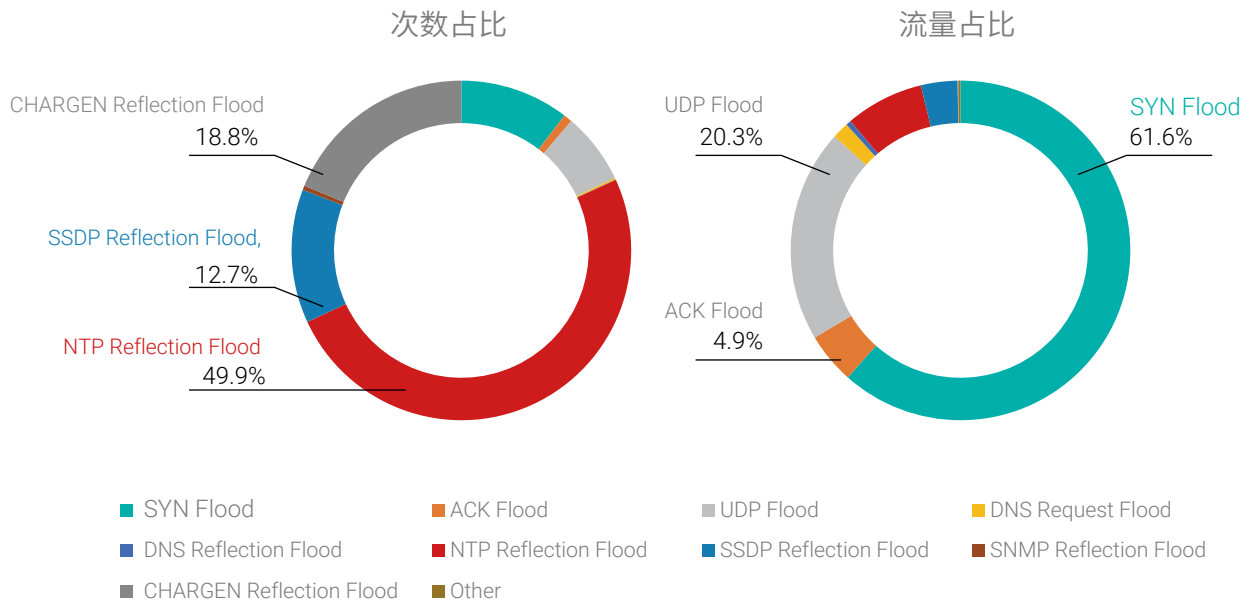
5.3 DDoS 攻击类型分析

5.3.1 各攻击类型次数和流量占比

2017 年，Top3（按攻击次数统计）DDoS 攻击类型均为反射类型攻击，仍然是 NTP Reflection Flood、SSDP Reflection Flood 和 CHARGEN Reflection Flood，占比合计 81.4%，与 2016 年几乎持平，略低于 2017 年上半年。这与我们 2016 年发布的 DDoS 态势报告中的观点相符，反射型 DDoS 攻击会存在较长时间。

从各类攻击流量大小占比来看，UDP Flood 占比继续下降，SYN Flood 攻击流量占比继续增长。SYN Flood 占比 61.6%，相比 2016 年上升 12.5 个百分点。主要原因是今年 SYN Flood 中、大规模攻击明显增多（见下节）。

图 5.15 按 DDoS 攻击总次数 / 总流量统计各类型占比图

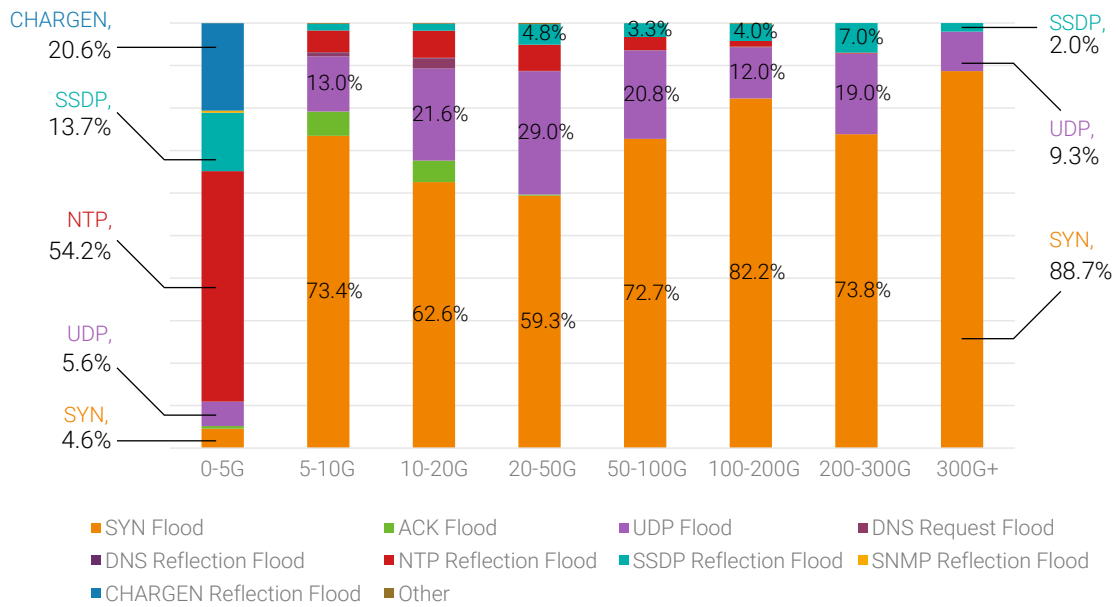


数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

5.3.2 攻击类型各流量区间分布

2017 年，DDoS 攻击呈现更加复杂的变化趋势。相比 2016 年，SYN Flood 攻击在各峰值区间的占比均在增长，尤其在中、大规模的 DDoS 攻击中，其占比翻了两翻。SYN Flood 攻击在近年出现的 1514 字节的 SYN 报文大包类型攻击，是其中、大规模 DDoS 攻击中占比增加的主要原因。

图 5.16 DDoS 攻击类型各流量区间分布图



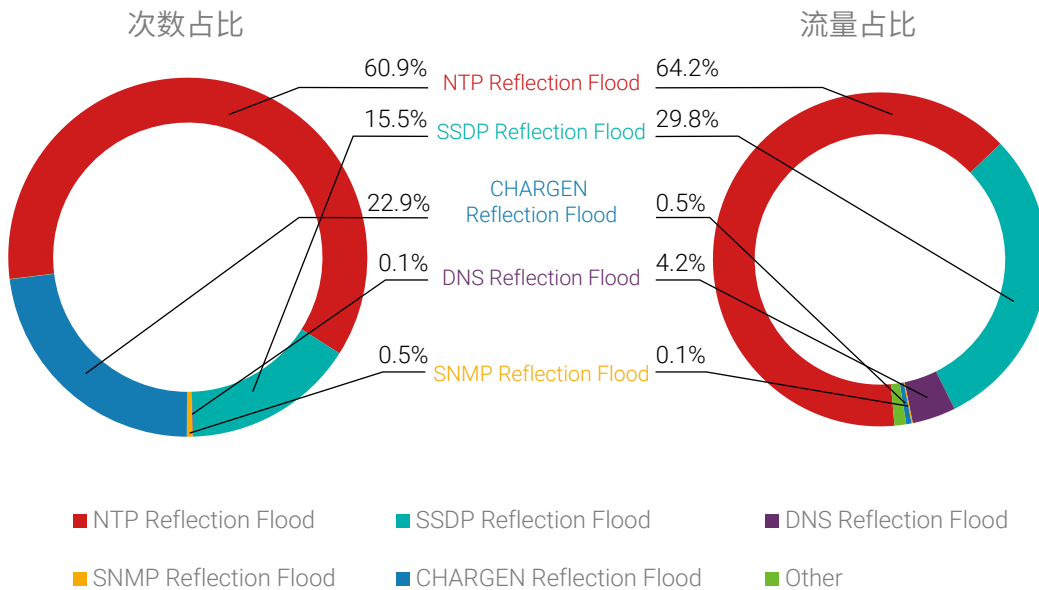
数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

5.4 反射攻击

5.4.1 以 NTP 为代表的传统类型反射攻击活动放缓

2017 年，反射放大攻击（DRDoS, Distributed Reflection Denial of Service）的攻击次数和总攻击流量占比如下图所示。无论是从攻击次数还是攻击总流量上来看，NTP Reflection Flood 均占首位，分别占全部反射攻击次数的 60.9% 和 64.2%。反射器的数量和反射器的放大比例，通常是攻击者在选择反射攻击类型的两个重要因素，由于网络存在大量公开 IP 地址的 NTP 服务器，且 NTP 反射攻击时的放大比达到 556.9，故导致了近几年 NTP 类型反射攻击的一直比较流行。

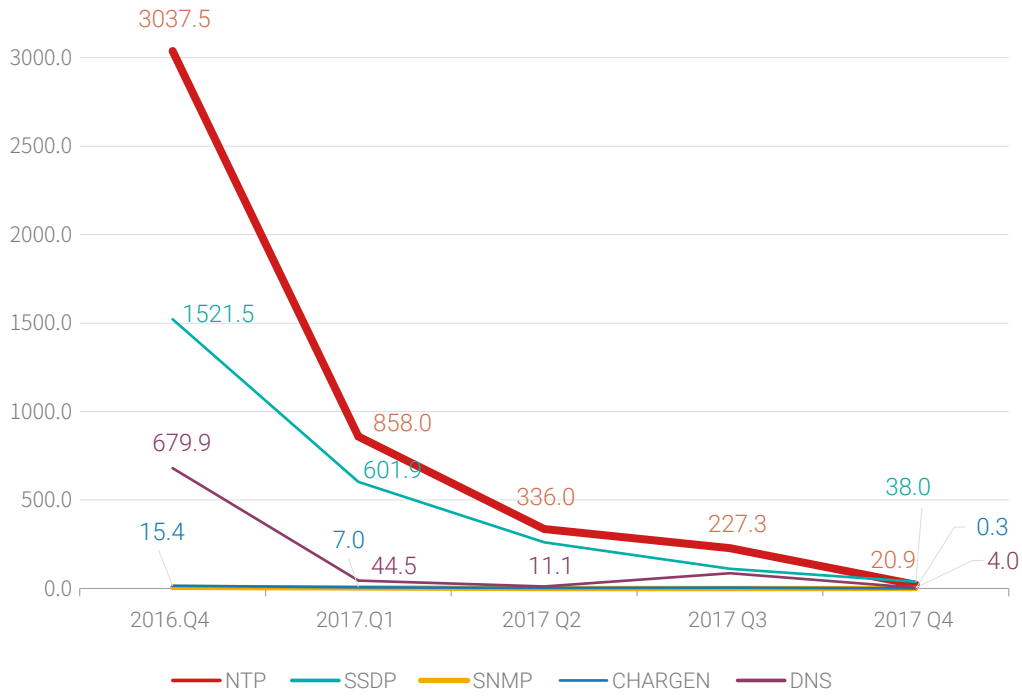
图 5.17 各类反射攻击攻击次数和流量占比



数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

但从各类反射攻击总流量、攻击规模（峰值）、参与反射攻击的活跃反射器来看，2017 年这些常见的反射类攻击趋势都在下降。2017 Q1 季度比 2016 Q4 反射攻击总流量减少 71%。

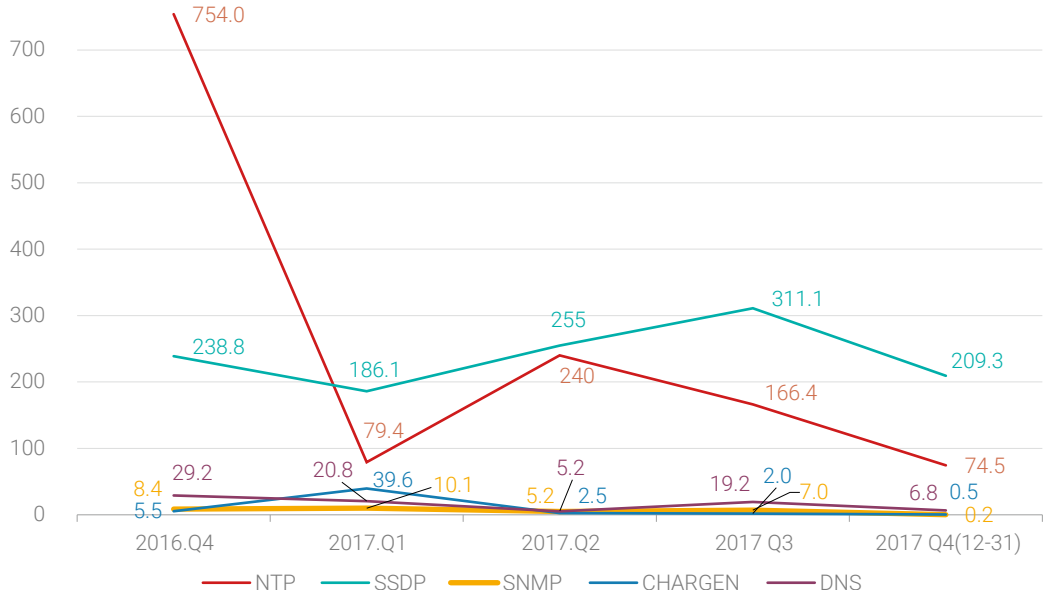
图 5.18 各季度反射攻击总流量趋势（单位：TBytes）



数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

2017 年常见的几类反射攻击的攻击规模（最高攻击峰值）均有下降趋势。虽在 2017 年 Q2 和 Q3 季度部分反射类攻击最高峰值略有增长，但到 2017 年 Q4 季度仍然低于 2016 年同期水平。

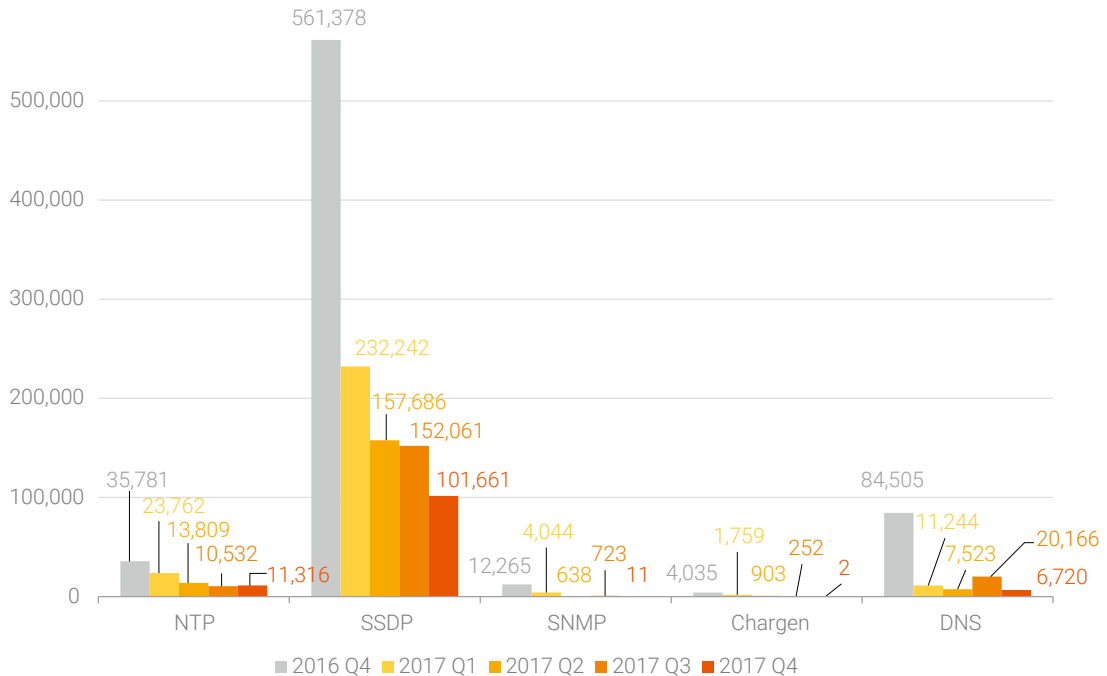
图 5.19 各类反射攻击各季度单次攻击最高峰值（单位:Gbps）



数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

2017 年常见的几类反射攻击活跃（参与攻击的）反射器数量均呈下降趋势。

图 5.20 各类反射攻击各季度活跃反射器数量（单位：个）



数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

这些常见类型的反射攻击流量的减少，攻击规模的降低，都与它们在全球范围内可用的反射器数量逐年减少有关。一方面，由于这些类型的反射攻击已经肆虐网络较长时间，无论是企业还是用户对其攻击的危害都已经有了比较清晰的认识，因此含有已知漏洞的很多服务器都已经被打了补丁或者升级到较新版本，又或者直接关闭了本不需要开启的服务。另一方面，攻击者也在不断寻求新的，攻击成本更低、效果更明显的攻击工具或手段。如：新型的、放大倍数更高的反射型攻击、物联网僵尸网络发起的攻击等。

5.4.2 新型 Memcached 反射攻击来势汹汹，1.35Tbps 峰值创新高

2017 年，我们的监控数据显示，几种常见的反射类型，如 NTP、SSDP、CHARGEN、DNS 攻击活动均有所放缓。但就在人们即将放松对反射攻击的警惕时，2018 年年初一种新型的反射攻击——Memcached 反射放大攻击，引发各方关注。2018 年 3 月 1 日 Akamai 宣称其客户遭到了峰值为 1.35Tbps 的 Memcached DRDoS 攻击¹³，而在这之前的几天，该类反射攻击的最大峰值也不过是 270Gbps¹⁴，500Gbps¹⁵。几日之隔，攻击峰值的历史纪录就迅速被翻倍刷新，攻击发生的频率也呈爆发式增长。绿盟科技在第一时间发布了关于 Memcached DRDoS 的预警¹⁶，同时中国电信云堤联合绿盟科技发布了对 Memcached DRDoS 的深入分析¹⁷。

Memcached 是一个高性能的开源分布式内存对象缓存系统，主要用于提高 Web 应用的扩展性，能够有效解决大数据缓存的很多问题，在全球范围内都有广泛使用。Memcached 基于内存的 key-value 存储小块数据，并使用该数据完成数据库调用、API 调用或页面渲染等。攻击者正是利用 key-value 这项功能构造了大流量的 Memcached 反射攻击。

13 <https://blogs.akamai.com/2018/03/memcached-fueled-13-tbps-attacks.html>

14 <https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/>

15 <https://www.arbornetworks.com/blog/asert/memcached-reflection-amplification-description-ddos-attack-mitigation-recommendations/>

16 <http://blog.nsfocus.net/memcached-ddos/>

17 <http://blog.nsfocus.net/memcached-drdos-analysis/>

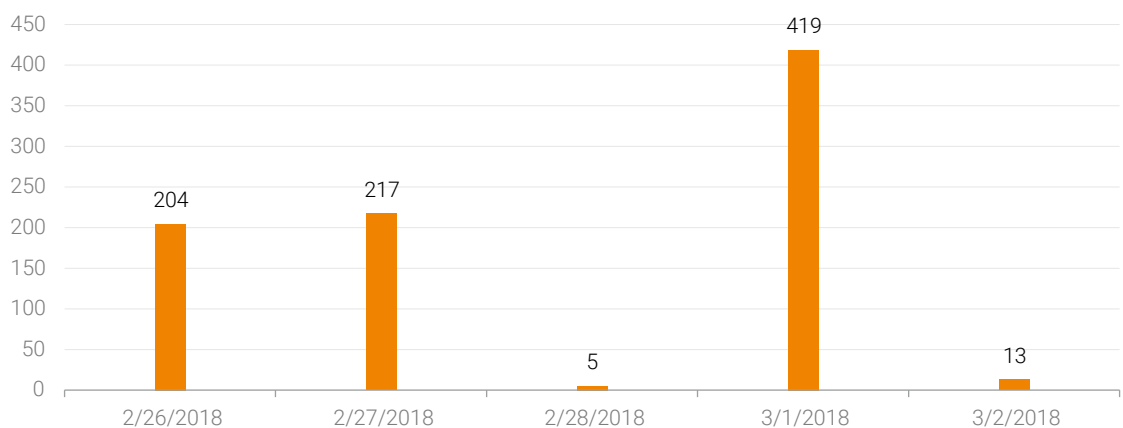
下表引自 US-Cert¹⁸，详细列举了各类反射攻击的放大倍数。US-Cert 提供的数据显示它能够实现 51,000 倍的放大效果，仅从放大倍数来看，Memcached 反射攻击的危害程度远远高于其他反射攻击类型。

表 1 各类反射攻击放大倍数

反射攻击针对的协议	带宽放大倍数
DNS	28 to 54
NTP	556.9
SNMPv2	6.3
NetBIOS	3.8
SSDP	30.8
CharGEN	358.8
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake Network Protocol	63.9
Steam Protocol	5.5
Multicast DNS (mDNS)	2 to 10
RIPv1	131.24
Portmap (RPCbind)	7 to 28
LDAP	46 to 55
CLDAP	56 to 70
TFTP	60
Memcache	10,000 to 51,000

根据中国电信云堤的攻击监控数据显示，从本周一至周五（2月26日至3月2日 06:00）短短5天内，全球就发生了79起利用 Memcached 协议的反射放大攻击。日攻击总流量最高达到 419TBytes。

图 5.21 Memcached 反射放大攻击日攻击总流量（单位：TBytes）

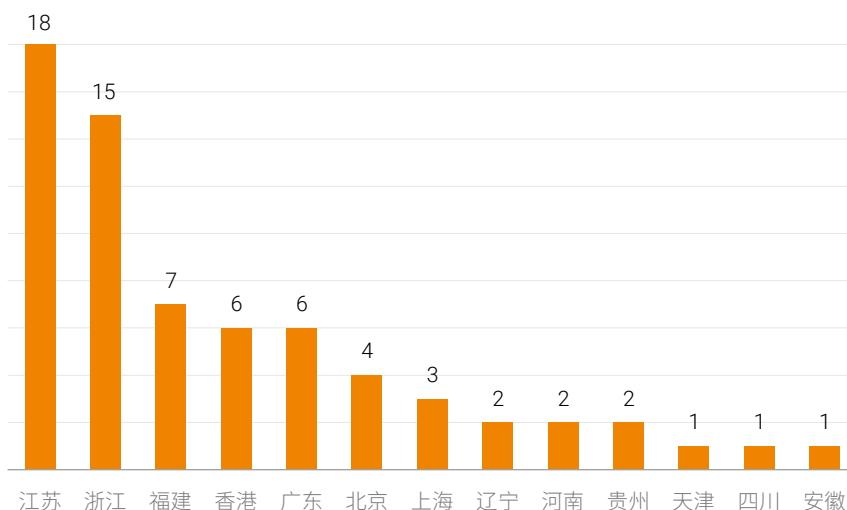


数据来源：中国电信云堤

18 <https://www.us-cert.gov/ncas/alerts/TA14-017A>

其中，针对我国境内的 Memcached 反射放大攻击就有 68 次，江苏、浙江两省被攻击频繁。针对我国境内的攻击，单次攻击最高攻击峰值达 505Gbps。攻击持续时间最长的一次发生在 3 月 1 日，持续 1.2 小时，总攻击流量达 103.8TBytes。

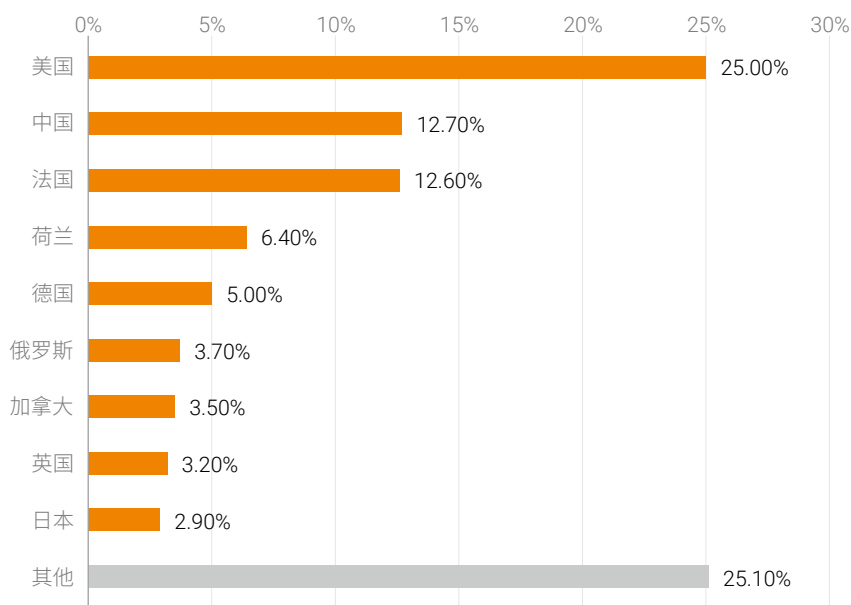
图 5.22 中国各省份地区 Memcached 反射放大攻击次数



数据来源：中国电信云堤

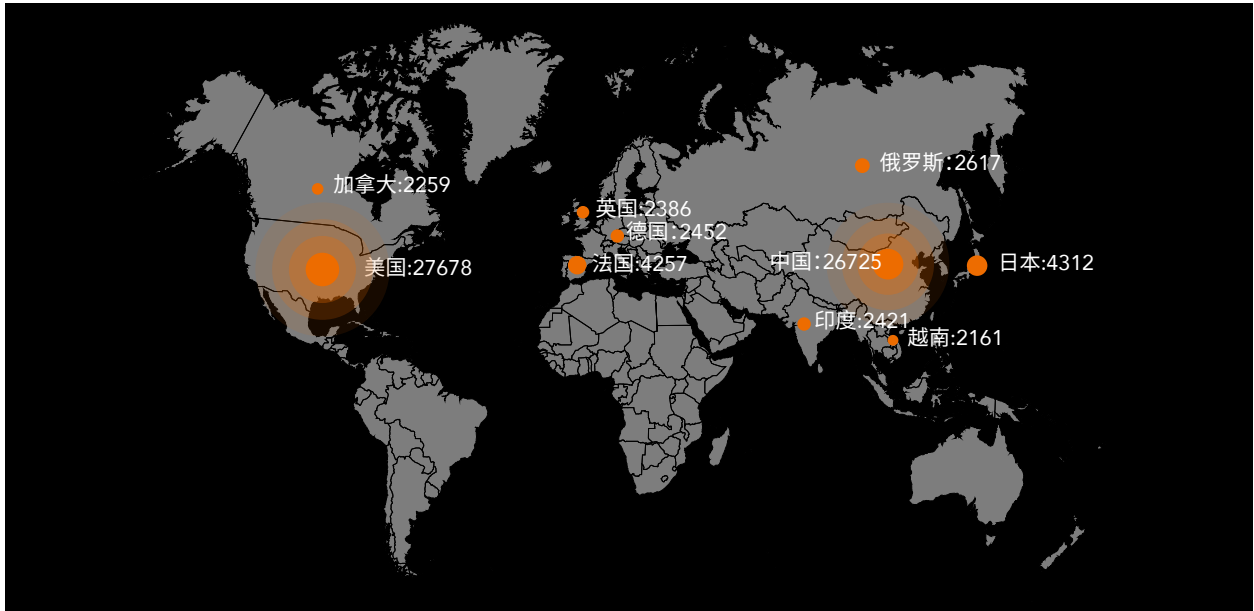
溯源分析的结果显示，全球总共有 3790 个 Memcached 服务器被利用参与到这些 Memcached 反射放大攻击。这些被利用反射源遍布于全球 96 个国家或地区范围内。其中，美国就占了全球的 1/4。分布在中国地区的被利用的 Memcached 服务器位列第二位，占比 12.7%。在中国各省份占比如下所示，广东、北京、浙江为 TOP3。

图 5.23 Memcached 反射攻击源全球各国家分布占比



数据来源：中国电信云堤

绿盟科技威胁情报中心（NSFOCUS Network Threat Intelligence，简称 NTI）的统计结果显示，全球范围内存在被利用风险的 Memcached 服务器达 104,506 台。从地理分布来看，美国可被利用的 Memcached 服务器最多，其次是中国。



数据来源：绿盟科技威胁情报中心（NTI）

大量的可利用的 Memcached 反射器为构造超级 DRDoS 攻击提供了有力的先决条件。如果不及时修复治理，预计基于 Memcached 反射攻击的攻击事件会继续增加，后果不敢想象。

从攻击影响范围来看，所有互联网的业务都可能成为 Memcached DRDoS 的攻击对象。一方面带宽或业务遭受超大流量的攻击，导致出口带宽完全被占满，正常业务无法访问；另一方面企业内部的 Memcached 系统可能被不法分子利用成为攻击帮凶。我们呼吁各地区、各行业客户保持高度警惕，谨防 Memcached 反射攻击对服务器造成直接冲击或利用 Memcached 反射攻击作为障眼法混合其他攻击造成信息安全危害。关于 Memcached DRDoS 的具体的防护和加固建议请详见《深度剖析 Memcached 超大型 DRDoS 攻击》¹⁹。

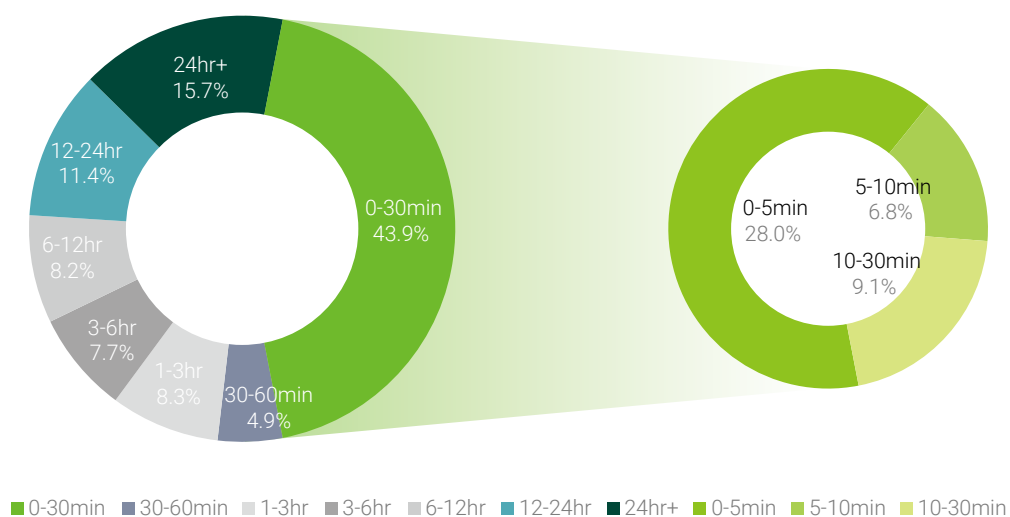
19 <http://blog.nsfocus.net/memcached-drdos-analysis/>

5.5 DDoS 攻击持续时间

5.5.1 DDoS 攻击持续时间占比

2017 全年，持续超过一天的长时攻击增多，半小时以内的短时攻击略有下降，但仍然占主导地位。攻击时长在 30 分钟以内的 DDoS 攻击占全部攻击的近一半，占 43.9%，相比 2016 年下降 7.5 个百分点；攻击时长超过 24 小时的长时间持续攻击呈增长趋势，总体占比 15.7%，相比 2016 年增长 5 个百分点。随着 DDoS 攻击的服务化、产业化，再加上全球大量的物联网设备被攻陷并沦为僵尸主机，使得发起一次 DDoS 攻击的成本大幅降低，这样黑产可以在同样的成本下发起规模更大、更持久的攻击，从而促进了长时攻击的增多。

图 5.24 攻击持续时间占比图



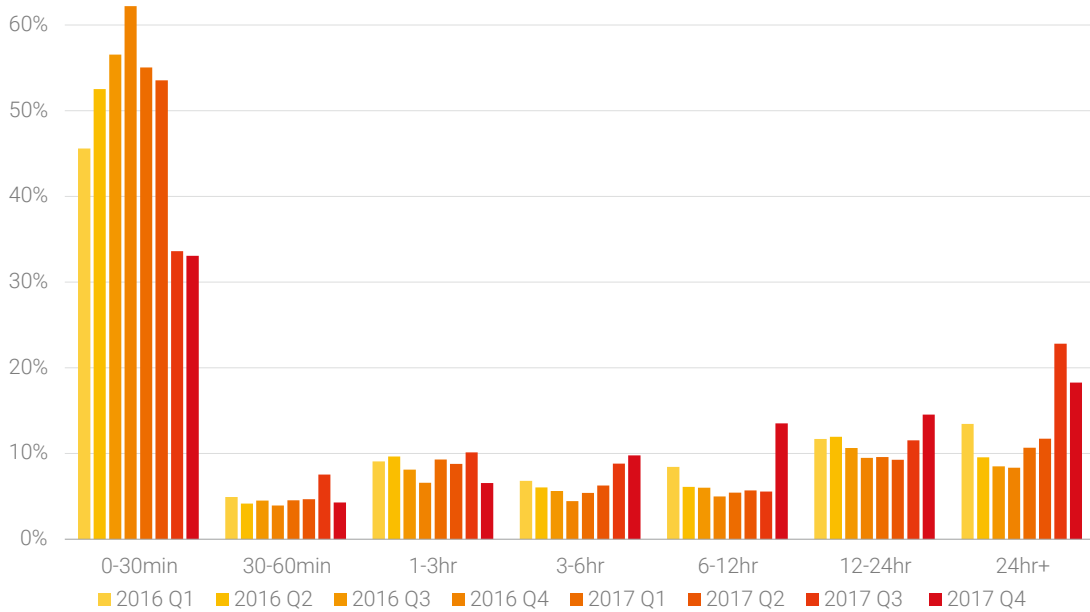
数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

5.5.2 DDoS 攻击持续时间变化趋势

2017 年持续三小时以上的攻击占比呈增长趋势。

我们对攻击持续时间跟踪了较长时间，2017 年 Q3 和 Q4 季度，30 分钟以内攻击从 Q2 季度的占一半以上降低到只占三成，三小时以上攻击自 2017 年 Q1 季度开始持续每季度都在增长。

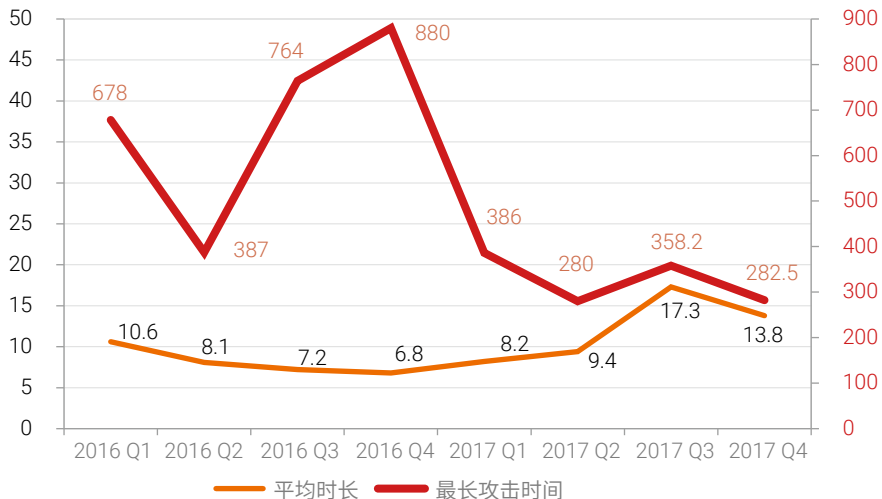
图 5.25 各季度攻击持续时间占比图



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

2017 年平均攻击时长为 12 小时，相比 2016 年平均攻击时长增长约 1/3。2017 年全年各季度最长攻击时长相比 2016 年呈下降趋势。2017 年我们监控到的最长一次 DDoS 攻击持续了 16 天 2 小时 (386 小时)。

图 5.26 各季度平均攻击时长和最长攻击时长 (单位:小时)

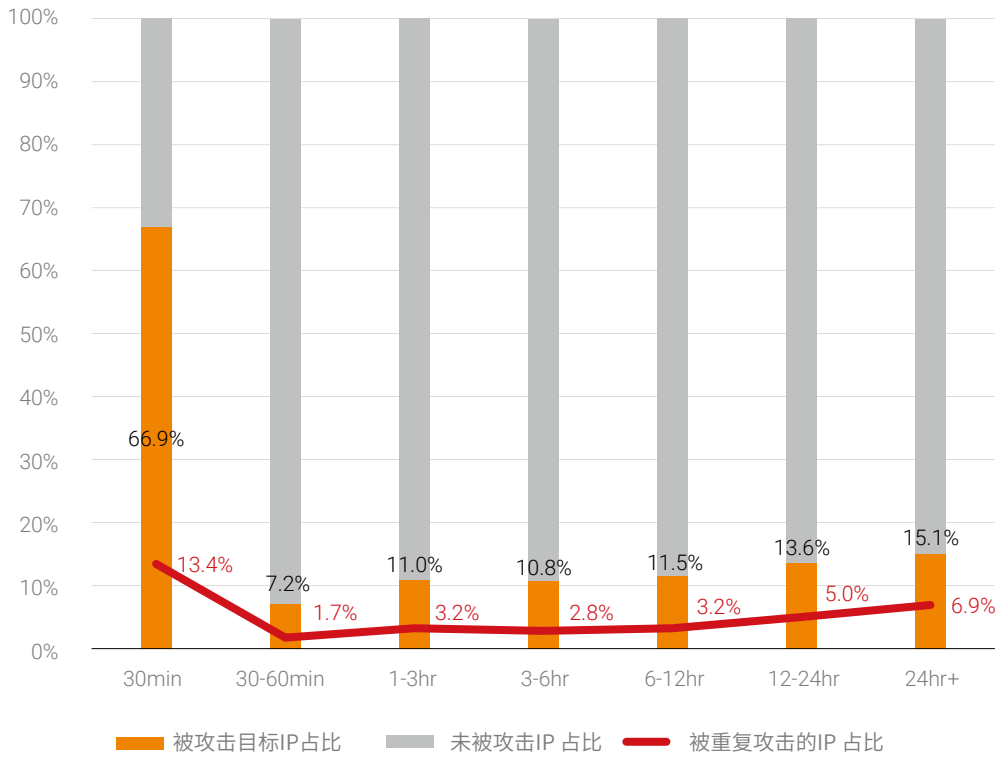


数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

5.5.3 被攻击频次与攻击时长

30 分钟以内的短时攻击中目标 IP 被攻击且被重复攻击的概率最大。

图 5.27 不同攻击持续时间与攻击频次



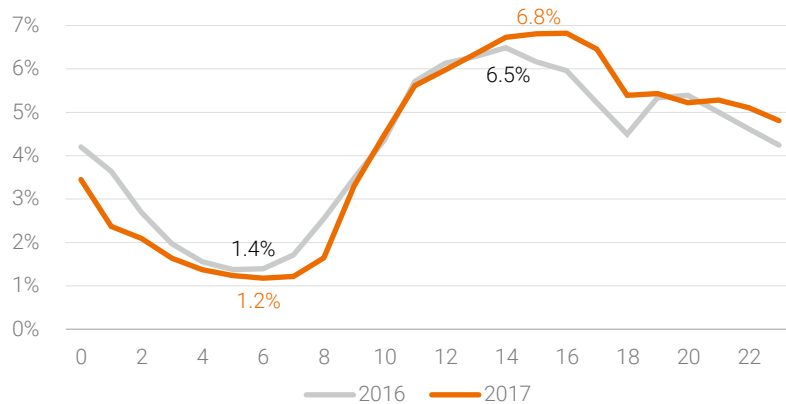
数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

5.6 DDoS 攻击时间画像

5.6.1 一天 24 小时 DDoS 攻击活动分布

从一天 24 小时来看攻击占比，2017 年与 2016 年变化不大。2017 年工作及娱乐时间（10 点 -22 点）攻击占比呈上升趋势，对应的睡眠休息时间攻击占比呈下降趋势。2017 年在线业务的客户访问量，也是工作及娱乐时间上升、睡眠休息时间下降，攻击者通常也是利用该规律，当在线业务访问量最大时，发起 DDoS 攻击，以此来提升的攻击的效果和影响。2017 年业务高峰时段（10 点 -22 点）发生的 DDoS 攻击占全天的 75.7%。

图 5.28 2017 vs 2016 一天 24 小时 DDoS 攻击占比

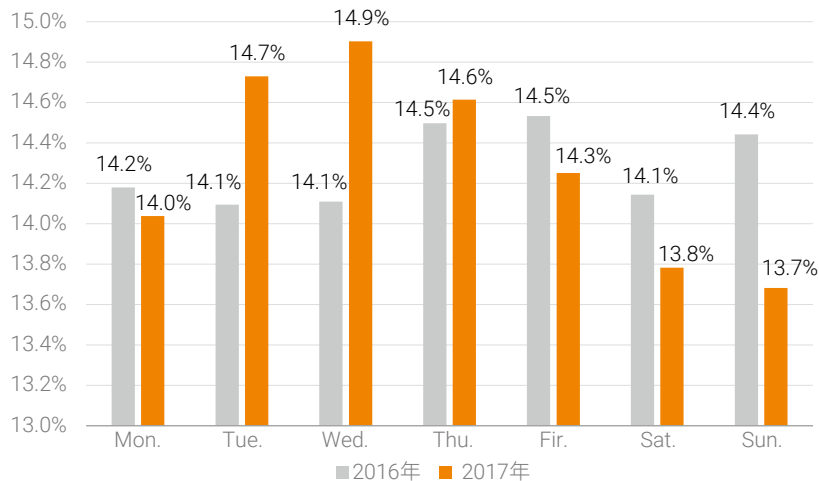


数据来源：中国电信云堤

5.6.2 一周 7 天 DDoS 攻击活动分布

一周七天攻击次数占比来看，对比 2016，2017 年工作日攻击次数占比升高，周末攻击次数占比降低。总体体现为 DDoS 攻击在工作日更频发。

图 5.29 2017 vs 2016 年每周七天 DDoS 攻击次数占比



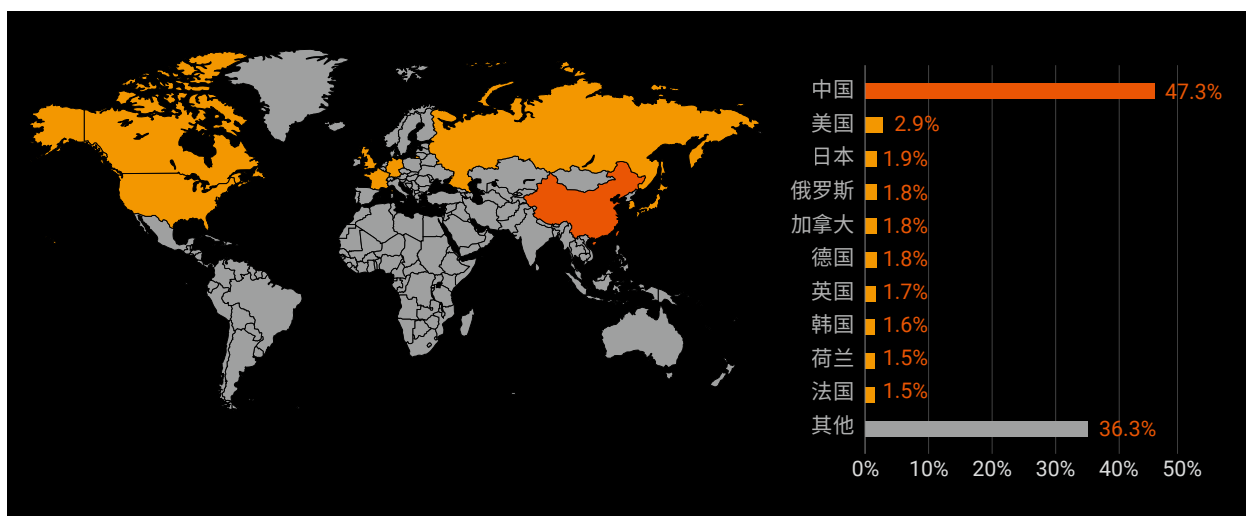
数据来源：中国电信云堤

5.7 DDoS 攻击地域分布

5.7.1 DDoS 攻击源地域分布

经我们的统计，2017年中国依然是DDoS受控攻击源最多的国家，占比为47.3%，约为全球的一半受控攻击源；美日俄加德等每个国家均约为2%左右，其余的受控攻击源则在发达国家的分布相对平均。

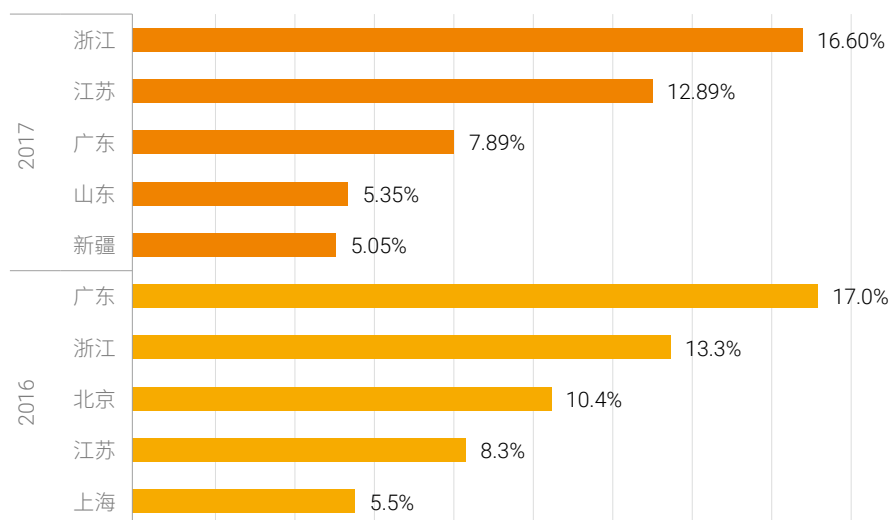
图 5.30 攻击源国家排名 TOP10



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

2017年国内发起DDoS攻击的省份主要分布在沿海和西北地区，发起DDoS发起攻击次数的Top 5省份依次为浙江、江苏、广东、山东和新疆，合计占比达47.88%。山东、新疆首次列入国内TOP5。

图 5.31 2017 vs 2016 攻击源国家 TOP5

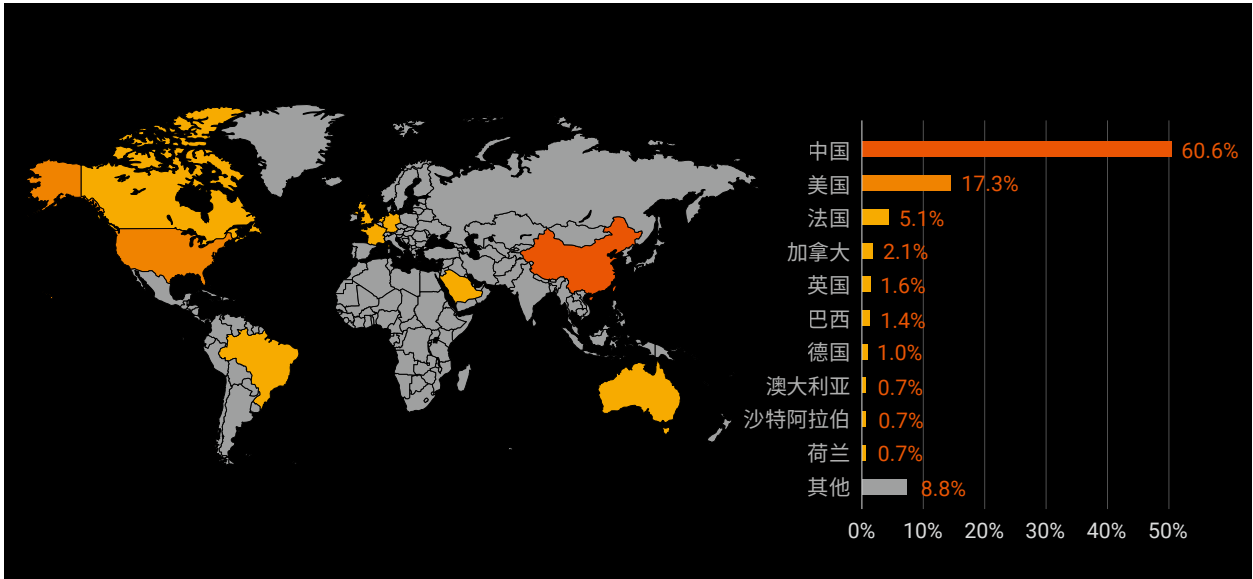


数据来源：中国电信云堤

5.7.2 DDoS 被攻击目标地域分布

2017 年，受攻击最严重的国家是中国，攻击占全部被攻击国家的 60.6%，其次是美国和法国，三者占据全球被攻击国家总和的 83.0%。相比 2016 年，中美法三国总和占全部被攻击国家下降 10.8%。

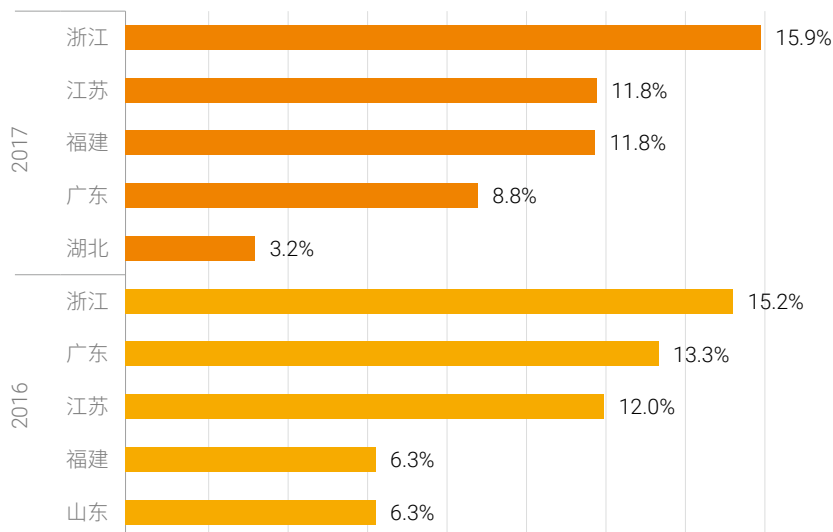
图 5.32 攻击目标国家排名 TOP10



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

我国中东部沿海地区一直是被 DDoS 攻击的高发地，浙江、江苏、福建、广东等地全年遭受攻击占全国总攻击数量的 51.5%。浙江省依然为今年遭受攻击最多的省份，福建排入 TOP3。

图 5.33 2017 vs 2016 攻击目标国家 TOP5



数据来源：中国电信云堤



6. 物联网僵尸网络发展趋势

物联网僵尸网络从传播、感染到攻击能力不断升级，感染目标平台不断扩张，其威胁将进一步扩大

6.1 物联网僵尸网络发展趋势	33
6.2 热点 IoT Botnet 对比分析	38

6.1 物联网僵尸网络发展趋势

6.1.1 感染方式升级：从弱口令破解到 0day 漏洞利用

过去的 2016 年是物联网僵尸网络大爆发的一年，出现的以 Mirai 为代表的物联网僵尸网络多半采用 Telnet 和 SSH 弱口令破解的方式感染物联网设备。2016 年 11 月 Mirai 变种利用 TR-064 路由器安全漏洞攻击大量的家用路由器，德国电信 Telekom 约 90 万客户断网，英国 Kcom 公司、英国 TalkTalk 公司（36 万客户）²⁰、英国 Post Office Broadband（10 万客户）以及爱尔兰电信 Eir 等都陆续受到影响²¹。

2017 年出现了更多基于物联网僵尸网络的变种，它们大多集成了更加复杂的漏洞扫描和利用能力，甚至有些会利用 0-day 漏洞对物联网设备进行感染。黑产对恶意 botnet 的维护更新漏洞速度之快让人震惊。

如：

IoTroop^{22 23} 目前已知利用的漏洞数量达到 15 个以上，涉及到 GoAhead、D-link、TP-link、Netgear、AVtech、MikroTik、Linksys、Synology 等多个产品。其中涉及到 GoAhead 漏洞就 5 个，分别为 CVE-2017-8225/ CVE-2017-8224/ CVE-2017-8223/ CVE-2017-8222/ CVE-2017-8221。

Okiru/Satori²⁴ 就利用了国内某品牌无线路由器类设备存在的 0-day 漏洞（CVE-2017-17215），远程攻击者可通过向设备 37215 端口发送恶意报文利用漏洞执行任意代码。除此之外，还使用了 Realtek SDK miniigd SOAP 服务远程代码执行漏洞 CVE-2014-8361，Realtek SDK 是瑞昱（Realtek）公司的一套 SDK 开发包，Realtek SDK 的 miniigd SOAP 服务中存在安全漏洞，远程攻击者可通过发送特制的 NewInternalClient 请求利用该漏洞执行任意代码。主要受影响的品牌为 D-link 的多个型号 Dri 系列的家用路由器。

Persirai²⁵ 和 Gafgyt²⁶ 利用漏洞感染 IoT 设备的同时，也保留了最初的 Telnet/SSH 弱口令爆破的功能。比如，Gafgyt²⁷ 最初发现是使用 Telnet/SSH 弱口令扫描爆破获取 IoT 设备，后面的版本就发现开始集成了磊科 Netcore 路由器的漏洞扫描和利用模块。

6.1.2 感染平台进一步扩张：具备跨平台传播能力

1. 传统基于 Windows、Linux 平台的 Botnet 恶意程序开始把目标瞄准了物联网设备

开源 Mirai 导致物联网僵尸网络变种快速增加，传统的基于 Windows 平台的僵尸网络家族看到 IoT 的数量、规模和攻击威力后，快速向 IoT 平台演进²⁸。Jenki、台风等僵尸家族就是典型代表。目前 Jenki 家族的被控木马已经横跨 Windows、Linux、IoT 三大领域。

20 <https://www.incapsula.com/blog/new-variant-mirai-embeds-talktalk-home-routers.html>

21 https://motherboard.vice.com/en_us/article/nz7ky7/hackers-say-knocking-thousands-of-brits-offline-was-an-accident-mirai

22 <https://research.checkpoint.com/new-iot-botnet-storm-coming/>

23 <http://blog.netlab.360.com/iot-reaper-a-quick-summary-of-a-rapid-spreading-new-iot-botnet/>

24 <http://www.freebuf.com/articles/paper/158464.html>

25 <https://www.incapsula.com/blog/from-mirai-to-persirai.html>

<http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/>

26 <http://toutiao.secjia.com/gafgyt-iot-malware>

27 <http://www.freebuf.com/articles/terminal/148668.html>

28 <https://mp.weixin.qq.com/s/SFYHBaju-CkNTpoViValbg>









2. 利用 window 木马实现跨平台传播的能力

基于 Mirai 的变种 BKDR_MIRAI.A²⁹，使用 windows 木马在 windows 平台和 IoT 平台进行传播和感染。如果发现是基于 Linux 的系统，就会放置基于 IoT 的 Mirai 恶意程序，如果发现是 windows 系统，就会放置 Windows 木马程序，并负责继续扫描要感染的目标。该木马还可以识别主机软件，如数据库系统 MS SQL 或者 MySQL，它会创建一个 admin 权限的新账户，可以执行数据库任意操作。

该变种是否与 Mirai.Nov³⁰ 有联系尚不确定。Mirai.Nov 最初通过基于 Windows 平台的 Dofloo 僵尸网络投放样本的³¹。

3. 兼容更多物联网平台

Mirai.Nov 样本中发现，其被控端木马已经兼容 armv5l、armv6l、i586、i686、mipsel、mips、x86_64、powerpc 8 个类型的系统架构，囊括大部分的 IoT 系统架构，这也为后期的大批量拓展僵尸网络奠定架构兼容基础。

 mirai.mipsel-v1-1031	2017/11/3 11:15	MIPSEL-V1-1031...	43 KB
 mirai.x86_64-v1-1031	2017/11/3 11:14	X86_64-V1-1031...	34 KB
 mirai.i686-v1-1031	2017/11/3 11:14	I686-V1-1031 文件	29 KB
 mirai.i586-v1-1031	2017/11/3 11:12	I586-V1-1031 文件	28 KB
 mirai.armv6l-v1-1031	2017/11/3 11:09	ARMV6L-V1-103...	53 KB
 mirai.armv5l-v1-1031	2017/11/3 11:08	ARMV5L-V1-103...	30 KB
 mirai.powerpc-v1-1031	2017/11/3 11:07	POWERPC-V1-1...	31 KB
 mirai.mips-v1-1031	2017/11/3 11:07	MIPS-V1-1031 ...	43 KB

Amnesia³² 支持 10 种物联网平台

- armv4l
- armv5l
- i386
- m68k
- MIPS
- MIPSEL
- PowerPC-440fp
- SPARC
- x86_64

29 <http://blog.trendmicro.com/trendlabs-security-intelligence/mirai-widens-distribution-new-trojan-scans-ports/>

30 <http://www.freebuf.com/articles/web/153689.html>

31 <http://www.freebuf.com/articles/paper/159800.html>

32 <http://get.cyberx-labs.com/radiation-report>

6.1.3 隐蔽性增强：使用更隐蔽的扫描方式和沙箱技术

1. 扫描方式更加隐蔽

1) BKDR_MIRAI.A³³ 将原来集成于 Bot 上的扫描破解模块分离出来，利用 windows 木马多种方式的进行 Bot 感染³⁴，如包含包含 SQL 盲注、暴力破解 (SSH/Telnet) 等。

2) Mira.Nov³⁵ 同样将 scan 模块单独分离出来。bot 模块主要功能简化为 DDoS 攻击和 C2 交互通讯。这样做的目的可以降低 Bot 代码因 Telnet/ssh 弱口令破解以及漏洞扫描时被发现的几率，方便僵尸网络进行长期潜伏，还可快速复用潜在 Bot，但由于缺少 Bot 集群的扫描能力，僵尸网络的拓展速度相对也会受到影响。

3) IoTroop^{36 37} 会主动抑制扫描速度，以降低被检测和发现的风险。

2. 使用传统的虚拟技术逃避沙箱检测

研究人员发现基于 IoT/Linux 的 Amnesia/Tsunami 使用了 Virtual machine 逃避技术³⁸。Virtual machine 逃避技术常用域基于 Windows 和 Android 系统的恶意软件，用于躲避沙箱的检查和析。Amnesia 恶意软件会试图判断其是否运行在沙箱上，如检测是否是 VMware 或基于虚拟设备的 QEMU 环境，如果检测到运行于此类环境，恶意软件会删除这个机器上的所有文件。

6.1.4 攻击武器库不断升级：集成反射攻击能力

基于 IoT/Linux 的恶意僵尸网络程序不仅具备应用层攻击的能力，还集成了反射攻击的能力。据分析，IoT_Reaper 集成了约 100 个 DNS 开放服务器，具备发起 DNS 反射攻击的能力。据估计单个 C2 已经感染 2 万太，大概有 200 万待感染设备。Gafgyt 同样具备 UDP Amplification 反射攻击的能力³⁹。

这些 IoT/Linux 设备本身数量巨大，一旦集成一定数量的可用的反射器，那么此类 DDoS 反射攻击的威力将远远超出传统的反射攻击。攻击的成本也会大大降低。除了 Botnet 控制设备的数量，攻击的规模还与反射器可用数量和具体反射器类型直接相关，例如 NTP 可放大倍数最大，SSDP 可用反射器最多。

6.1.5 黑产继续加紧争夺 IoT Botnet 资源

1. 传统的 Botnet，也在扩展 IoT 感染能力

一些传统 Windows、Linux 平台的 Botnet 扩展 IoT 感染能力，加紧在争夺 IoT 设备资源。有资料表明⁴⁰，24% 的 Mirai botnet 的主机与 Gafgy 或 Bashlite 的攻击利用的 IP 重合。这么高的重复率表明：不同恶意软件家族瞄准了相同的漏洞百出的 IoT 设备。

2. 某些 botnet 为了防止同类恶意软件的感染对物联网设备本身进行“加固”

很多恶意软件在感染 IoT 设备后，就会有目的的封掉一些端口，这些端口通常是其他恶意软件对 IoT 设备进行感染常用的端口，主要目的是防止同类恶意软件利用这些端口再次感染，导致失掉对该设备的控制。比如，

33 <http://blog.trendmicro.com/trendlabs-security-intelligence/mirai-widens-distribution-new-trojan-scans-ports/>

34 <https://securelist.com/newish-mirai-spreader-poses-new-risks/77621/>

35 <http://www.freebuf.com/articles/web/153689.html>

36 <https://research.checkpoint.com/new-iot-botnet-storm-coming/>

37 <http://blog.netlab.360.com/iot-reaper-a-quick-summary-of-a-rapid-spreading-new-iot-botnet/>

38 <https://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/>

39 <http://toutiao.secjia.com/gafgyt-iot-malware>

40 <https://mp.weixin.qq.com/s/SFYHBaju-CkNTpoViValbg>

声称是为了保护物联网设备安全的恶意软件 Hajime 它在感染设备后，会关闭 23，7547，5555 和 5358 这些端口⁴¹。

```

int iptables_1A5F4()
{
    int v0; // r5@1
    int v2; // [sp+0h] [bp-5Ch]@2
    int v3; // [sp+40h] [bp-1Ch]@1
    signed int v4; // [sp+44h] [bp-18h]@1
    signed int v5; // [sp+48h] [bp-14h]@1
    signed int v6; // [sp+4Ch] [bp-10h]@1

    v3 = 23;
    v4 = 7547;
    v5 = 5555;
    v6 = 5358;
    v0 = 0;
    do
    {
        sub_1F0A0(
            (int)&v2,
            64,
            (int)"iptables -A INPUT -p tcp --destination-port %d -j DROP",
            *(int *)((char *)&v3 + v0 * 4));
        ++v0;
        sub_23CFC(&v2);
    }
    while ( v0 != 4 );
    sub_23CFC("iptables -D INPUT -j CWMP_CR");
    return sub_23CFC("iptables -X CWMP_CR");
}

```

BEDE5CCB	00	B0	AF	02	00	7B	1D	00	00	69	70	74	61	62	6C	65{...iptable
BEDE5CDB	73	20	2D	41	20	49	4E	50	55	54	20	2D	70	20	74	63	s -A INPUT -p tc
BEDE5CEB	70	20	2D	2D	64	65	73	74	69	6E	61	74	69	6F	6E	2D	p --destination-
BEDE5CFB	70	6F	72	74	20	37	35	34	37	20	2D	6A	20	44	52	4F	port 7547 -j DRO
BEDE5D0B	50	00	00	00	00	00	00	00	00	17	00	00	00	7B	1D	00	P.....{..
0123DFFF	01																.

同样，类似 hajime，声称自己是正义行为的 BrickerBot⁴²，会通过重写 Flash 存储对 IoT 设备进行加固，防止其他恶意软件的感染。BrickerBot 的作者宣布自从 2016 11 月份开始的“Internet Chemotherapy”计划，BrickerBot 已经“加固”了 1000 万个物联网设备。

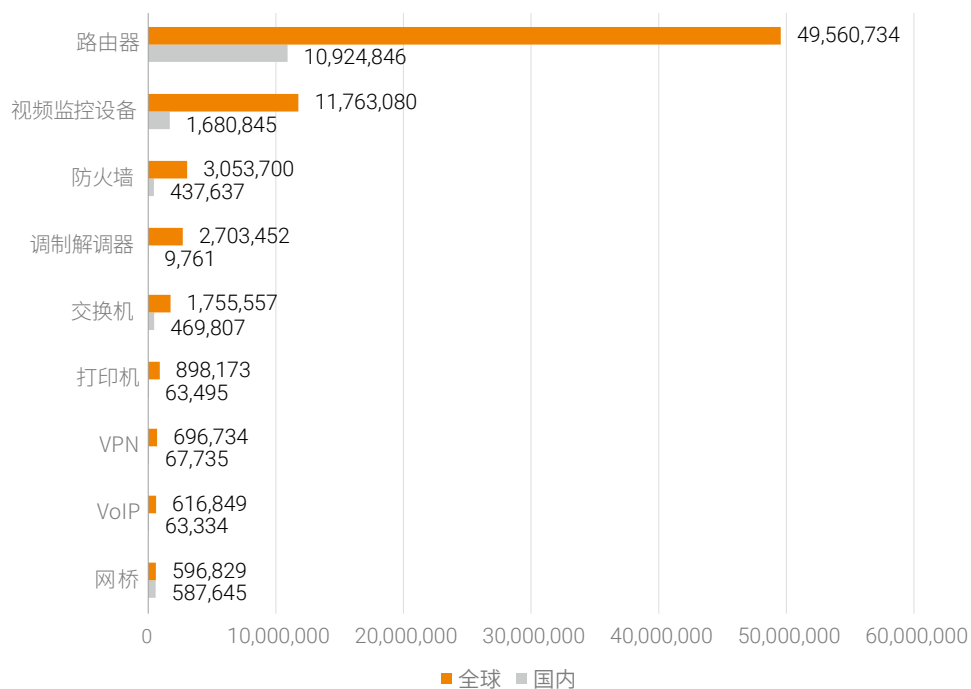
41 <http://zhishi.secjia.com/pdf/770583325.pdf>

42 <https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/>

6.1.6 来自物联网设备的威胁将继续扩大

在物联网的体系架构中，物联网终端设备和传统数通设备，均为不可或缺的部分，其两类设备中的安全现状和趋势，势必将成为物联网能否稳健、可持续性发展的关键因素；物联网的安全事件中，通常都是通过全网扫描获取暴露的设备 IP 地址及端口信息，然后进一步实施针对性的入侵和控制；所以暴露在物联网中的设备数量类型及分布，已经成为物联网安全潜在风险的一个重要指标。

图 6.1 全球及国内物联网相关设备暴露情况（单位：台）



数据来源：《2017 物联网安全研究报告》

通过数据收集和分析，我们在图 6.1 中，列出了若干暴露情况较为严重的物联网设备及具体分布。

从全球分布来看，传统数通设备由于其在网络实际部署的基数较大，其暴露的数量也远高于物联网终端设备，其中最常见的路由器、防护墙台数分别达到了 4956 万和 305 万台，分列暴露数排名的第一位和第三位；随着视频监控设备在物联网中大规模应用，其暴露的数量排名第二，达到了 1176 万台。

从国内分布来看，路由器、视频监控系统设备和防火墙分别占据了暴露台数排名的前三位，分别达到了 1092 万、168 万和 43 万台。

路由器作为网络基础设施中最常见的设备，其设备中暗藏的安全问题不容忽视；由于运营商网络中部署的路由器，对其部署和配置都有明文要求，不能在网络中暴露，目前在网络中暴露主体以家庭路由器为主。

假设国内暴露在网络中的家用路由器被感染的概率为 1%，那么国内将有约 11 万的家用路由器存在成为僵尸网络的风险，通常情况家用路由器的上行带宽为 12.5Mbps，则最大可能输出 1.3Tbps 的 DDoS 攻击流量。

在物联网终端设备中，网络摄像头是日常中接触最多的设备，由于其价格便宜和部署简单，已经在物联网中大规模部署，目前 http81 和 IoT_reaper 新型僵尸网络均是以摄像头为主要攻击对象。

假设国内暴露在网络中的摄像头被感染的概率为 1%，那么国内将有约 1.68 万台视频监控设备存在成为僵尸网络的风险，以采用 1080P 的视频格式各地方监控所需的网络上行带宽至少为 40 Mbps，则最大可能输出的攻击流量 672Gbps。

按照当前物联网设备令人堪忧的安全状况和修复情况看，暴露在网络中的这些设备被感染的概率要远高于 1%，这些资源一旦掌握在不法分子手中，威胁将不可估量。

6.2 热点 IoT Botnet 对比分析

6.2.1 热点 IoT Botnet 概述

Mirai 作为近些年最耳熟能详的僵尸网络，其巅峰时期，其控制的存在漏洞的 IoT 设备一度达到了惊人的 60 万台的规模；不法分子通过僵尸网络获取利益的通常为提供 DDoS 攻击租售服务或者对目标服务进行敲诈等方式，随着 2017 年的比特币的涨幅达到 1600%，我们看到，僵尸网络成为了比特币的重要挖矿资源，这也是更多新型僵尸网络在 2017 年发展迅速的主要原因；

本节将对 2017 年的新型的僵尸网络进行汇总，并从寄宿平台、传播手法和潜在威胁等方面进行详细的对比解析。

6.2.2 寄宿平台对比分析

通过对比 2017 年的 7 种新型僵尸网络，其感染设备已经由最初的网络摄像头，扩充为家庭路由器、机顶盒等常用家用设备，Hajime 和 BrickerBot 两种僵尸网络甚至在任何网络终端设备中传播；

感染的基础平台主要分为 IoT 和 linux 两类，主要由于目前物联网设备的硬件计算能力由于成本和应用场景的约束，其主要基本平台以耗费硬件性能较低的 IoT 和 linux 为主。

表 2 IoT 相关 Botnet 寄宿平台对比

僵尸网络分类	感染硬件类型	感染基础平台
IoT_reaper ^{43 44}	1. 路由器设备：Dlink、Netgear、Linksys; 2. 摄像头设备：Goahead、JAWS、AVTECH 3. 网络硬盘录像机：Vacon	IoT/linux
Persirai ^{44 45}	摄像头设备	IoT
Hajime ⁴⁷	互联网任何设备	IoT
Gafgyt ⁴⁸	路由器设备：Netcore、Netis	IoT/Linux
Amnesia ⁴⁹	摄像头设备：DVR 设备	IoT
Rowdy ⁵⁰	机顶盒设备	Linux
BrickerBot ⁵¹	摄像头、机顶盒等	Linux

43 <https://research.checkpoint.com/new-iot-botnet-storm-coming/>

44 <http://blog.netlab.360.com/iot-reaper-a-quick-summary-of-a-rapid-spreading-new-iot-botnet/>

45 <https://www.incapsula.com/blog/from-mirai-to-persirai.html>

46 <http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/>

47 <http://blog.nsfocus.net/hajime-sample-technical-analysis-report/>

48 <http://toutiao.secjia.com/gafgyt-iot-malware>

49 <https://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/>

50 <http://blog.nsfocus.net/iot-set-top-box-malware-rowdy-network-analysis-report/>

51 <https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/>

6.2.3 传播手法对比分析

新型僵尸网络的感染方式，已经不仅仅限于 Mirai 单纯破解弱口令的方式，各种针对漏洞和后门的利用也加大了僵尸网络的速度和规模；而且不法分子还在持续增加新的漏洞，以保持其僵尸网络的可持续发展；

传播方式以主要 telnet 自动化扫描特定端口为主，但新型的 HTTP 等应用层的探测方式也成为未来的发展趋势。

表 3 IoT 相关 Botnet 传播手法对比

僵尸网络分类	感染方式	传播方式
IoT_reaper	漏洞利用，已经集成 15 个漏洞	Telnet 自动化扫描
Persirai	<ol style="list-style-type: none"> 1. 默认口令和弱口令利用 2. 漏洞利用，已经集成了 3 个漏洞 	WEB 扫描
Hajime	<ol style="list-style-type: none"> 1. 默认口令和弱口令 2. 利用 RCE 漏洞利用 	<ol style="list-style-type: none"> 1. 搜索 DHT 网络 2. Arris 电缆调制解调器 3. TR-069 协议利用
Gafgyt	Netcore 路由器 igdmpd 漏洞的利用	主动扫描 53413 端口
Amnesia	利用 RCE 漏洞利用	HTTP 响应关键字扫描
Rowdy	默认口令和弱口令利用	Telnet 自动化扫描
BrickerBot	默认口令和弱口令利用	Telnet 自动化扫描

6.2.4 潜在威胁对比分析

新型僵尸网络的感染规模从近一万到上千万不等，与被感染设备的安全性和感染方式的技巧均有较大的关系；

僵尸网络的威胁主要还是以 DDoS 攻击为主，其攻击带宽预估最大能够达到近 T 的级别，攻击类型也有传统 TCP、UDP、CC 为主，也出现了具备 lua 执行环境具备执行复杂高效的 CC 攻击能力的僵尸网络；

BrickerBot 僵尸网络需要特别说明，其创建的初衷并非恶意制造 DDoS 攻击，而是称为“互联网化疗”意在让易受攻击的设备脱机，迫使设备所有者安装更新固件；但业界和专家普遍认为其对物联网设备本身进行永久拒绝服务（PDoS-Permanet Denial of Service）。

表 4 IoT 相关 Botnet 潜在威胁对比

僵尸网络分类	感染规模	潜在 DDoS 攻击威胁
IoT_reaper	10k/d 的日活节点	<ol style="list-style-type: none"> 攻击带宽为 100G； 基于 lua 执行环境具备执行复杂高效的 CC 攻击
Persirai	12w 被感染节点 (10% 活跃比率) 12k/d 的日活跃节点	<ol style="list-style-type: none"> 攻击带宽为 120G； 攻击类型以 SSDP 和 UDP 为主；
Hajime ⁵²	日活跃节点 6~8 万	<ol style="list-style-type: none"> 攻击带宽为 600~800G； 暂时并未有任何类型攻击；
Gafgyt	全球 150 万台被感染，中国境内 120 多万台	<ol style="list-style-type: none"> 全球攻击带宽最大能达到为 15Tbps； 攻击类型以 UDP、TCP、HTTP 为主
Amnesia	23w 台设备存在漏洞，感染率为 1%， 2.3w 台设备	<ol style="list-style-type: none"> 攻击带宽为 230G； 攻击类型以 UDP、HTTP 为主
Rowdy	监控僵尸网络 3000 台 (国内)	<ol style="list-style-type: none"> 攻击带宽为 30G； 攻击类型以 SYN、ACK、HTTP、DNS、GRE
BrickerBot	1 千多万物联网设备	对物联网设备本身进行永久拒绝服务 (PDoS-Permanet Denial of Service)

52 <https://sec.xiaomi.com/article/33>



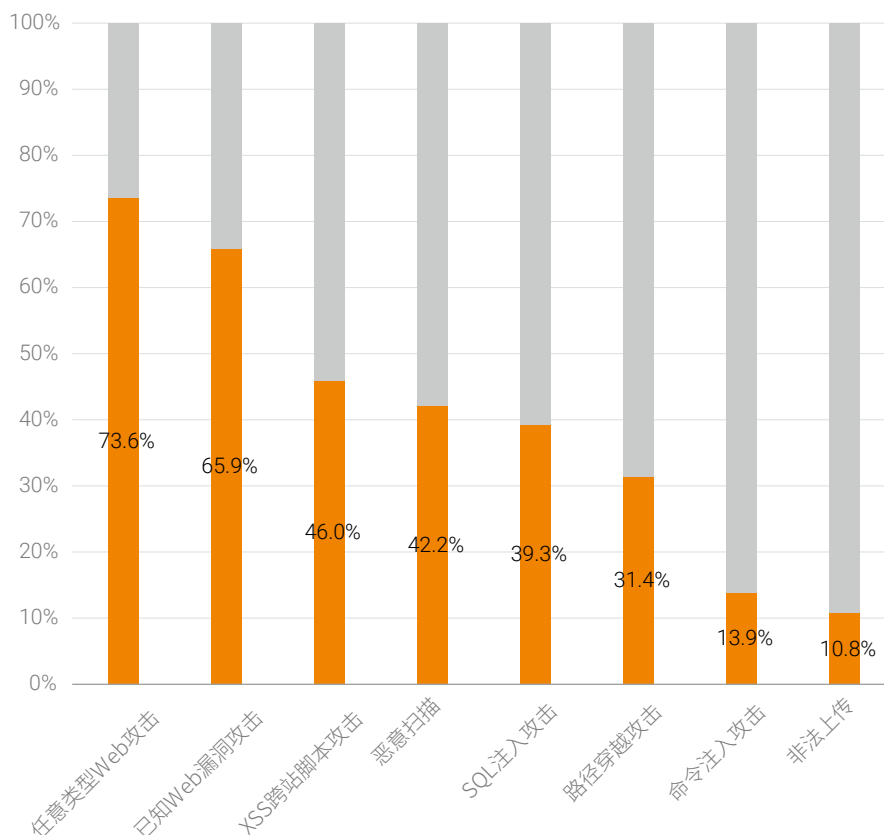
7. 2017 年 Web 应用攻击态势

7.1 被攻击目标站点	42
7.2 被攻击目标行业	43
7.3 Web 应用攻击类型	43
7.4 利用 Web 服务器已知漏洞的攻击	46
7.5 利用 Web 框架或应用已知漏洞的攻击	47
7.6 Web 攻击源 IP 攻击广度与其 IP 信誉	49
7.7 Web 应用攻击时间分布	50
7.8 Web 应用攻击地域分布	52
7.9 热点漏洞分析	53

7.1 被攻击目标站点

2017 年我们防护的 Web 站点中，有 73.6% 的 Web 站点曾遭受过任意类型的 Web 应用攻击。从攻击利用的手段看，利用已知 Web 漏洞攻击的攻击目标范围最广，有 65.9% 的站点曾遭受了此类攻击（包括针对已知 Web 服务器漏洞和 Web 框架漏洞的攻击）。其次是 XSS 跨站脚本攻击，恶意扫描和 SQL 注入攻击，被攻击的站点分别占总站点数量的 46.0%、42.2% 和 39.3%。在信息化的时代，企业的商业风险与其关键业务面临的 Web 安全威胁息息相关。而 Web 面临的安全威胁随着企业 Web 应用的数量和 Web 应用包含的漏洞数增加而迅速增加。有研究⁵³表明，平均每个 Web 站点大概包含 5-32 个漏洞，而每个开放的漏洞平均生命周期是 300 天，高危漏洞的生命周期甚至超过 500 天，也就是说大多数的 Web 站点在大部分时间内都是包含漏洞的，对于 Web 站点的已知的漏洞，如不及时修复，等于将自己的业务缺陷直接暴露在互联网上，企业将面临巨大风险。

图 7.1 遭受 Web 应用攻击的站点占比



数据来源：绿盟科技可管理安全服务（MSS）

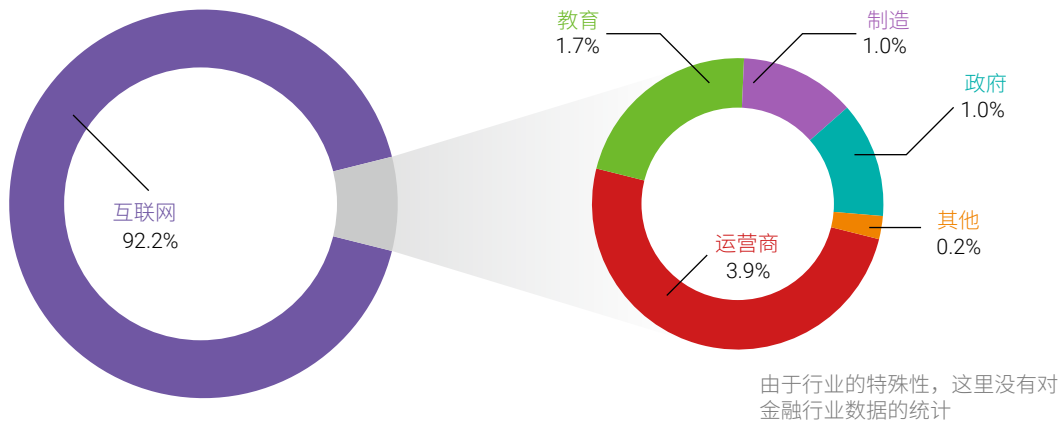
53 <https://info.whitehatsec.com/rs/675-YBI-674/images/WH-2016-Stats-Report-FINAL.pdf>

7.2 被攻击目标行业

由于各行业的业务形态和承载业务的基础架构千差万别,其所遭受到的Web应用攻击的情况也存在较大差异。2017年,遭受Web应用攻击最多的行业是互联网企业,其攻击总次数占全部攻击数量的92.2%。一方面互联网行业大量的业务以Web形态提供服务,另一方面背后需要架设复杂IT架构提供支撑,使得互联网行业是Web应用类攻击的重灾区。

单从行业自身业务特征看,不光是互联网行业,各行各业都应该重视Web类的攻击。可以说,针对Web应用的攻击是打开企业内网的第一道大门,一旦实施成功,轻则网页被篡改,损失声誉,重则可能导致大量敏感信息泄露或数据库被删,丢失重要数据,不但会造成重大经济、名誉上的损失,也需要承担相应的法律责任。

图 7.2 各行业遭受 Web 应用类攻击的攻击次数占比



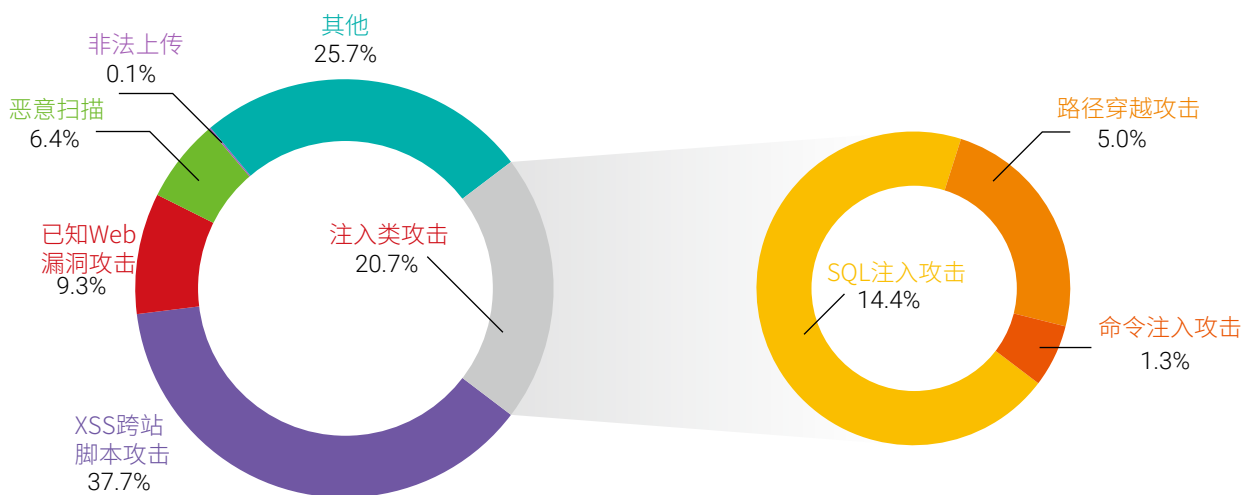
数据来源:绿盟科技可管理安全服务(MSS)

7.3 Web 应用攻击类型

7.3.1 Web 应用攻击类型

我们对2017年发生的Web应用攻击事件的类型进行统计,占比如下图所示。排名最高的是XSS跨站脚本攻击,占比达37.7%。其次是注入类攻击,占比为20.7%,其中包括SQL注入攻击(14.4%)、路径穿越(5%)、命令注入(1.3%)等。排名第三的是已知Web漏洞攻击,包含针对服务器的已知漏洞攻击和针对Web框架或插件的已知漏洞攻击,占比为9.3%。OWASP连续两年将注入类攻击排在最高风险级别,在2017年重构的《OWASP Top10》中再次将此类攻击风险定位为A1级别。XSS跨站脚本攻击的风险虽然从A3下调至A7,但其仍然是黑客进行Web攻击时最常利用的攻击方式。

图 7.3 针对 Web 应用的各类攻击攻击次数占比

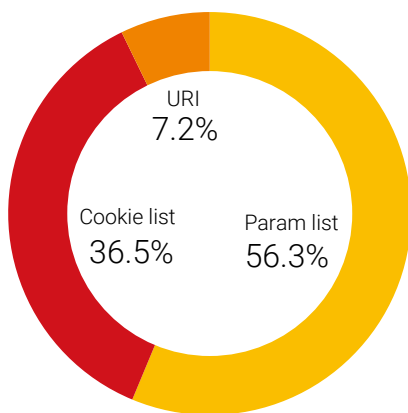


数据来源：绿盟科技可管理安全服务 (MSS)

7.3.2 注入类攻击常见 Payload 注入位置

很多 Web 攻击者精心构造 HTTP 攻击报文，将其尽可能的伪装成正常请求并发送给攻击目标，使得目标服务器按照非正常流程运行，以达到获得系统或服务器敏感信息、上传恶意文件等目的。如 SQL 注入、命令行注入等攻击，这些攻击最常见的攻击插入位置如下图所示，其中 URL 中的参数列表 (Param List) 是黑客最喜欢插入攻击语句的地方，这种情况占全部攻击插入或修改位置的 47.3%。其次是 Cookie，占比 45.1%，剩下的是在 URI 处。

图 7.4 注入类攻击常见 Payload 注入位置

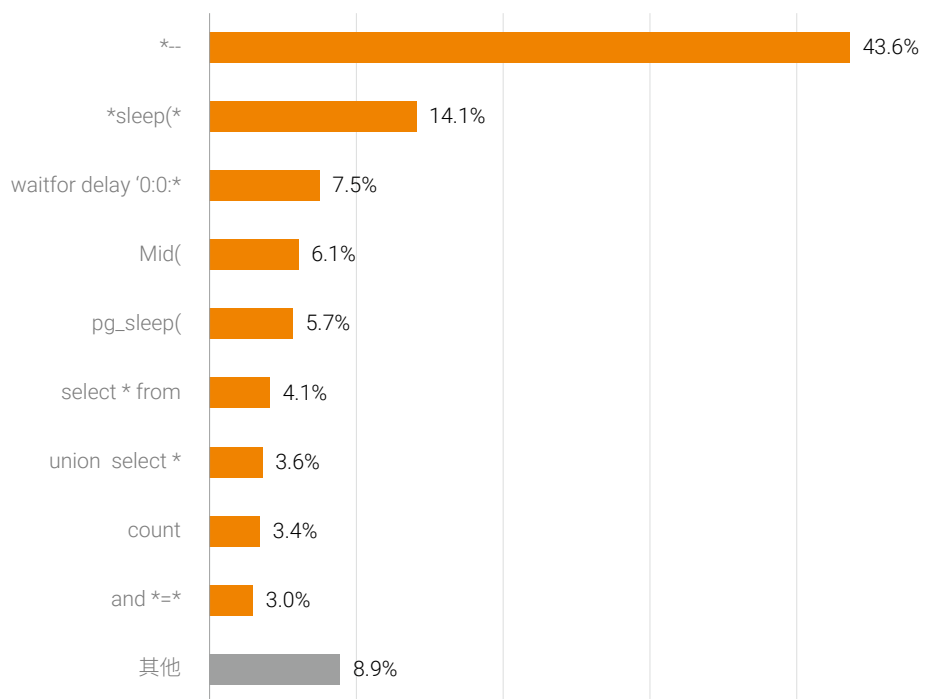


数据来源：绿盟科技可管理安全服务 (MSS)

7.3.3 SQL 注入攻击常见 Payload

注入类攻击中，最常见的就是 SQL 注入攻击。SQL 注入是从正常的端口访问，把 SQL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令。而且表面看起来跟一般的 Web 页面访问没有什么区别，所以目前市面上的大多数防火墙对 SQL 注入是无法有效识别的，需要专门的 Web 应用防火墙对此类攻击进行专门防护。2017 年，我们统计 SQL 注入攻击中黑客最常使用的 SQL 注入 Payload Top 10 如下图所示。

图 7.5 2017 年黑客最常使用的 SQL 注入 Payload Top 10



数据来源：绿盟科技可管理安全服务 (MSS)

1. *-- 的插入语句最为常用，占全部攻击 Payload 的 43.6%。直接将 -- 写在 sql 的中间可以注释掉过滤条件，直接获取数据库的数据结构。这种插入用法非常简单，在注入探索数据库的初期较常用到。
2. *sleep(* 插入语句排名第二，占比 14.1%。与 pg_sleep(* 类似，如 select sleep(2)--、select pg_sleep(5)-- 等常用于 MySQL、PostgreSQL 数据库基于时间的盲注，waitfor delay '0:0:*' 也是这个作用，常用于 MSSQL 数据库基于时间的盲注。并且在通常情况下 sleep 函数返回值为恒为 0，可以借助 sleep(n)=0 的永真性执行 sql 注入。
3. Mid(占比 6.1%，此函数常用来截取字符串。例如：MID(DATABASE(),1,1)>' a'，查看数据库名第一位，MID(DATABASE(),2,1) 查看数据库名第二位，依次查看各位字符。常用于对数据库名称、用户名等的猜测。

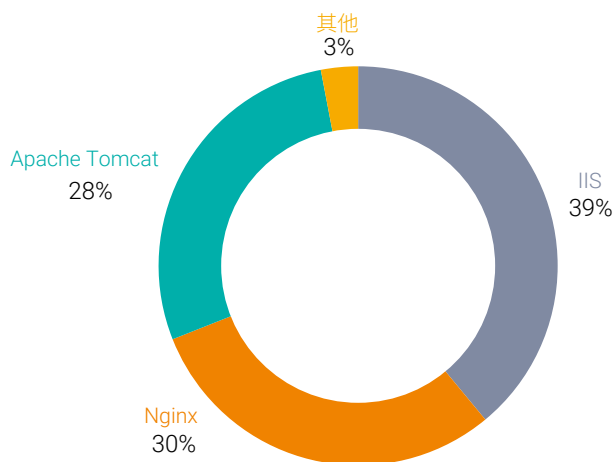
从 SQL 注入攻击 Payload 的特征字符串统计看，大多数攻击都处于初期对站点漏洞是否存在的探测踩点阶段。

7.4 利用 Web 服务器已知漏洞的攻击

7.4.1 受攻击的目标服务器类型

在利用已知漏洞的攻击中，受攻击的 Web 服务器类型主要是：Microsoft IIS（39%）、Nginx（30%）、Apache Tomcat（28%）。这三种服务器类型也是大多数企业网站最常用的服务器类型。

图 7.6 受攻击的 Web 服务器类型占比

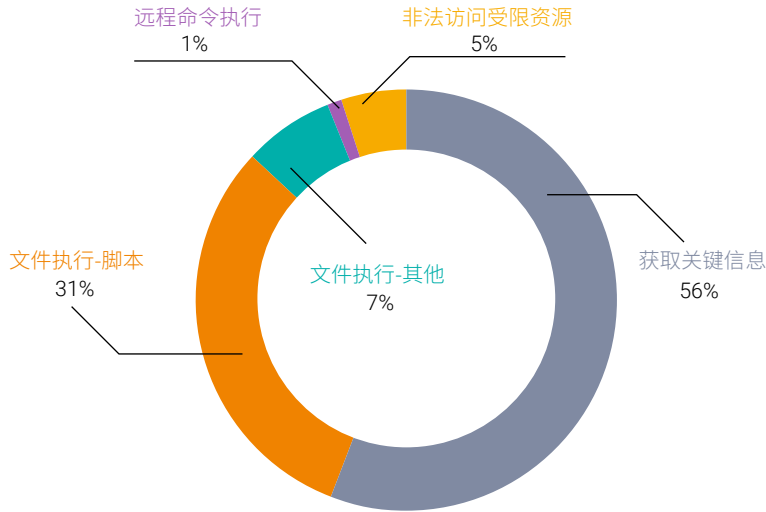


数据来源：绿盟科技可管理安全服务（MSS）

7.4.2 攻击利用 Web 服务器已知漏洞的类型

从漏洞类别上看，大部分的漏洞利用都能够导致关键信息的泄露，这包括对目录文件的枚举、文件路径的泄露以及网站脚本文件源码泄露、系统配置文件信息被读取等，这部分攻击占全部攻击的 56%。另外一类显著的攻击方式是文件执行类的攻击，这类攻击，通常会利用服务器程序对 URL、文件名解析的缺陷结合文件上传功能，将上传的文件当做脚本运行，利用 Webshell 实现进一步的入侵操作。此外，还有一部分攻击能够越权访问受限的资源，在受限的目录位置进行文件读取、下载、上传操作，甚至直接执行目录中的可执行文件。

图 7.7 攻击中 Web 服务器被利用的漏洞类型



7.4.3 利用 Web 服务器已知漏洞攻击 Top10

下图是 2017 被攻击的 Web 服务器漏洞 Top10。值得注意的是，与《2017 年中互联网安全观察》提到的趋势一致，大部分攻击中黑客尝试使用的漏洞是一些已经非常“古老”的漏洞。

表 5 2017 被攻击利用的 Web 服务器漏洞 Top10

漏洞名称	产品	发布时间	CVSS 分数	攻击比例
Apache Tomcat isp 应用服务器程序头信息泄露漏洞 (CVE-2008-5519)	Apache Tomcat	2009	2.6	9.8%
Tomcat 目录遍历漏洞 (CVE-2008-2938)	Apache Tomcat	2008	4.3	1.0%
IIS 文件上传漏洞 (CVE-2009-4445, CVE-2009-4444)	Microsoft	2009	6	0.5%
Microsoft iis 安全扩展名输入验证漏洞 (CVE-2010-1899)	Microsoft	2009	4.9	0.4%
Nginx 文件遍历漏洞 (CVE-2009-3898)	Nginx	2009	4.9	0.4%
IIS CGI 程序名解析错误导致文件执行漏洞 (CVE-2000-0886)	Microsoft	2000	7.5	0.3%
Apache 头部数据长度异常导致服务器资源耗尽 (CVE-2011-3192)	Apache Tomcat	2011	7.8	0.2%
IIS 文件扩展名解析错误导致 ASP 代码泄漏 (CVE-1999-0253)	Microsoft	1999	7.5	0.2%
IIS 中 Unicode 字符解码错误导致远程命令执行 (CVE-2000-0884)	Microsoft	2000	7.5	0.1%
IIS 脚本文件名解析漏洞 (CVE-2009-4444)	Microsoft	2009	6	0.1%

数据来源：绿盟科技可管理安全服务 (MSS)

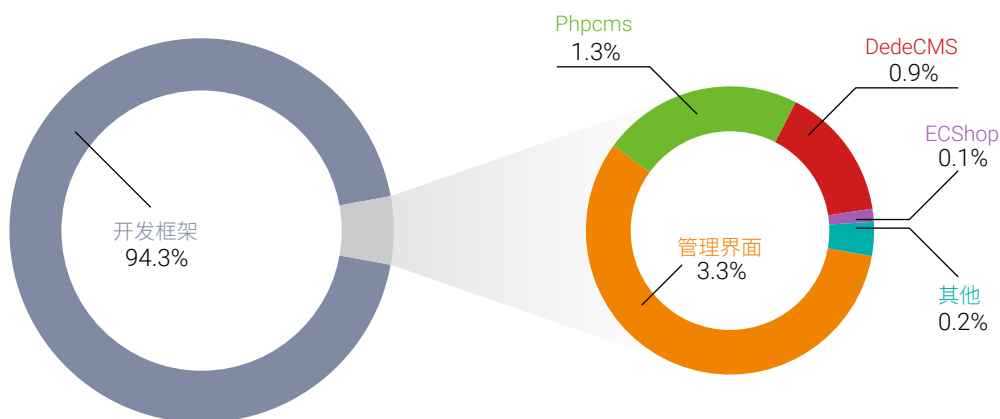
7.5 利用 Web 框架或应用已知漏洞的攻击

7.5.1 受攻击的 Web 框架或应用类型

Web 框架是指一类用于构建 Web 程序的框架类程序，用来支持动态网站、网络应用程序及网络服务的开发，很多通用型的 Web 业务系统也是基于类似的架构进行开发的，常见的框架包括 Django、ThinkPHP、

Apache Struts、Spring 等。Web 应用包括使用 PHP、JSP、ASP 语言搭建的各类 CMS（DedeCMS、ECShop、WordPress、phpBB、phpCMS、PHPWind 等），以及一些用于管理界面类的 Web 应用程序。2017 年，在针对这些重要的 Web 框架或应用的漏洞攻击中，我们看到对框架类程序的攻击是最频繁的，有 94.3% 的攻击是针对框架类的。针对 Struts2 的漏洞攻击是其中的典型代表。

图 7.8 2017 被攻击的 Web 框架或应用的类型



7.5.2 利用 Web 框架或应用已知漏洞 TOP10

下图是 2017 年利用已知 Web 框架或应用漏洞的攻击 Top10。由数据可知，Apache Struts2 相关漏洞仍旧是被利用最频繁的漏洞，攻击 Top10 中占了 7 个，其中 2 个是 2017 年爆出的。2017 年 3 月 7 日爆发 Apache Struts2 CVE-2017-5638 的高危漏洞（CVSS 评分 10），占全部已知漏洞攻击的 16.8%。关于该漏洞的影响范围、攻击和修复情况，具体请见《绿盟科技 2017 H1 DDoS 与 Web 应用攻击态势报告》。关于 2017 年 9 月爆出的 Apache Struts 2 REST 插件安全漏洞（CVE-2017-9805）的分析及攻击情况请见 6.9.1 节。

表 6 2017 年被攻击利用的 Web 框架或应用漏洞 Top10

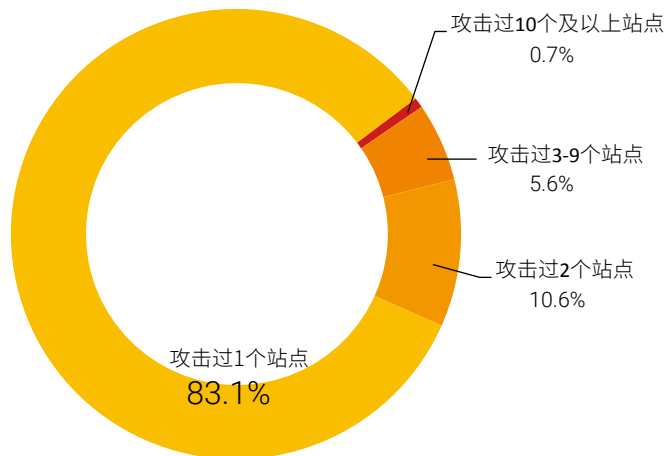
漏洞名称	产品	发布时间	CVSS 分数	攻击比例
Struts2 REST 插件远程代码执行漏洞 (CVE-2016-4438)	Apache Struts2	2016	7.5	49.8%
Struts2 Jakarta 插件远程命令执行 (CVE-2017-5638)	Apache Struts2	2017	10	16.8%
Apache Struts2 REST 插件安全漏洞 (CVE-2017-9805)	Apache Struts2	2017	6.8	7.6%
Struts2 远程命令执行 (CVE-2013-1966)	Apache Struts2	2013	9.3	6.9%
Struts2 远程命令执行 (CVE-2013-2251)	Apache Struts2	2013	9.3	4.8%
ElasticSearch 沙盒绕过导致远程代码执行 (CVE-2015-1427)	ElasticSearch	2015	7.5	0.4%
Struts2 ClassLoader 操作漏洞 (CVE-2014-0094)	Apache Struts2	2014	5	0.3%
Struts2 恶意 Ognl 表达式导致远程代码执行 (CVE-2016-3081)	Apache Struts2	1916	9.3	0.2%
DedeCMS 多个 SQL 注入漏洞 (CVE-2011-5200)	DedeCMS	2012	7.5	0.1%
pivotal Spring Data REST、Spring Boot 和 Spring Data 安全漏洞 (CVE-2017-8046)	pivotal_software	2017	7.5	0.1%

数据来源：绿盟科技可管理安全服务（MSS）

7.6 Web 攻击源 IP 攻击广度与其 IP 信誉

我们对所有参与过 Web 攻击的攻击源 IP 的攻击广度进行了分析，发现有 16.9% 的 IP 曾经对 2 个及以上的 Web 站点发起过攻击。

图 7.9 Web 应用攻击源 IP 攻击广度



■ 攻击过10个及以上站点 ■ 攻击过3-9个站点 ■ 攻击过2个站点 ■ 攻击过1个站点

数据来源：绿盟科技威胁情报中心（NTI）

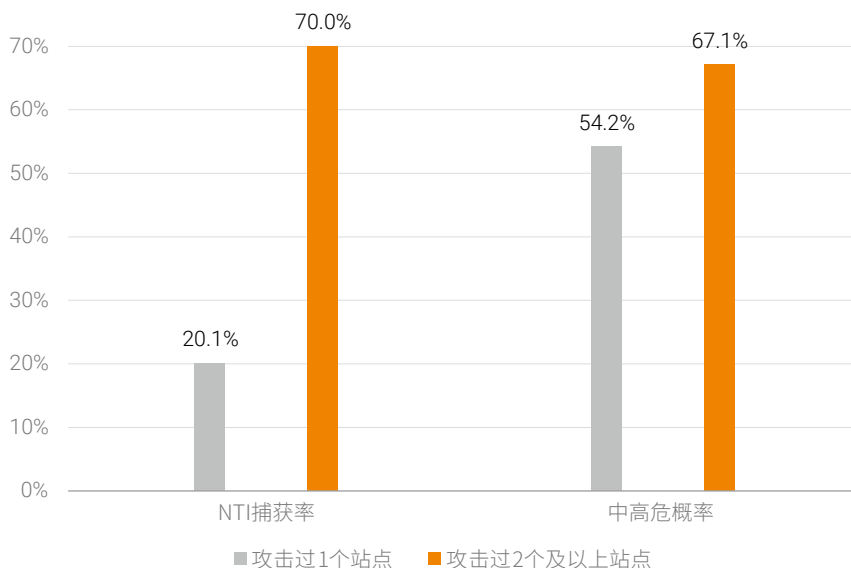
结合绿盟科技威胁情报中心（NTI）信誉数据进行分析，发现攻击过 1 个站点的攻击源 IP 中，在 NTI 上有不良 IP 信誉记且被标识为中、高危的占 54.2%；攻击过多个（2 个及以上）Web 站点的攻击源 IP 中被标识为中、高危的占比为 67.1%。表明攻击源 IP 攻击广度越高，攻击源越活跃，在 NTI 上被标识为异常的概率越大，其为高级别威胁的概率也越大。

在 5.2.4 节中，我们对参与 DDoS 攻击的攻击源同样作了信誉情况分析，与 Web 攻击源在捕获率和中高威胁等级标识的概率上会有差异。比如，对于惯犯攻击源（攻击过 2 个及以上目标的），DDoS 的攻击源的捕获率为 94.1%，Web 攻击源的为 70%；在威胁等级识别上，DDoS 的攻击源被标识为中、高威胁等级的概率为 20.9%，而 Web 的攻击源为 67.1%。这主要由于 DDoS 和 Web 应用攻击这两种攻击在攻击性质、攻击手段及造成的影响方面各不相同，NTI 在的攻击源数据处理上会不同。比如，DDoS 攻击发生时通过消耗网络带宽或服务资源导致目标服务直接不可用，攻击停止后服务可用性恢复，而 Web 应用攻击比较隐蔽，很多时候是为了获取系统权限或机密数据，一旦实施成功会对目标会造成较长远的影响（这里说的是对业务的直接影响，不包括对公司信誉、业务流失等间接影响）。另外一方面，一般 Web 攻击的攻击源都为真实 IP，为了达到目的，很多时候攻击者会逐步开展攻击，比如先扫描站点漏洞，再进行漏洞利用的渗透，一旦成功攻击者就有可能控制系统，如获取机密数据、恶意破坏数据库等等，因此，认为实施某些类别 Web 攻击的攻击源的威胁等级更高。

我们对 2017 年参与过 DDoS 攻击和参与过 Web 攻击的攻击源进行比对，发现其中有近 5 万个攻击源既发起过 DDoS 攻击也发起过 Web 攻击。这其中，有超过 60% 的攻击源曾经向外发起过扫描，而这部分攻击源中有 88.3% 为中高威胁等级。虽然这些 IP 不一定固定属于某个黑客组织，但由于托管机构、主机拥有者对自身资产的监管不严，导致这部分设备受到黑客控制的频率相较其他 IP 要高出很多，几乎成为黑产的“固定攻击资产”。

这批 IP 占比不高，但是在网络中引起了不少的麻烦和混乱。据绿盟科技《2017 网络安全观察》报告统计：网络中 0.39% 的攻击源对 90% 的攻击事件负责。

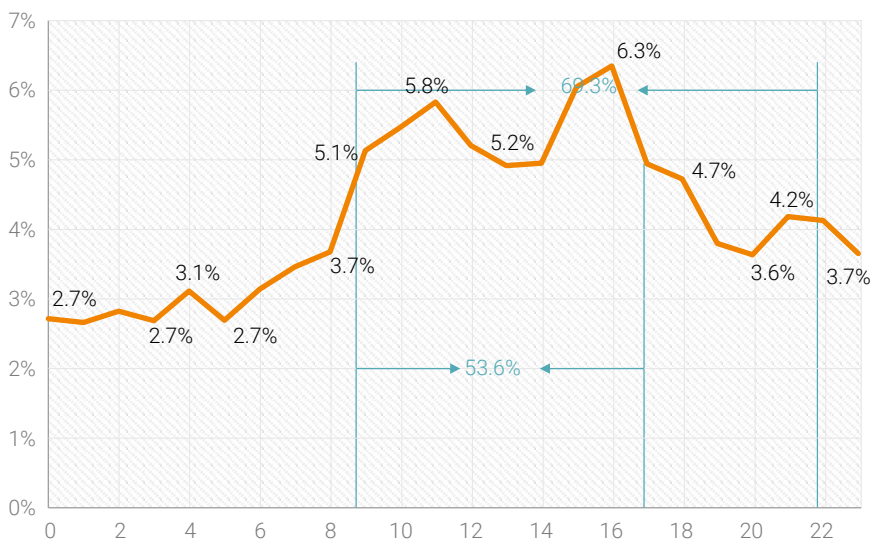
图 7.10 Web 应用攻击源 IP 攻击过的目标站点数量与 IP 信誉情况



7.7 Web 应用攻击时间分布

一天 24 小时各个时段发生的 Web 应用攻击分布如下图所示。Web 业务使用高峰时间段在早上 9 点到晚 22 点，这段时间 Web 应用攻击频发。尤其在上午 9 点到下午 17 点间 Web 业务使用最高峰期，也是攻击者最活跃的时间，这段时间发生的 Web 攻击占全部攻击的 53.6%。

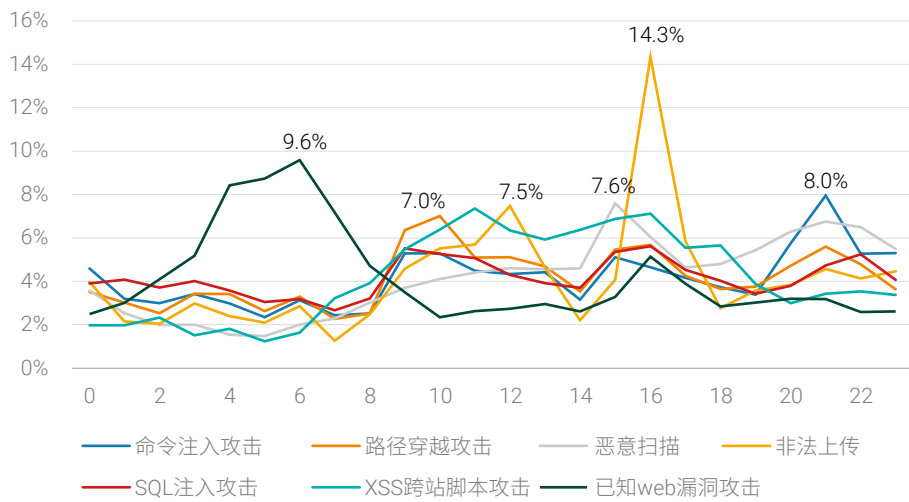
图 7.11 Web 应用攻击源 IP 攻击过的目标站点数量与 IP 信誉情况



数据来源：绿盟科技可管理安全服务 (MSS)

我们统计了各类 Web 应用攻击在一天 24 小时各时间段攻击次数变化趋势，如下图所示。其中已知 Web 漏洞攻击较多发生在业务量较低的凌晨，在 4-6 点间处于攻击最频发的时段，这类攻击有很多集成的自动化工具，大部分不需要客户端交互进行。而其他类型攻击一般多发生在 Web 业务使用高峰时段（早 9 点到晚 22 点），此时造成的影响和破坏力也更大。

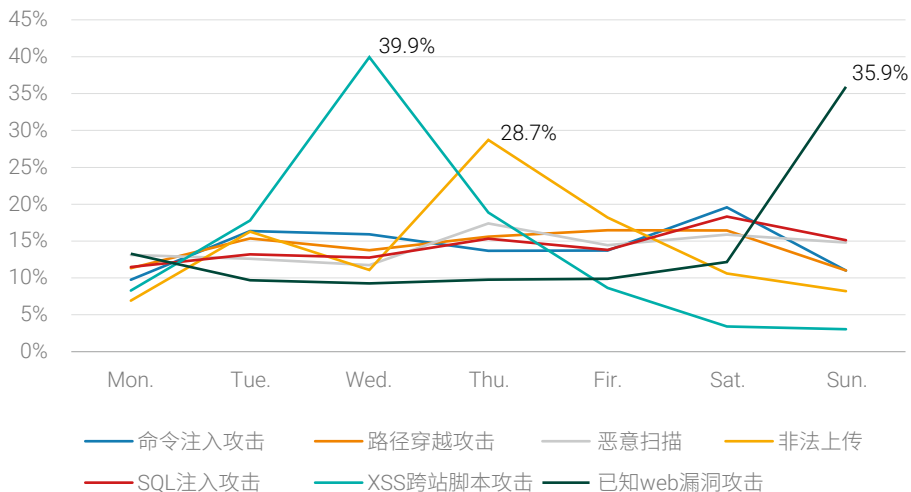
图 7.12 一天 24 小时各类型 Web 应用攻击频次分布



数据来源：绿盟科技可管理安全服务（MSS）

一周 7 天中 8 类攻击类型的攻击趋势如下图所示。其中波动较为明显的有跨站脚本攻击、非法上传、已知 Web 漏洞攻击。XSS 在星期三的时候攻击量占一周 XSS 总攻击量的 39.9%，在周末两天中攻击量很少，仅占比 3%。UPLOAD 在星期四有一个小高峰，占比达到 UPLOAD 一周攻击总量的 28.7%。已知 Web 漏洞攻击在工作日的攻击占比较少，在星期天突然上升，占比达到一周 Web 漏洞攻击总量的 35.9%，这个现象也与已知 Web 漏洞中自动化攻击占比很大的原因有关系。其余几项攻击类型在一周的攻击量分布较均匀。

图 7.13 一周 7 天各类 Web 应用攻击攻击频次分布



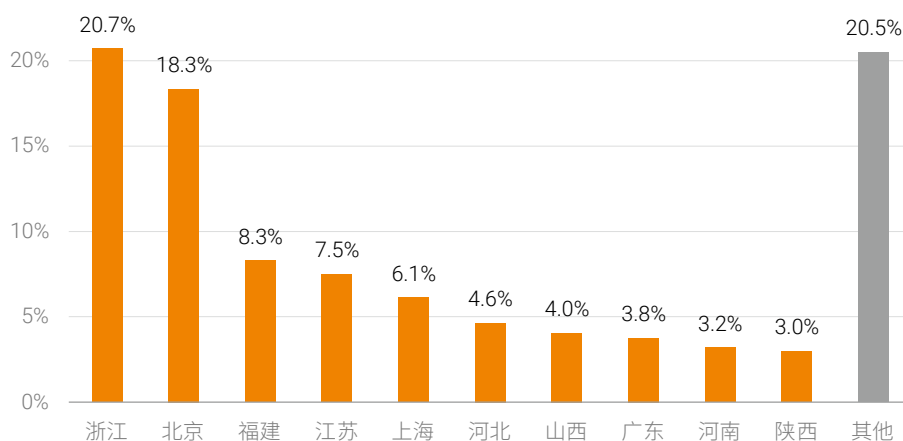
数据来源：绿盟科技可管理安全服务（MSS）

7.8 Web 应用攻击地域分布

7.8.1 攻击源主机地理分布

Web 应用攻击的攻击源在中国地区的占比 Top10 如下图所示。其中浙江和北京占比相对较高，分别是 20.7% 和 18.3%。

图 7.14 Web 应用攻击的攻击源中国各省份占比分布

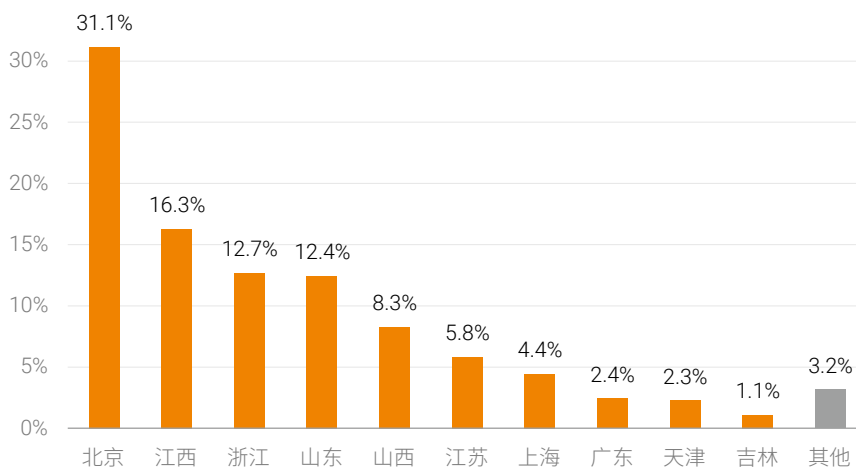


数据来源：绿盟科技可管理安全服务 (MSS)

7.8.2 攻击目标地理分布

Web 应用攻击的攻击目标中国各省份分布情况如下图所示。其中北京受到的攻击量最大，占比 31.1%。其次是江西，被攻击次数占比达到 16.3%。

图 7.15 中国各省份 Web 应用攻击的攻击目标占比分布



数据来源：绿盟科技可管理安全服务 (MSS)

7.9 热点漏洞分析

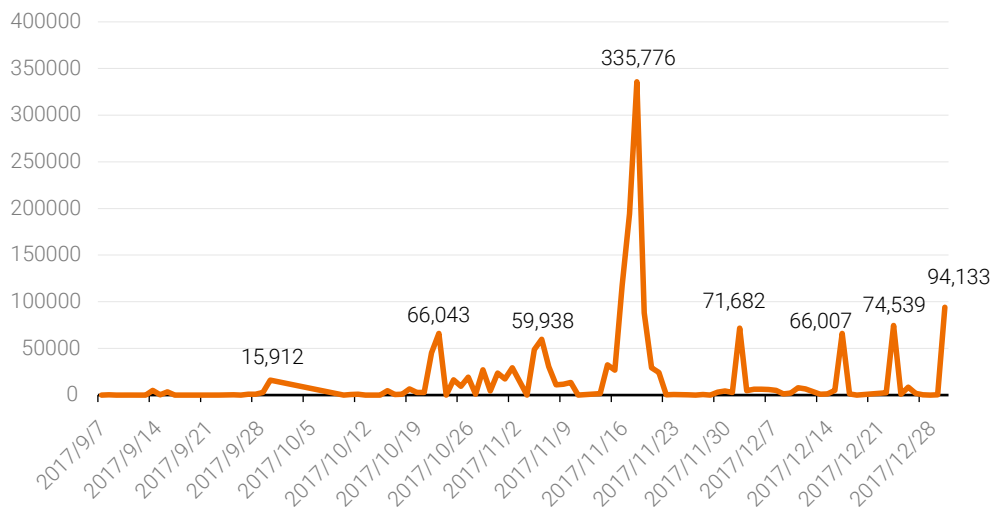
7.9.1 Apache Struts 2 REST 插件安全漏洞 (CVE-2017-9805)

Apache Struts 2 REST 插件安全漏洞 (CVE-2017-9805)⁵⁴ 是 2017 年 9 月份爆出的漏洞，危险评分 6.8。Apache Struts 2.5 版本至 2.5.12 版本和 2.1.2 版本至 2.3.33 版本的 REST 插件存在远程代码执行漏洞。当 Struts2 通过 REST 插件使用 XStream 的实例 xstreamhandler 处理反序列化 XML 有效载荷时没有进行任何过滤，导致远程攻击者可以利用该漏洞构造恶意的 XML 内容，进而获取业务数据或服务器权限，执行任意代码。

Apache Struts2 作为世界上最流行的 Java Web 服务器框架之一，被广泛用于政府、企业组织、金融等行业的门户网站的底层模版建设，其被爆出的漏洞非常多，仅 2017 年一年就爆出 8 个 Apache Struts2 相关漏洞，其中 4 个是高危漏洞。由图 6.10 可知，2017 年利用 Web 框架或应用已知漏洞攻击中，Apache Struts2 的漏洞是最频繁被利用的漏洞，Top10 就占了 7 个。

我们统计了该漏洞从 2017 年 9 月 7 日到 2017 年 12 月 31 日之间的攻击次数，如下图所示。针对所有 NSFOCUS 监控的 Web 站点，三个月内共发生了 1,712,983 次针对该漏洞的攻击，在 11 月 16 号到 11 月 21 号攻击量骤增，最高达 335,776 次 / 日。

图 7.16 CVE-2017-9805 漏洞攻击分布图 (单位: 次)



数据来源: 绿盟科技可管理安全服务 (MSS)

建议企业及时修复该漏洞，并针对该漏洞做好检测和防御措施。绿盟科技在《Struts2 s2-052 REST 插件远程代码执行技术分析 with 防护方案》⁵⁵ 中给出了关于该漏洞的处置方法，包括漏洞修复方案、专业安全设备如 WAF/NF/IPS/RSAS/WVSS 等针对该漏洞的检测和防御方法。

7.9.2 WebLogic XMLDecoder 反序列化漏洞 (CVE-2017-10271)

Oracle Fusion Middleware Oracle WebLogic Server 组件安全漏洞 (CVE-2017-10271)⁵⁶ 是 2017 年 10 月 23

54 <http://blog.nsfocus.net/struts2-s2-052-rest-plug-in-remote-code-execution-technical-analysis/>

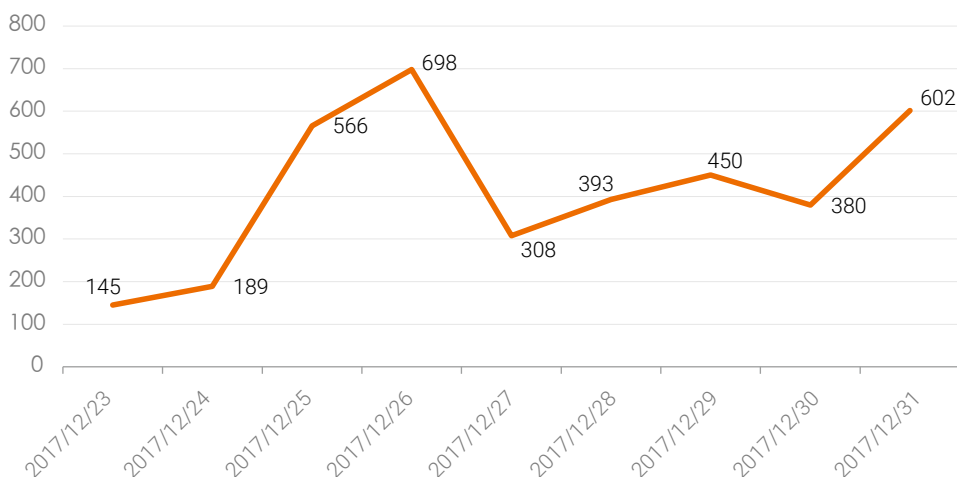
55 <http://blog.nsfocus.net/struts2-s2-052-rest-plug-in-remote-code-execution-technical-analysis/>

56 <http://toutiao.secjia.com/nsfocus-internet-security-threats-weekly-201750>

日发布的漏洞，危险评分 7.5。Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能，Oracle WebLogic Server 是其中的一个适用于云环境和传统环境的应用服务器组件。Oracle Fusion Middleware 中的 Oracle WebLogic Server 组件的 WLS Security 子组件存在安全漏洞，使用精心构造的 xml 数据可能造成任意代码执行，攻击者只需要发送精心构造的 HTTP 请求，就可以拿到目标服务器的权限。攻击者可利用该漏洞控制组件，影响数据的可用性、保密性和完整性。

下图统计了 NSFOCUS 监控的 Web 站点 2017 年最后一周针对此漏洞的攻击量，一周攻击总量有 3397 次，最高达 698 次 / 日。

图 7.17 CVE-2017-10271 漏洞攻击分布图（单位：次）



数据来源：绿盟科技可管理安全服务（MSS）

在 Weblogic WLS 组件漏洞(CVE-2017-10271)漏洞暴露不久后，绿盟科技接到多个行业客户的安全事件反馈，经分析发现攻击者利用该漏洞向 Weblogic 主机植入 watch-smartd 挖矿恶意程序⁵⁷。该恶意程序的运行会极大的消耗服务器 CPU 和内存资源，而且一旦感染很难清除。

Weblogic WLS 组件漏洞(CVE-2017-10271)属于没有公开细节的野外利用漏洞，虽然官方在 2017 年 10 月份发布了该漏洞的补丁，但大量企业尚未及时安装补丁。此次漏洞利用主要用于传播挖矿程序，不排除后面会被黑客用于其它目的，如构建 Botnet 进行 DDoS 攻击。利用该漏洞攻击者能够同时攻击 Windows 及 Linux 主机，并在目标中长期潜伏。由于 Oracle WebLogic 的使用面较为广泛，因此攻击面涉及各个行业。建议企业尽快对存在该漏洞的主机进行修复，并及时更新专业安全防护设备关于该漏洞的检查和防御的插件，调整相应的防御策略。

绿盟科技在《Weblogic WLS 组件漏洞处置建议》⁵⁸、《Weblogic WLS 组件漏洞技术分析与防护方案》⁵⁹中已经给出了该漏洞的处置建议，包括漏洞修复方案、恶意程序检测方法、专业安全设备如 WAF/NF/IPS/RSAS/WVSS 等针对该漏洞的检测和防御方法。

57 <http://toutiao.secjia.com/weblogic-host-mining>

58 <http://blog.nsfocus.net/weblogic-solution/>

59 <http://blog.nsfocus.net/weblogic-vulnerability/>



8. DDoS 和 Web 应用攻击防护

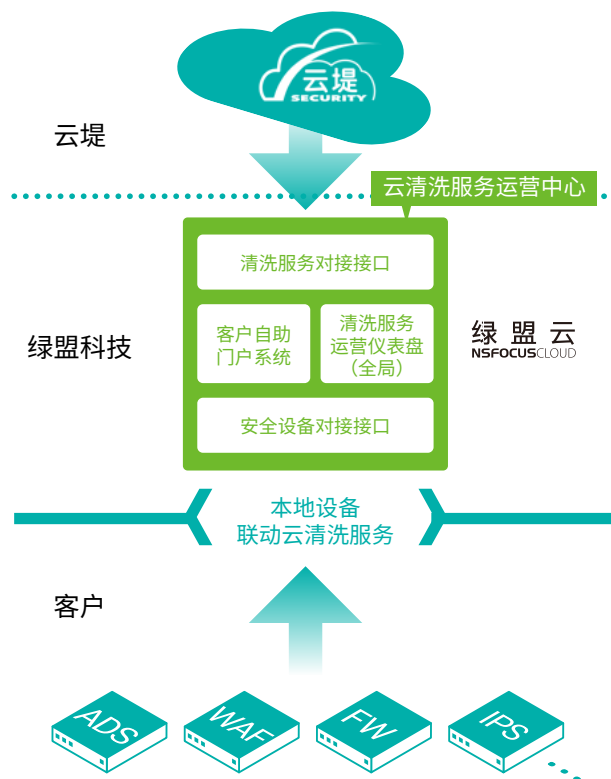
“云”、“大”、“物”、“移”时代背景下，网络安全威胁也在不断变化，传统防御手段受到挑战

8.1 DDoS 攻击防护.....	56
8.2 Web 应用攻击防护.....	58

8.1 DDoS 攻击防护

DDoS 攻击规模不断增大，2017 年我们观察到 300G 以上的超大规模攻击增多约 3 倍，百 G 以上的攻击已经常态化；攻击技术和手段不断出新；针对物联网的僵尸网络升级换代迅速，物联网大量沦为攻击工具；随着 DDoS 攻击服务化、产业化，使得发起 DDoS 攻击的成本不断降低。如此严峻的攻击形势下，DDoS 防护面临诸多挑战。通常情况下，抗 D 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。中国电信“云堤”提供突破性的近源清洗服务，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，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 8.1 云清洗场景



混合云清洗场景：

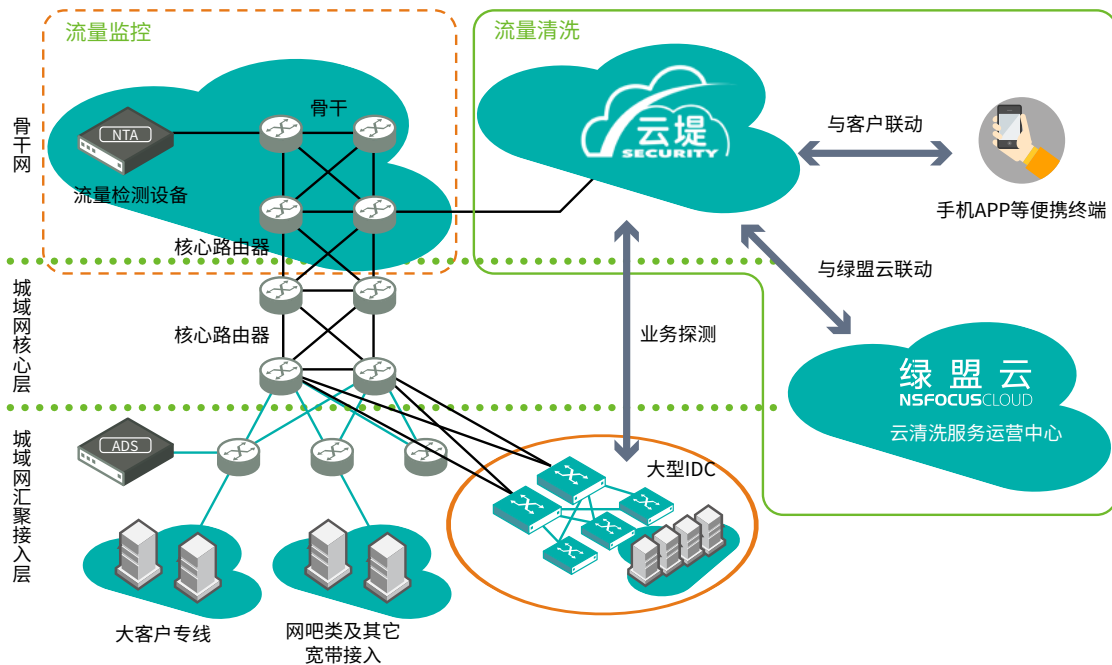
1. 用户有绿盟安全设备，购买了绿盟的云清洗服务；
2. 云清洗服务开通时，提供自服务账号给用户，用户自行配置与本地设备联动的相关配置后，用户本地设备将 DDoS 攻击流量信息上传至绿盟云。如果用户处的攻击流量超过设定阈值，将自动联动云清洗服务或短信通知用户当前攻击超阈值的情况，请其自行决定是否联动云清洗服务，如需要联动，可以做到一键联动云清洗服务；或自动触发云清洗服务；
3. 用户可以通过自服务页面实时查看清洗情况（云清洗和本地清洗报表），绿盟运维工程师运维在运营界面密切关注客户 DDoS 攻击清洗情况。

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，中、小规模攻击由本地防护设备清洗，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 8.2 混合防护方案



图 8.3 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。

绿盟科技基于十多年来在抗 D 攻防方面的经验积累及产品持续创新，2017 年推出了单体最大 240Gbps 防护能力的 ADS NX5-10000 型号抗 D 设备，专门面向高性能 DDoS 清洗应用场景，包括运营商骨干网和城域网、各类大型数据中心，以及清洗服务节点。结合绿盟科技威胁情报中心提供的全球僵尸网络情报数据、IP 信誉，及基于绿盟 DDoS 态势感知平台大数据分析的攻击预警，实现快速、智能抗 DDoS 攻击，保障用户业务持续、安全、稳定的运行。

8.2 Web 应用攻击防护

通过第七章 Web 应用攻击态势分析，可以看出：XSS 跨站脚本攻击、注入类攻击、恶意扫描，依然是黑客进行 Web 攻击时最常用的攻击手段；站点第三方组件安全问题凸显，对已知漏洞的攻击依然为黑客攻击站点的主要入口点，而社交媒体等渠道能快速披露、传播漏洞信息及漏洞利用工具，让攻击测试变得越来越容易；同时，以扫描为代表的自动化攻击的流行，造成站点漏洞被暴露的概率更高，更容易被黑客入侵。

另一方面，对客户市场业务调查了解到，当前虚拟化、云平台的普及，越来越多的客户将对公 Web 应用迁移至云环境下，使得为云上用户提供更好的 Web 安全防护有了更高要求。这与 Gartner 战略性规划假设保持一致，即“到 2020 年底，面向公众的 Web 中 50% 以上将受到基于云的 WAF 服务平台的保护，这种服务平台结合 CDN、分布式拒绝服务攻击（DDoS）保护、僵尸缓解服务和 WAF”。

基于目前的市场发展趋势，及一年来统计到的 Web 应用攻击事件，Web 应用攻击防护不再单纯依赖防御，检测和响应成为必须；不再强调单点的检测及单纯的报警，需结合多方资源配合及服务运营，为用户提供全面的 Web 安全防护。绿盟科技的 Web 应用防护解决方案，能够全面降低 OWASP TOP 10 风险、有效抵御自动化攻击带来的威胁、确保网站的可用性。涉及的产品和服务具体如下：

1. 云安全：

绿盟 Web 应用防火墙，支持接入多种公有云平台，如阿里云、亚马逊、微软、腾讯云、华为云等，为在公有云环境中部署的客户网站提供云安全防护能力、为云平台厂商提供安全增值服务。

2. 威胁情报：

可联动的自动化攻击防护方案：通过与绿盟威胁情报中心进行联动，实时获取最新的高危 IP 信誉库，在 WAF 上自动生成防护策略。通过启用 IP 信誉功能，可有效防止撞库、羊毛党（刷单、刷积分）的问题，同时有效减少疑似攻击行为的告警噪音，达到提升告警精度的效果。

3. 多引擎防护体系：

通过使用机器学习方法的攻击检测机制，对海量的攻击样本进行学习构建模型，引入误报率更低、性能更优

的智能检测引擎，降低传统规则防护难以调和的漏报率和误报率。

提供灵活配置、高度细化的规则类及算法型的核心防护引擎，支持灵活的检测对象定义、多种检测条件的逻辑组合、提供贴近于自然语言支持复杂场景描述的自定义规则等众多机制，保证规则的精准、有效。

提供智能补丁引擎，支持绿盟 WAF 与 WVSS 产品自动联动，实现检测与防护安全闭环管理。针对 WVSS 生成检测报告，WAF 自动生成“防护策略”，提供小时级安全保障能力，持续循环改善网站安全。

提供自学习引擎，引入的自学习 + 白名单机制，有效增强了 0day 漏洞的防护能力和精准防护能力。基于统计学方法的自学习技术，分析用户行为和指定 URL 的 HTTP 请求参数，协助管理员构建正常的业务流量模型，形成白名单规则。

4. DDoS 联合防护：

支持 Web 应用防火墙与绿盟科技抗拒绝服务系统（ADS）联动，解决了 WAF 上游带宽被大流量 DDoS 攻击堵死且自身防护能力已无法满足清洗需求的问题，并能根据攻击流量大小自动判断和控制清洗层次，按需、合理调用 WAF 自身 Anti-DDoS 模块和清洗中心的清洗资源，是绿盟科技 Web 安全解决方案中重要的一环。

5. 运营支撑：

WAF with MSS 服务：面向客户，实现将客户本地的 WAF 设备与绿盟安全云对接和同步，提供远程的 IT 安全检测与管理服务，进行 WAF 设备运维与安全运维支撑。

6. 攻击取证：

主要用于攻击事件事后分析、攻击场景还原，以及串联用户所有 WEB 操作，进行用户行为研究，了解用户操作背后是否隐藏了潜在的攻击动机。



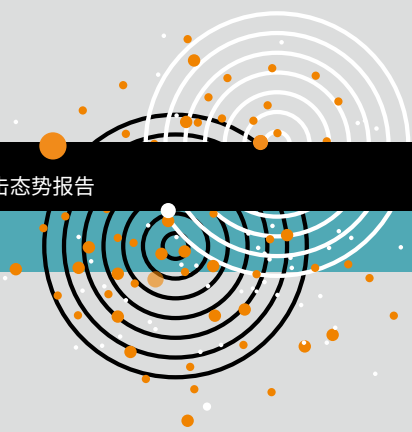
作者

中国电信云堤 张敏 常力元 刘紫千 刘长波 陈林 佟欣哲

绿盟科技 潘文欣 彭畅 李凯 陈俊 詹圣君 何坤

编辑

绿盟科技 郝明 黄柱 (平面设计)



2017 DDoS 与 Web 应用攻击态势报告

