

2017上半年



DDoS 与 Web 应用攻击

态势报告

Web 应用攻击



DDoS 攻击

绿盟科技官方微信





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

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。

1. 前言	1
2. 2017 年上半年 DDoS 攻击关键趋势	2
3. 2017 年上半年 Web 应用攻击态势概览	3
4. 2017 年上半年 DDoS 攻击趋势	4
4.1 DDoS 攻击次数和流量峰值情况	5
4.1.1 DDoS 攻击次数和攻击流量	5
4.1.2 攻击峰值各区间分布	5
4.1.3 单次攻击最高 / 平均峰值	7
4.2 DDoS 攻击类型分析	7
4.2.1 各攻击类型次数和流量占比	7
4.2.2 攻击类型各流量区间分布	8
4.3 反射攻击活动放缓	10
4.3.1 反射攻击次数和流量占比	10
4.3.2 反射攻击趋势分析	10
4.3.3 NTP 活跃反射器分布	12
4.4 DDoS 攻击持续时间	13
4.4.1 DDoS 攻击持续时间占比	13
4.4.2 DDoS 攻击持续时间变化趋势	14
4.4.3 DDoS 攻击持续时间与被攻击频次	15
4.5 DDoS 攻击源 / 目标地理分布	15
4.5.1 全球 DDoS 攻击源国家分布	15
4.5.2 中国 DDoS 攻击源省份分布	16
4.5.3 全球 DDoS 攻击目标国家分布	17
4.5.4 中国 DDoS 攻击目标省份分布	17
4.6 僵尸网络	18
4.6.1 中国 BotMaster 省份分布	18
4.6.2 中国 Bot 端省份分布	18
4.6.3 物联网僵尸网络	19
5. 2017 上半年 Web 应用攻击态势	21
5.1 Web 应用攻击类型分析	22
5.2 被攻击与未被攻击站点比例	23
5.3 攻击源情况分析	23
5.3.1 攻击源 IP 攻击广度与其 IP 信誉	23
5.3.2 攻击源主机数所在中国地区占比	24
5.4 Web 应用各类攻击方式分析	25
5.4.1 注入类攻击常见 Payload 注入位置	25
5.4.2 利用已知 Web 漏洞的攻击	26
5.4.3 SQL 注入攻击常见 Payload	27
5.4.4 路径穿越攻击常见 Payload	28
5.4.5 XSS 攻击常见 Payload	29
5.4.6 远程命令执行攻击常见 Payload	29
5.4.7 恶意扫描常见扫描器 Top 统计	30
5.4.8 非法文件上传类型 Top 统计	31
5.5 Struts2 CVE-2017-5638 高危漏洞	31
5.5.1 攻击次数趋势	33
5.5.2 受影响行业和地域	34

DDoS 特性

上升

2017 上半年对比 2016 下半年平均攻击峰值（平均攻击规模）
增长 **47.5%**

2017 Q2 环比 Q1，攻击总次数增长 **39.3%**，攻击总流量
增长 10.3%。

2017 Q2 环比 Q1，300Gbps 以上超大流量攻击呈上升趋势，
增幅 **720%**

主导

SYN Flood 攻击总流量占主导地位，占比 **56%**

SYN Flood 大流量攻击明显增多，在 300Gbps 的
超大流量攻击中占比 **91.3%**

短时攻击占主导位置，占比 **53.5%**

下降

2017 Q2 环比 Q1，小流量（峰值 <5Gbps）
攻击占比下降 **46** 个百分点

反射攻击 活动放缓，活跃反射器
数量呈下降趋势

物联网僵尸网络 扫描活动
降温

Web 特性

最多的攻击类别：

- SQL 注入攻击 + 已知 Web 漏洞攻击

常见注入类攻击：

- 攻击插入位置为 URL 中的参数列表
+ Cookie 字段

威胁情报可探知：

- 攻击源 IP 越活跃，其在 NTI 中的信
誉为高威胁的概率越大

及时修复已知漏洞， 可降低网站面临的安全威胁



1. 前言

从攻击实施的难易程度来看，Web 应用层攻击对攻击者的 Web 相关知识和技能要求更高，但正因为 DDoS 攻击技术门槛低，也使得 DDoS 攻击越发猖獗。从对攻击目标的威胁严重程度来看，DDoS 攻击一般是在攻击持续期间对目标网络或系统资源的可用性造成严重影响，具有攻击影响面大、直接损失严重等特点，如：可造成网络大面积瘫痪、各类服务不可用；而 Web 应用层攻击对目标可造成持久的资源可用性、可控性，数据的机密性、完整性的破坏，其影响具有持久性、隐密性等特点。从[很多案例](#)我们看到，很多时候 DDoS 攻击被黑客用作实施 Web 应用攻击的烟雾弹，也即先发起 DDoS 攻击吸引安全团队精力，同时暗地里进行 Web 应用层攻击，最终达到篡改、窃取敏感信息、获取系统控制权限等目的。

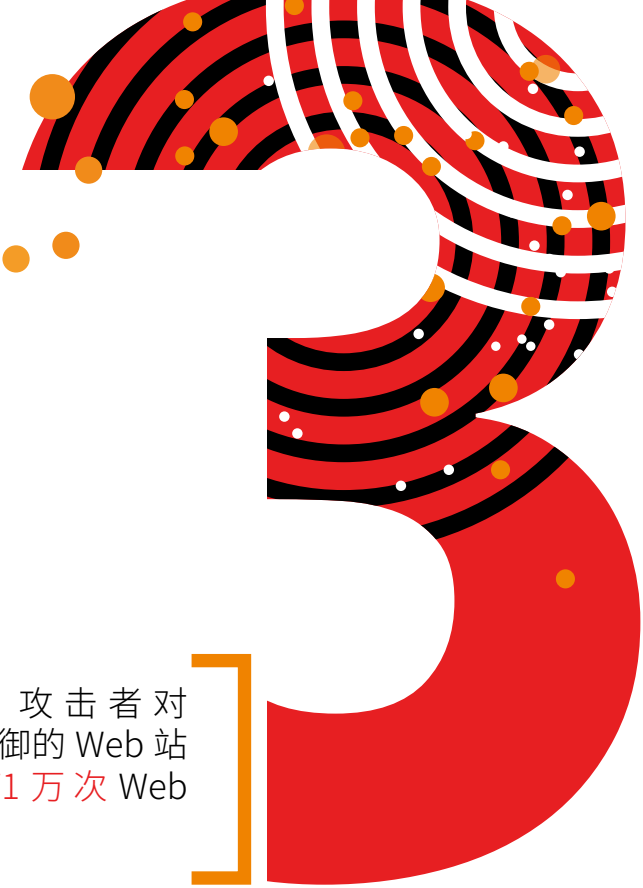
DDoS 攻击和 Web 应用攻击是当今互联网面临的较为突出的**两大安全威胁**。



2017 上半年我们监控到
DDoS 攻击 10 万余次,其中:

2. 2017 年上半年 DDoS 攻击关键趋势

1. DDoS 攻击总次数比 2016 下半年下降 **30%**, 攻击总流量下降 **38.4%**
2. 单次 DDoS 攻击平均峰值为 32Gbps, 相比 2016 年下半年升高 **47.5%**
3. 单次攻击平均攻击时长为 9 小时, 相比 2016 年下半年呈 **回升趋势**, 增长 28.6%, 但略低于 2016 年上半年水平
4. 有 **10.6%** 的目标 IP 曾经遭受过长达 24 小时以上的攻击, 其中 38.3% 曾在 1 个季度内遭受过 2 次或更多次 DDoS 攻击, 最高达到 20 次 / 季度
5. 300Gbps 的超大流量 DDoS 攻击呈 **增长趋势**, 共发生 46 次, Q2 比 Q1 增加了 720%
6. SYN Flood 大流量攻击明显增多, 在攻击峰值大于 300Gbps 的超大流量攻击中占比高达 **91.3%**, 相比去年增长 52.3 个百分点
7. 反射攻击整体活动放缓, Q2 总流量比 Q1 下降 80%, 其中最明显的是 DNS 反射攻击, 总流量下降 **301%**



2017 上半年，攻击者对 NSFOCUS 所防御的 Web 站点发起了 2,771 万次 Web 应用层攻击：

3. 2017 年上半年 Web 应用攻击态势概览

1. 有 82% 的 Web 站点曾遭受 Web 应用攻击，单个站点日平均被攻击次数为 21 次
2. 有 19.6% 的攻击源 IP 曾经对 2 个及以上的 Web 站点发起过攻击，这部分攻击源 IP 中有 74.3% 在绿盟科技威胁情报中心（NTI）中有不良 IP 信誉记录，且被标识为中、高危的占比 74.2%
3. 有 79.3% 的网站遭受的攻击为已知 Web 漏洞攻击，其中利用率最高的漏洞为 Struts2 相关漏洞，占全部已知 Web 漏洞攻击的 58.7%
4. SQL 注入攻击占比 40.8%，从攻击 Payload Top10 来看，大部分攻击发生在攻击初期阶段，主要是试探网站是否存在注入漏洞
5. Struts2 CVE-2017-5638 高危漏洞爆发一周内平均每天发生 2,771 次攻击，教育（23%）、政府（19%）、金融（17%）、互联网（10%）受该漏洞影响较大



反射攻击活动放缓，物联网僵尸网络扫描活动降温，基于 windows 和数据库系统的僵尸网络表现抢眼。

4. 2017 年上半年 DDoS 攻击趋势

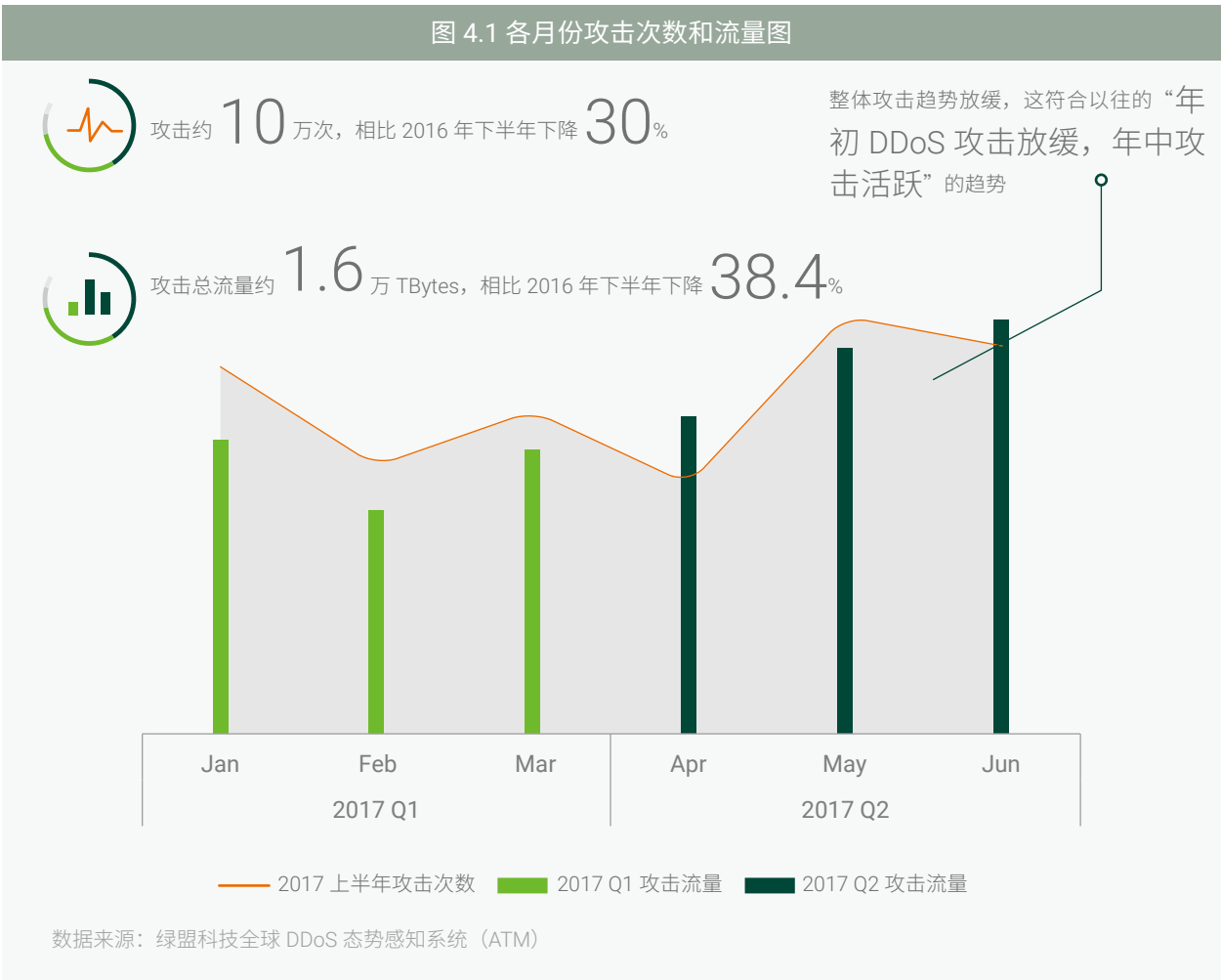
4.1 DDoS 攻击次数和流量峰值情况	5
4.2 DDoS 攻击类型分析	7
4.3 反射攻击活动放缓	10
4.4 DDoS 攻击持续时间	13
4.5 DDoS 攻击源 / 目标地理分布	15
4.6 僵尸网络	18

4.1 DDoS 攻击次数和流量峰值情况

4.1.1 DDoS 攻击次数和攻击流量

2017 年上半年，我们监控到 DDoS 攻击约 10 万次，相比 2016 年下半年下降 30%；攻击总流量约 1.6 万 TBytes，相比 2016 年下半年下降 38.4%，我们认为，这与今年年初开始反射攻击活动减少有关。

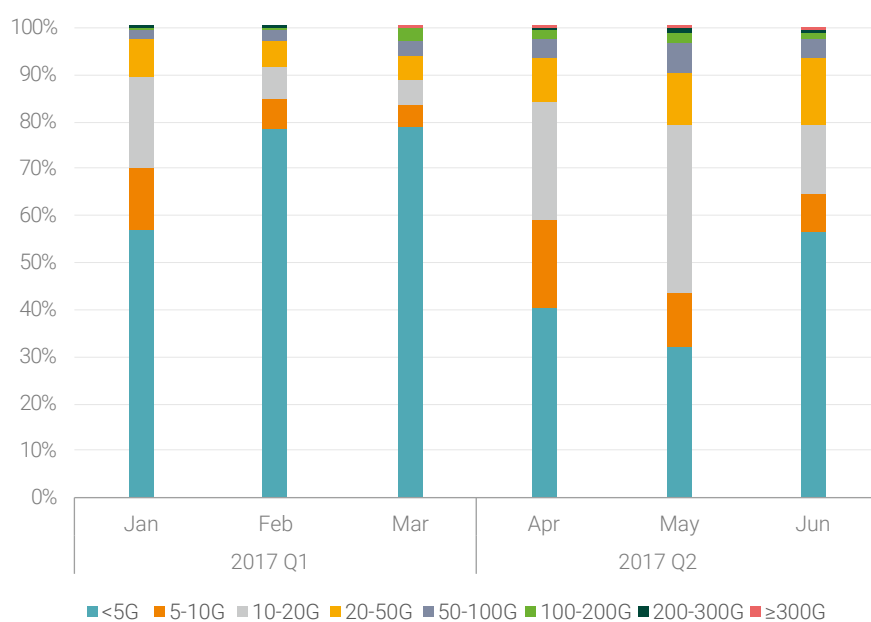
2017 上半年相比 2016 年整体攻击趋势放缓，2017 Q2 季度有回升的趋势。Q2 季度环比 Q1 季度总攻击次数增长 39.3%，总流量增长 10.3%。这符合以往的“年初 DDoS 攻击放缓，年中攻击活跃”的趋势。



4.1.2 攻击峰值各区间分布

2017 Q1 季度，DDoS 攻击仍然以峰值在 5Gbps 以下的小流量攻击为主，这部分攻击占全部攻击峰值区间的 73.3%。相比 Q1 季度，Q2 季度攻击峰值在 5Gbps 以下的小流量攻击明显减少，占比为 39.8%，而峰值在 5G 以上的攻击占比均有所上升，尤其是 300G 以上的攻击明显增加。

图 4.2 攻击峰值区间各季度占比图

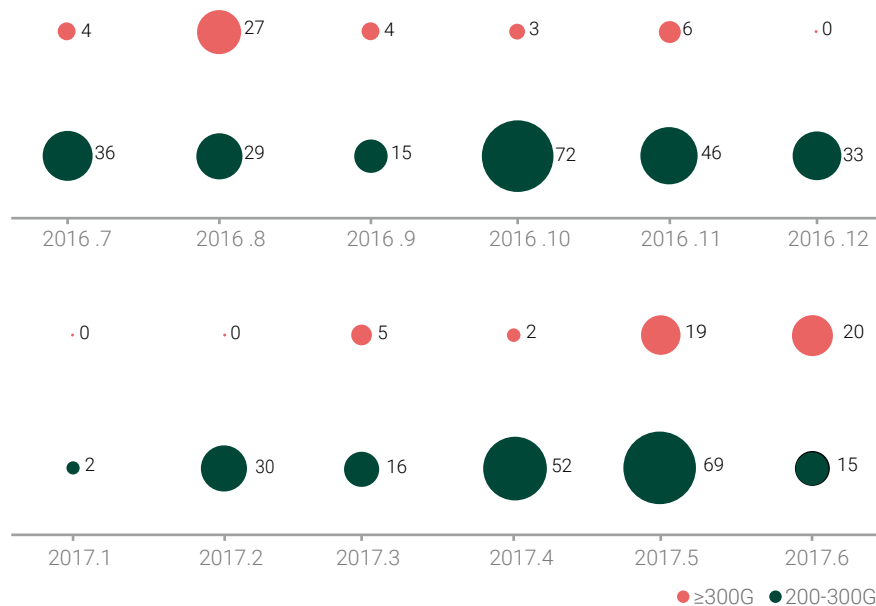


数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

2017 上半年，攻击峰值在 200Gbps 以上的大流量攻击共发生 230 次，相比 2016 下半年下降 16.4%。

2017 上半年攻击总数量虽有减少，但峰值大于 300Gbps 的超大流量攻击呈增长趋势，共发生 46 次，相比 2016 年下半年增长 4.5%，2017 Q2 相比 Q1 增加了 720%。

图 4.3 各月份大流量攻击次数



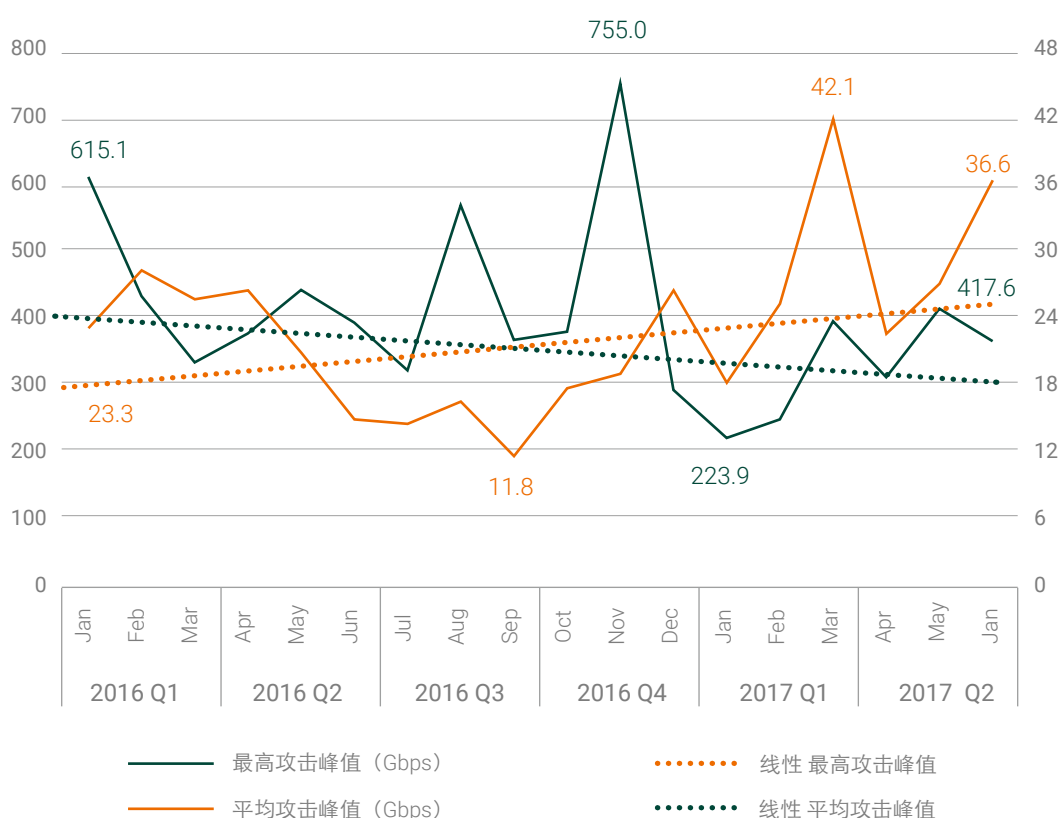
数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

4.1.3 单次攻击最高 / 平均峰值

2016 至 2017 上半年单次攻击的平均攻击峰值呈整体上升的趋势，在 2017 年 3 月份创新高，达 42.1Gbps。虽然 2017 上半年攻击总量减少，但 Q2 季度的大流量攻击拉高了整体的平均攻击峰值走势。

从单次攻击峰值来看，2017 上半年单次最高攻击峰值为 418Gbps，相比 2016 年整体呈下降趋势；单独看 2017 上半年，最高攻击峰值有回升的趋势。

图 4.4 各月份攻击峰值趋势图



数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

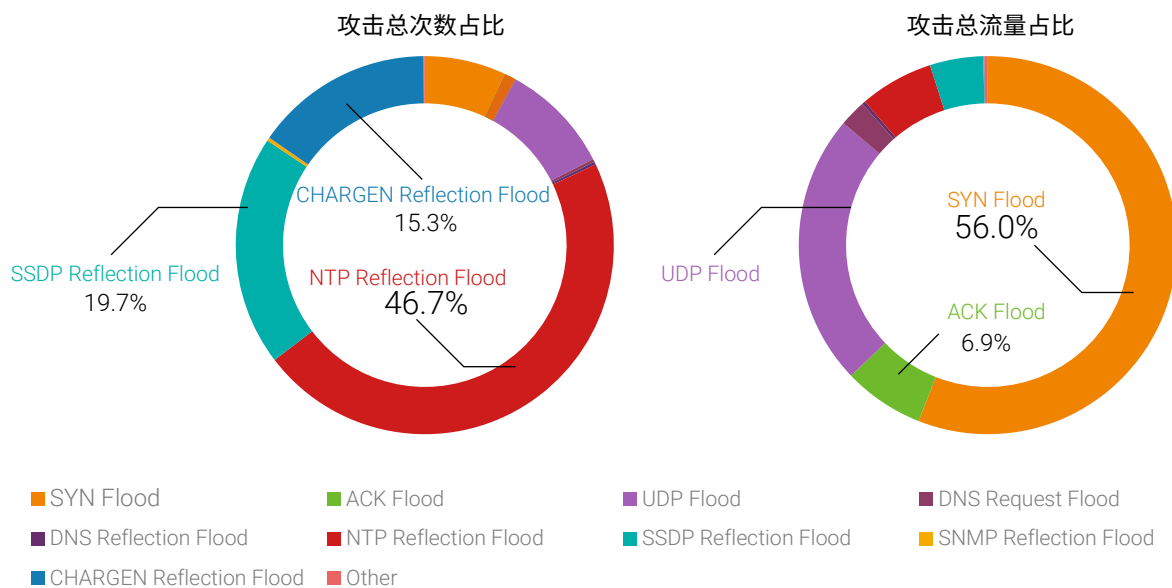
4.2 DDoS 攻击类型分析

4.2.1 各攻击类型次数和流量占比

2017 上半年，Top 3（按攻击次数统计）DDoS 攻击类型分别为 NTP Reflection Flood、SSDP Reflection Flood 和 CHARGEN Reflection Flood，均为反射类型，Top 3 合计占比达 81.7%。但反射攻击整体活动有所放缓，具体分析请见第 4.3 节。

从各类攻击流量大小占比来看，SYN Flood 和 UDP Flood 依然是流量最大的两种攻击类型，SYN Flood 流量占比达 56%，UDP Flood 流量占比为 23.3%。与 2016 年相比，SYN Flood 流量占比明显增多，上升 7 个百分点，UDP Flood 流量占比明显减少，下降 6.3 个百分点。这一趋势在大流量攻击中体现尤其明显，详见下一小节分析。

图 4.5 按 DDoS 攻击总次数 / 总流量统计各类型占比图

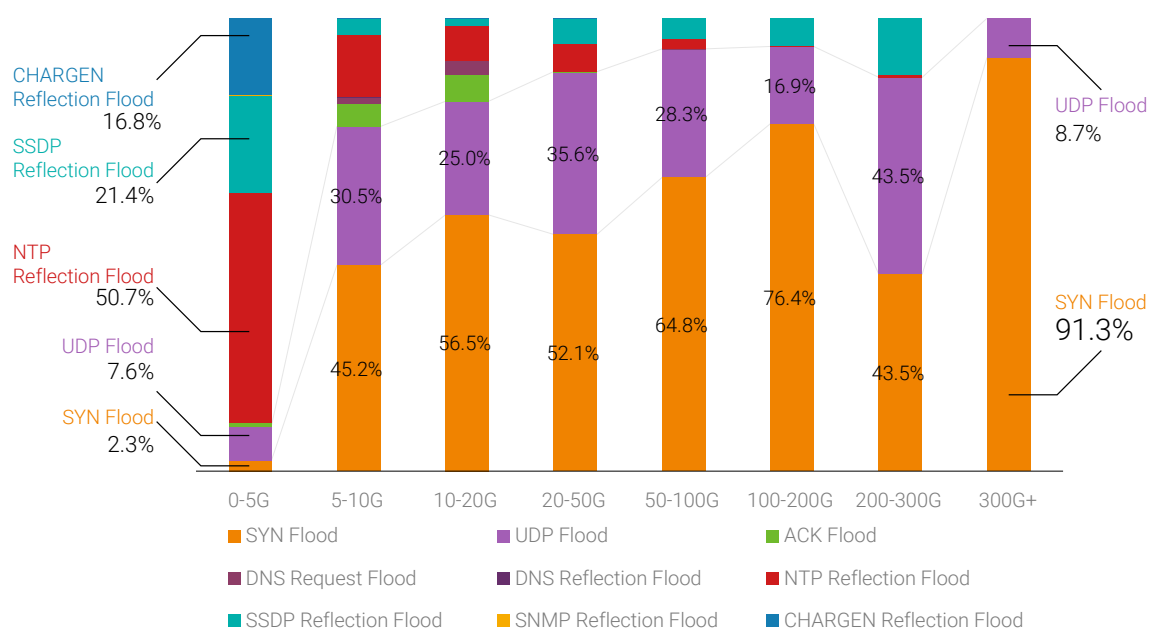


数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

4.2.2 攻击类型各流量区间分布

2017 上半年，特别值得注意的是，SYN Flood 大流量攻击明显增多，其在大流量攻击中占比明显上升。尤其在大于 300Gbps 的超大流量攻击中，SYN Flood 占比高达 91.3%，相比去年增长了 52.3 个百分点。与此同时，UDP Flood 攻击在大于 300Gbps 的超大流量攻击占比 8.7%，相比去年下降 34.9 个百分点。

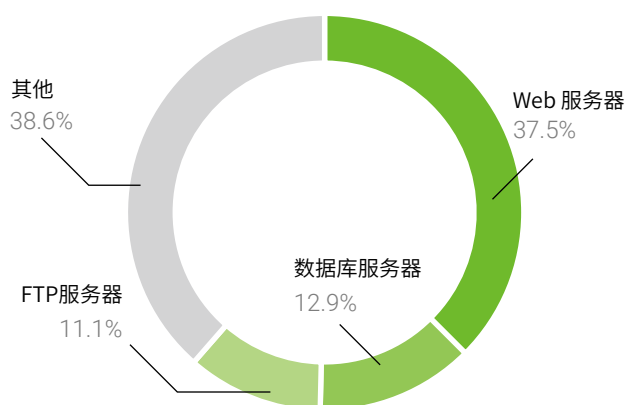
图 4.6 DDoS 攻击类型各流量区间分布图



数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

2017 上半年 TOP 5 攻击峰值事件攻击手段均为 SYN Flood。我们进一步对这五起攻击事件进行溯源分析，发现攻击源大多数为 Web 服务器，占比为 37.5%，其次是数据库系统，占比为 12.9%。一般 Web 服务器或数据库系统会被分配给较大的带宽，所以它们能发出的攻击流量也比普通 PC 要大，可见攻击者一直在寻求创造更高效的 Botnet。

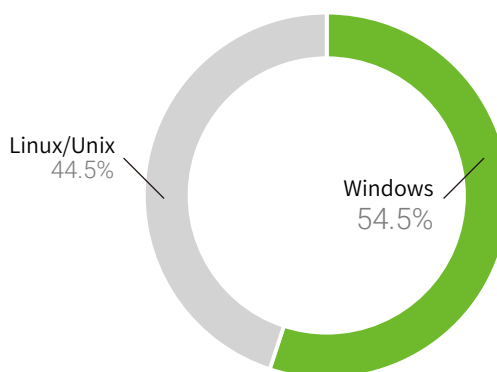
图 4.7 峰值 TOP 5 攻击事件攻击源业务类型统计



数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

这些攻击的攻击源中，有 54.5% 为 Windows 系统，超过 Linux 系统（44.5%）。虽然 Mirai 等物联网僵尸网络大量崛起，但在 2017 上半年的大流量攻击中基于 Windows 系统的攻击凸显，这与这段时间内某些基于 Windows 系统的僵尸网络活动频繁有关。

图 4.8 峰值 TOP 5 攻击事件攻击源系统类型统计



数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

4.3 反射攻击活动放缓

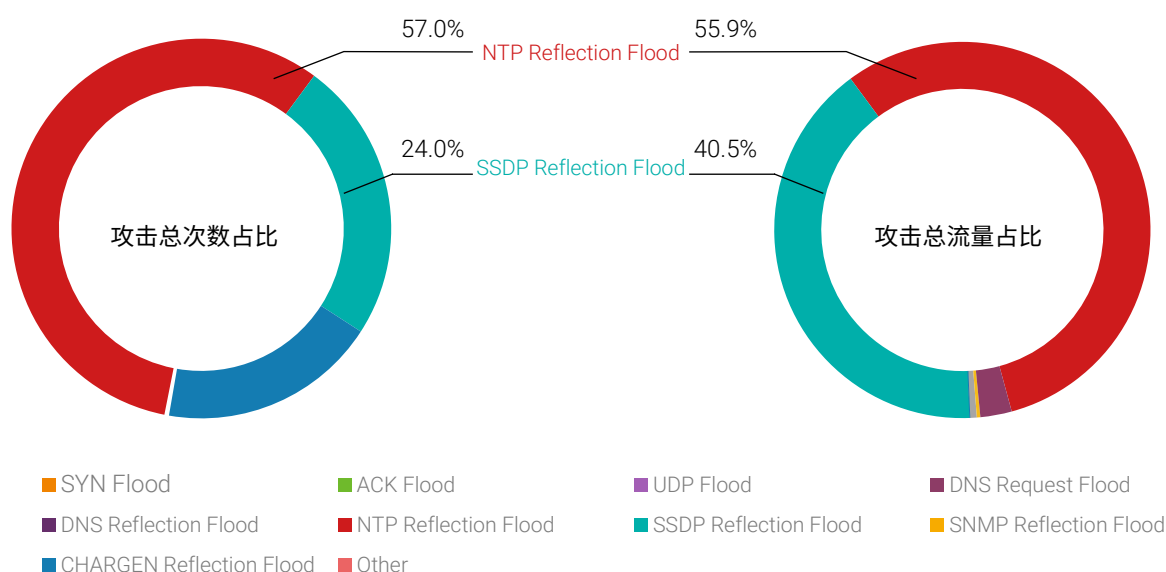
4.3.1 反射攻击次数和流量占比

2017 上半年，攻击次数占比和流量大小占比情况如下图所示。NTP Reflection Flood 和 SSDP Reflection Flood 攻击类型占比较大。

从攻击次数上来看，NTP Reflection Flood 仍霸占首位，攻击次数占全部反射攻击次数的 57%，其次是 SSDP Reflection Flood 和 CHARGEN Reflection Flood，分别占 24%、18.6%。

从攻击流量大小上来看，NTP Reflection Flood 攻击流量占比仍最多，占全部反射攻击流量的 55.9%，其次是 SSDP Reflection Flood，占 40.5%。

图 4.9 各类反射攻击流量、次数占比图



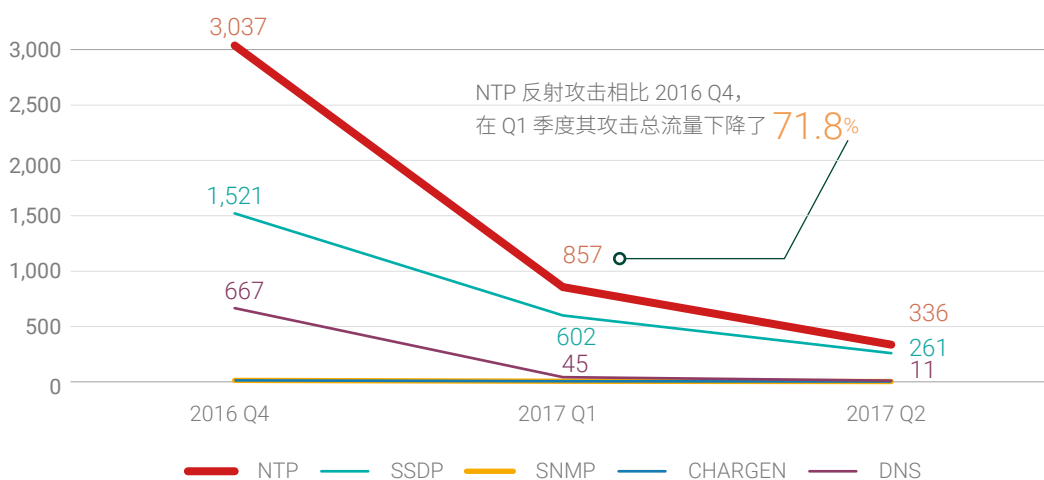
数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

4.3.2 反射攻击趋势分析

2017 上半年，反射类攻击整体活动放缓。从各类反射攻击总流量看，2017 Q1 季度相比 2016 Q4 反射攻击总流量下降 71%；Q2 季度，相比 Q1 季度下降 80%。

其中，NTP 反射攻击相比 2016 Q4，在 Q1 季度其攻击总流量下降了 71.8%，Q2 季度相比 Q1 季度继续下降，下降了 60.8%。DNS 反射攻击下降趋势较明显，Q2 季度比 Q1 季度下降了 301%。

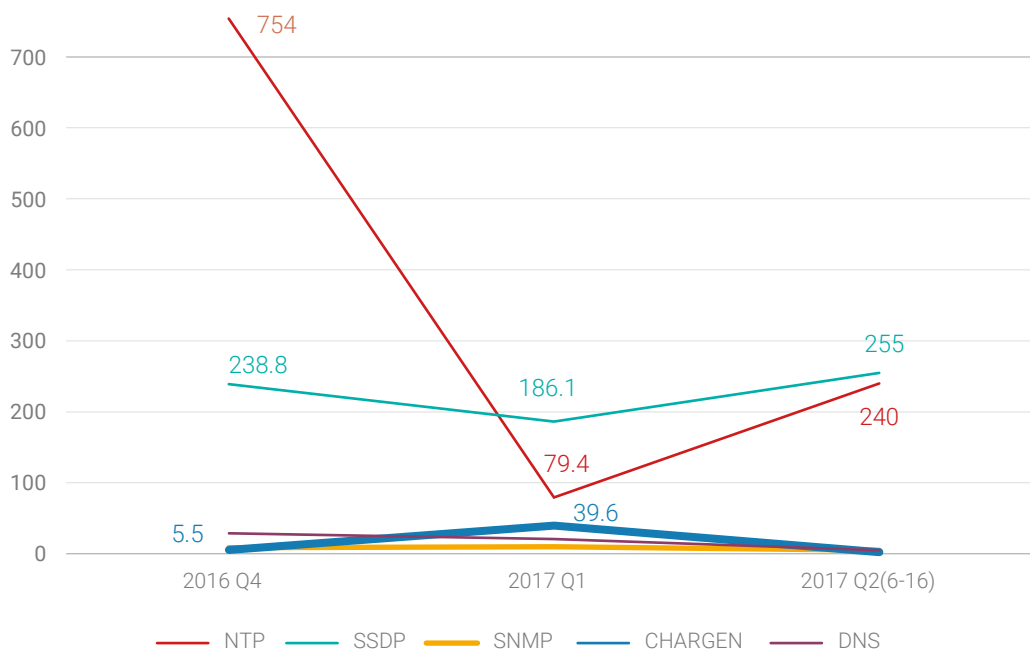
图 4.10 各季度反射攻击总流量趋势（单位：TBytes）



数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

2017 上半年，大部分反射攻击的最高攻击峰值相比 2016 Q4 季度均明显下降。在 Q1 季度，CHARGEN 反射攻击最高攻击峰值从 Q4 的 5.5Gbps 增长到 39.6Gbps；其余反射类均明显下降，虽在 Q2 季度略有增长，但仍然低于 2016 Q4 季度。

图 4.11 各类反射攻击各季度单次攻击最高峰值（单位：Gbps）

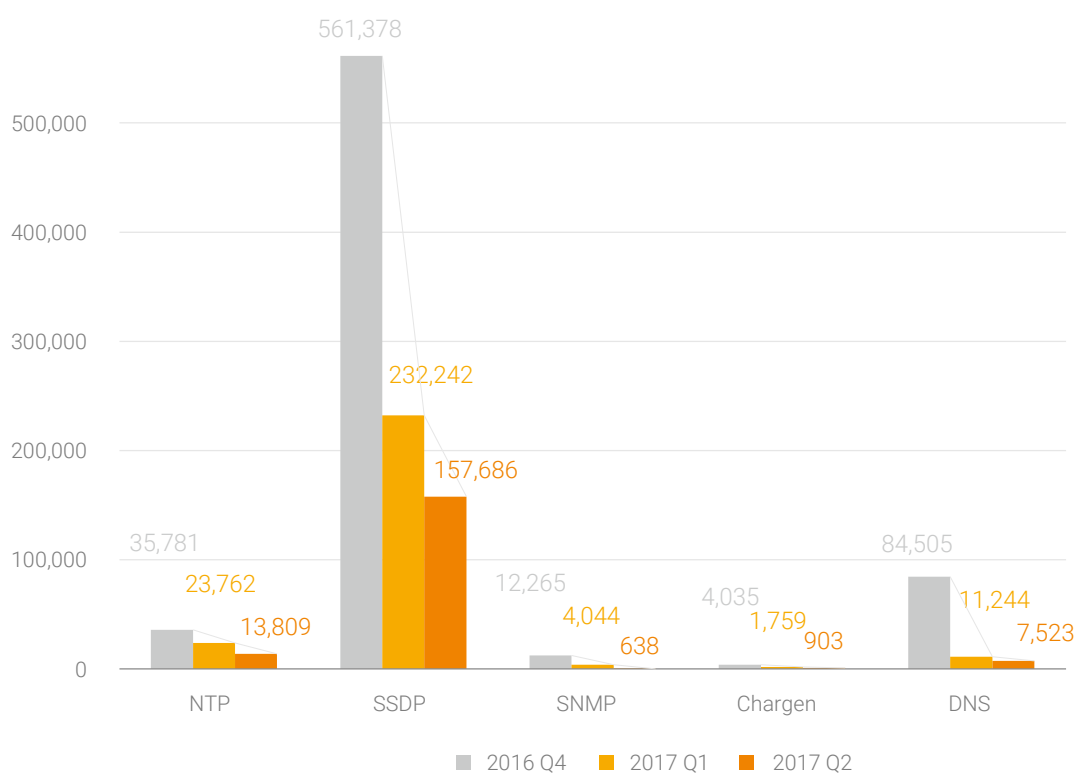


数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

各类反射攻击流量的减少，最高攻击峰值的降低，都跟各类反射攻击在全球范围内可用的反射器数量逐年减少有关。分析有两方面的原因，一方面，各运营商不断对反射攻击进行治理，如实施 [uRPF](#) (Unicast Reverse Path Forwarding)、[BCP 38](#) 等策略；另一方面，很多存在漏洞的服务器都已经被打了补丁或者升级到较新版本，再或者直接关闭了本不需要开启的服务。

我们列出了 2016 年 Q4 到 2017 年 Q2 各类反射攻击活跃反射器数量情况，如下图所示。可以看出，2017 上半年各类反射攻击活跃反射器数量均呈下降趋势。

图 4.12 各类反射攻击各季度活跃反射器数量（单位：个）



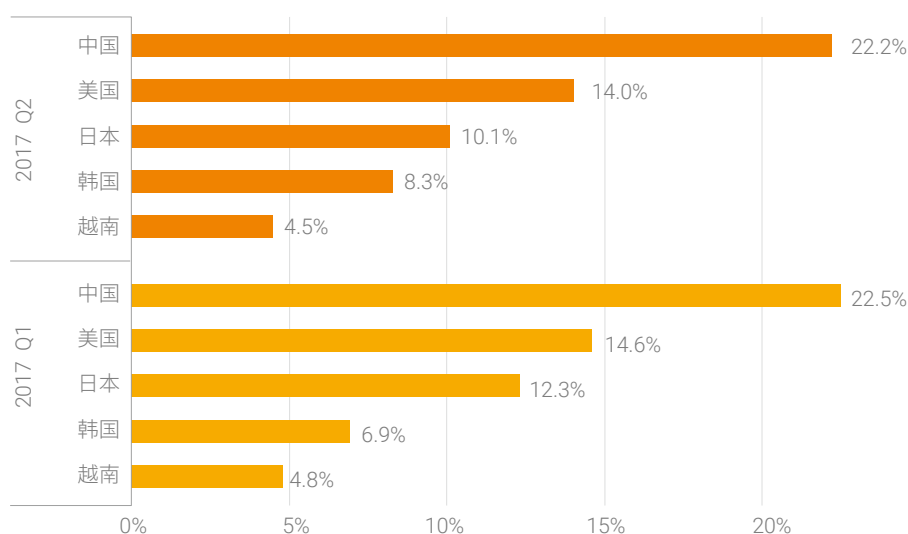
数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

4.3.3 NTP 活跃反射器分布

NTP 的活跃反射器数量虽然远低于 SSDP 的活跃反射器数量，但由于 NTP 反射攻击最高放大倍数可达 550 多倍，是 SSDP 放大倍数（30）的 18.3 倍，因此 NTP 反射攻击的攻击总流量和攻击峰值普遍高于 SSDP 攻击。

我们以 NTP 反射攻击为例，2017 年 Q1 和 Q2 季度，全球活跃 NTP 反射器个数分别为 23762 个和 13809 个；NTP 反射器个数 Top 5 国家如图所示。

图 4.13 活跃 NTP 反射器 Top 5 国家占比



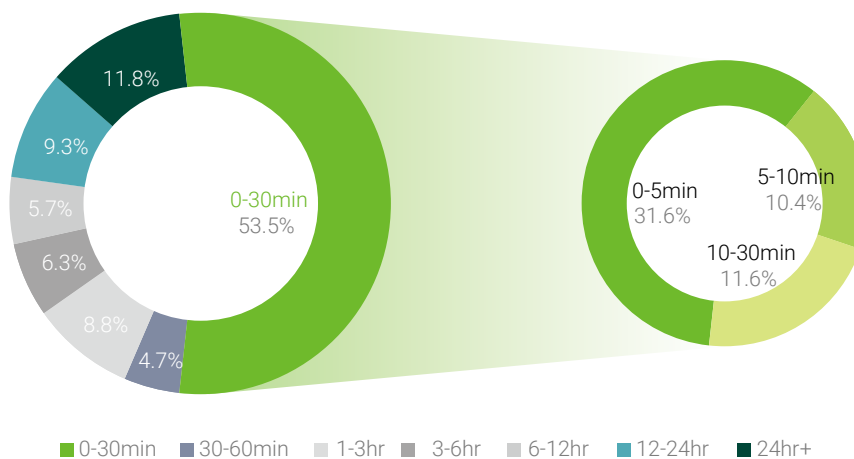
数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

4.4 DDoS 攻击持续时间

4.4.1 DDoS 攻击持续时间占比

2017 上半年，长时攻击增多，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 攻击占全部攻击的一半以上，占 53.5%，相比 2016 下半年下降 8.9 个百分点；攻击时长超过 3 小时的攻击呈增长趋势，总体占比 33%，相比 2016 下半年增长 5.7 个百分点。

图 4.14 攻击持续时间占比图

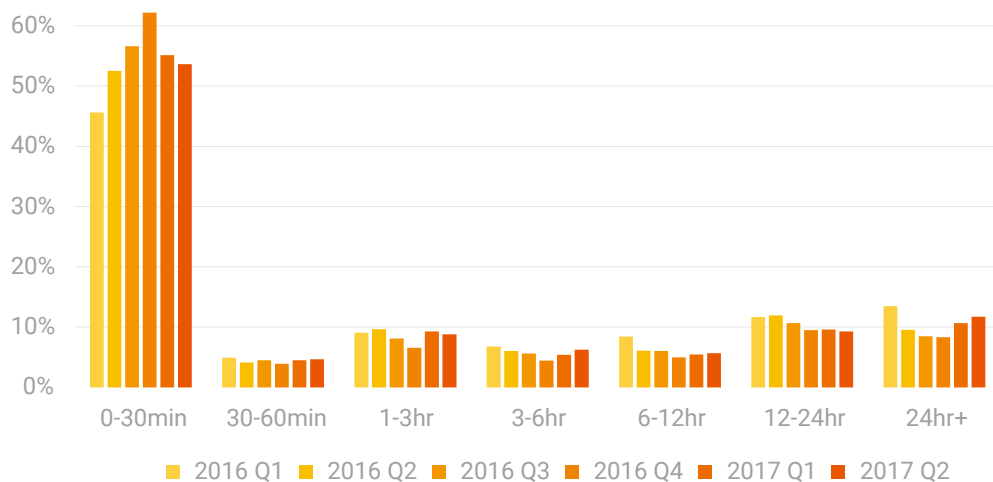


数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

4.4.2 DDoS 攻击持续时间变化趋势

我们已经对攻击持续时间跟踪了较长时间，基本每季度的攻击持续时间分布都差不多，都遵循“30 分钟以内攻击占一半以上，5 分钟以内攻击占 3 成”的规律。

图 4.15 各季度攻击持续时间占比图

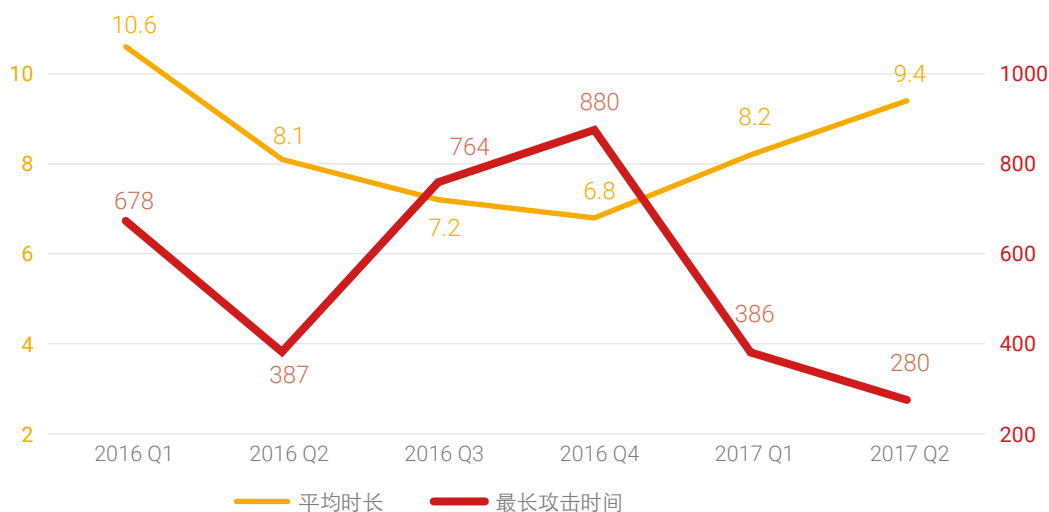


数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

2017 上半年平均攻击时长为 9 小时，相比 2016 下半年增长 28.6%。Q1 和 Q2 季度分别为 8.2 小时和 9.4 小时，呈回升趋势。

2017 上半年各季度最长攻击时长相比 2016 下半年呈下降趋势。2017 上半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)，发生在 Q1 季度，最高攻击峰值达 1.3Tbps，累计总攻击流量达 49TBytes。

图 4.16 各季度平均攻击时长和最长攻击时长 (单位：小时)



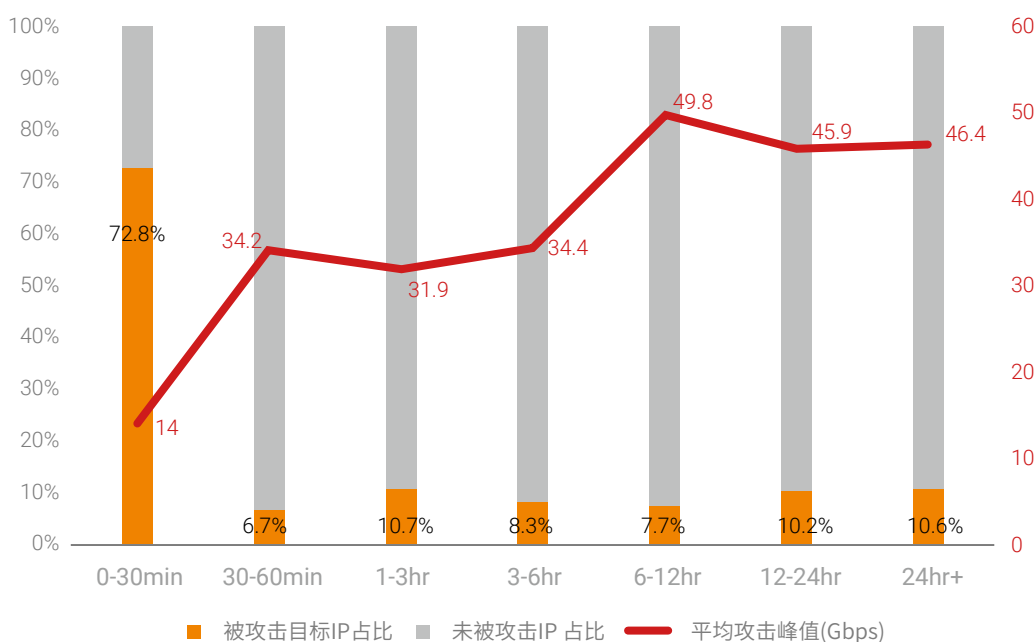
数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

4.4.3 DDoS 攻击持续时间与被攻击频次

我们统计了 2017 年上半年所有被攻击目标 IP 的情况，发现这些 IP 中有 72.8% 的 IP 曾经遭受过 30 分钟以下的 DDoS 攻击，其中 19.1% 曾在单个季度内遭受过 2 次或更多的 DDoS 攻击，遭受 DDoS 攻击最频繁的曾达到 13 次 / 季度；有 10.6% 的 IP 曾经遭受过长达 24 小时以上的攻击，其中 38.3% 曾在单个季度内遭受过 2 次或更多的 DDoS 攻击，最高达到 20 次 / 季度。这表明，攻击者发起持续时间较长的 DDoS 攻击时，对目标进行频繁多次攻击的概率更大。这与攻击者的攻击企图密切相关，追求高利润的攻击者比起那些为了好玩发起攻击的攻击者来说，他们更愿意投入资源发起更持久的 DDoS 攻击，如果一直没能达到攻击的目的或预期的收益，就会再次发起攻击，直至达成目标。

30 分钟以内结束的攻击，平均攻击峰值为 14Gbps，其中有 97.4% 的峰值在 50Gbps 以下，有 83% 的峰值在 20Gbps 以下。长达 24 小时以上的攻击，平均攻击峰值为 46.4Gbps，是 30 分钟以内结束攻击的 3.3 倍，其中有 39.4% 的攻击峰值在 50Gbps 以上，有 19.2% 的攻击峰值在 100Gbps 以上。这个数据表明，短时、频繁的 DDoS 攻击，其攻击峰值普遍低于持续时间较长而频繁的 DDoS 攻击。这与攻击者掌握的攻击资源情况相关，Botnet 数量越多、规模越大，攻击能力越强，攻击者就有能力为了更高的利益多次对目标发起高带宽、更持久的 DDoS 攻击。

图 4.17 不同攻击持续时间中被攻击目标 IP 占比



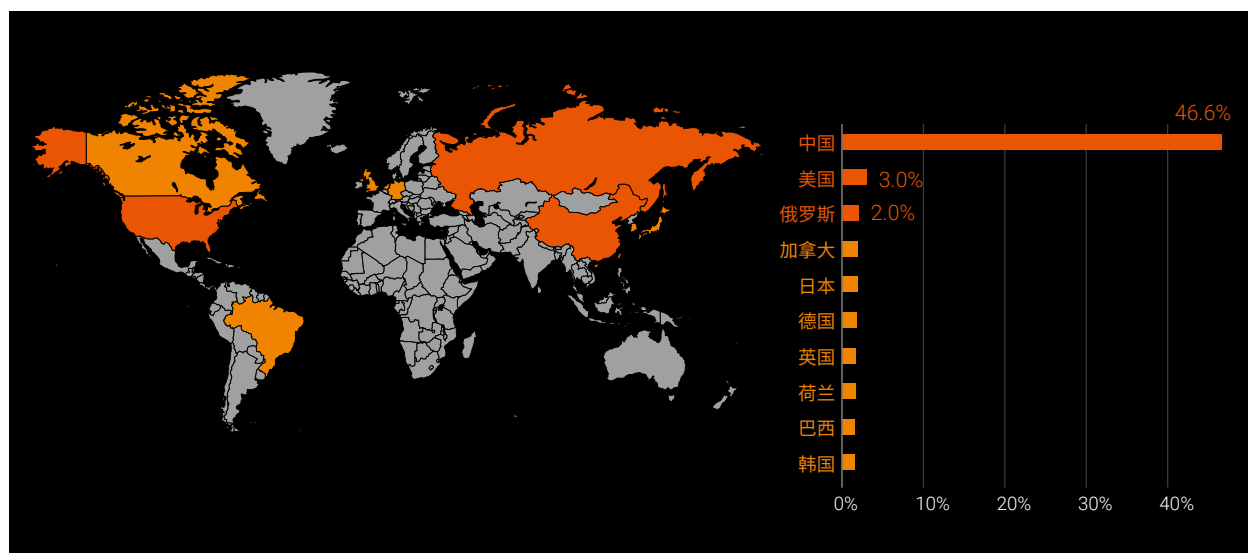
数据来源：绿盟科技全球 DDoS 态势感知系统 (ATM)

4.5 DDoS 攻击源 / 目标地理分布

4.5.1 全球 DDoS 攻击源国家分布

2017 上半年，中国依然是 DDoS 攻击受控攻击源最多的国家，发起攻击次数占全部的 46.6%，其次是美国和俄罗斯，分别占 3.0% 和 2.0%。

图 4.18 全球 DDoS 攻击源国家分布图及 Top 10

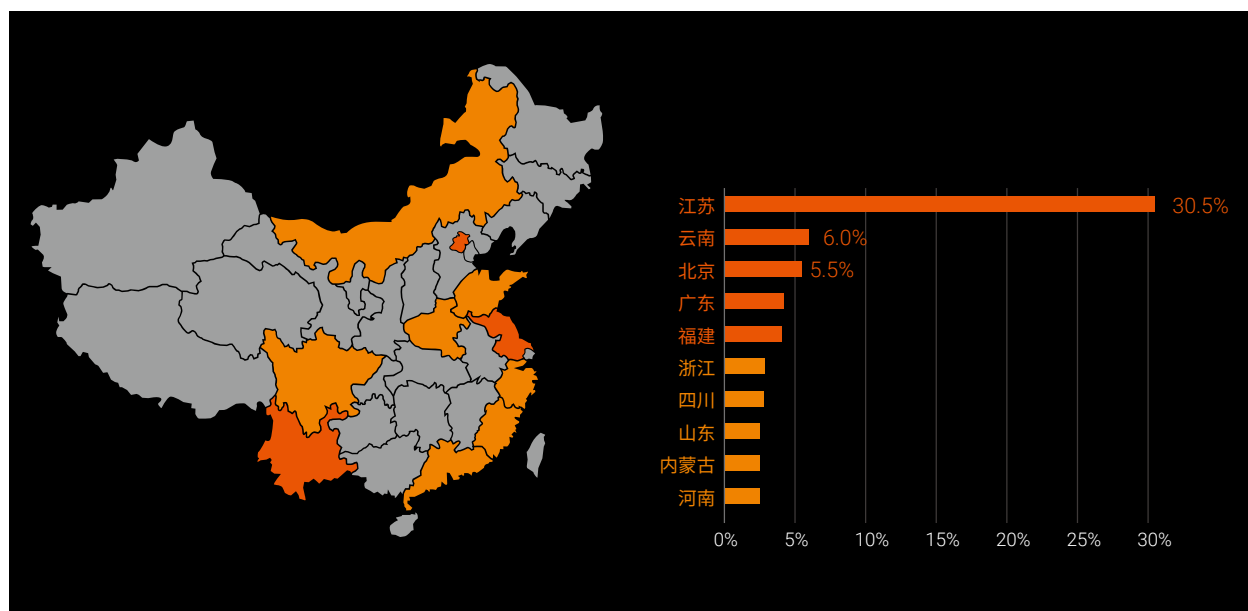


数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

4.5.2 中国 DDoS 攻击源省份分布

2017 上半年，国内发起 DDoS 攻击的省份主要分布在东南沿海地区、内蒙古、四川及云南地区，发起 DDoS 攻击次数的 Top 5 省份分别为江苏、云南、北京、广东、福建，合计占比达 50.3%。

图 4.19 中国 DDoS 攻击源省份分布图及 Top 10

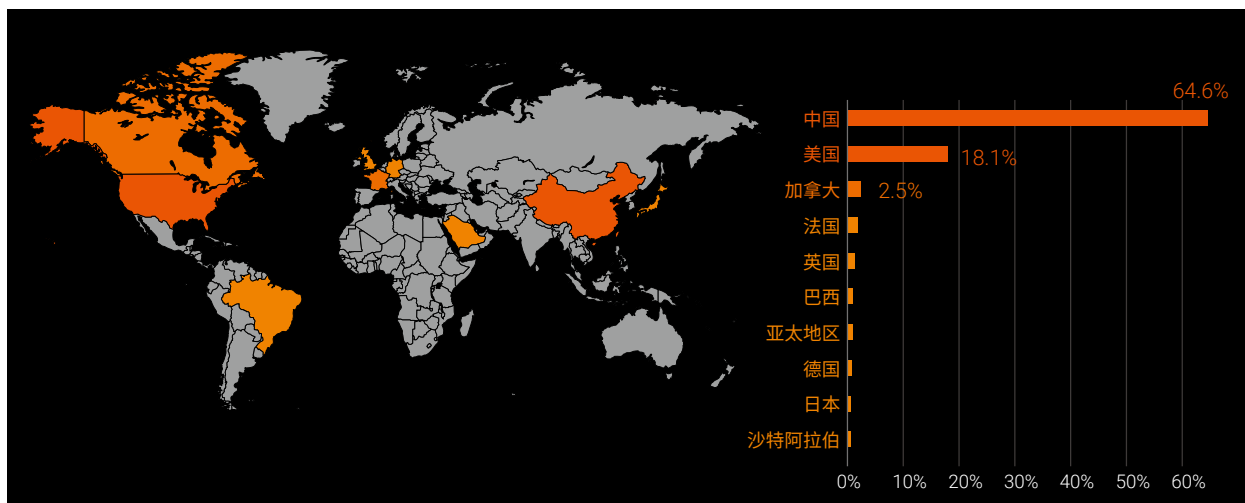


数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

4.5.3 全球 DDoS 攻击目标国家分布

2017 上半年，受攻击最严重的国家是中国，攻击次数占全部被攻击国家的 64.6%，其次是美国和加拿大，分别占 18.1%、2.5%。

图 4.20 全球 DDoS 攻击目标国家分布图及 Top 10

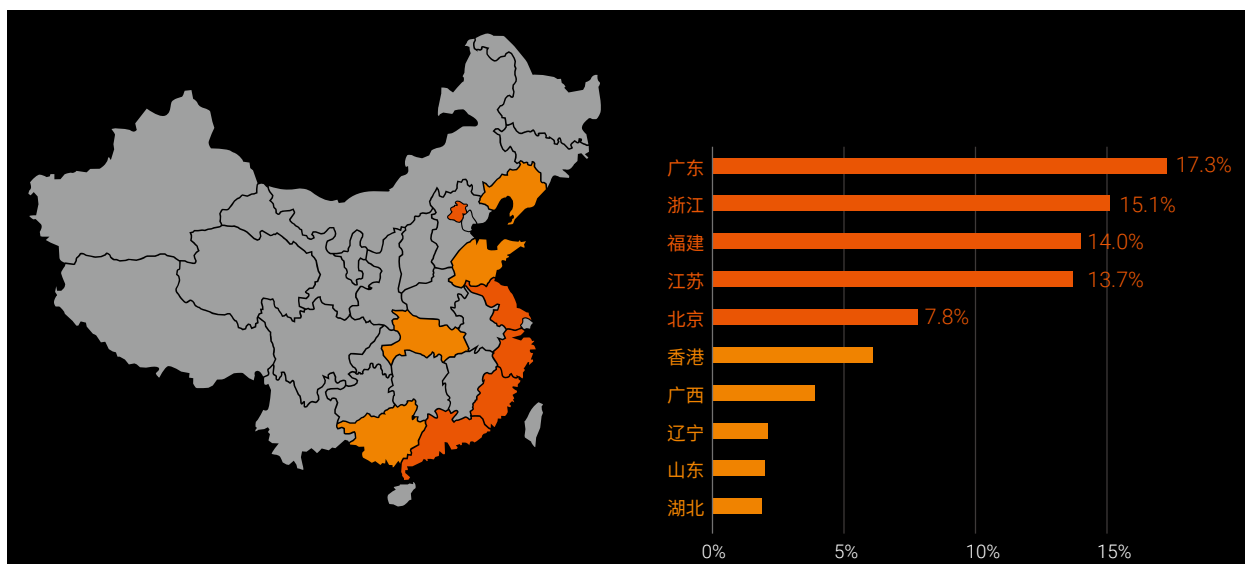


数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

4.5.4 中国 DDoS 攻击目标省份分布

我国中东部沿海地区一直是 DDoS 攻击的高发地。2017 上半年，受攻击严重的 Top 5 省份分别为广东、浙江、福建、江苏、北京，合计占比达 68%。

图 4.21 中国 DDoS 攻击目标省份分布图及 Top 10



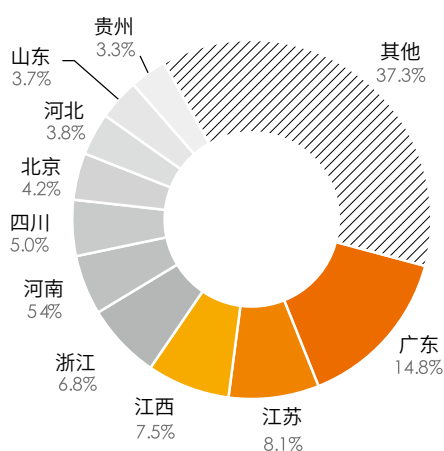
数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

4.6 僵尸网络

4.6.1 中国 BotMaster 省份分布

根据绿盟威胁情报中心和金山安全 2017 上半年的统计，僵尸网络 BotMaster 端主要分布在我国的广东（14.8%）、江苏（8.1%）、江西（7.5%）、浙江（6.8%）、河南（5.4%）等省份。

图 4.22 中国 BotMaster 省份占比 Top 10

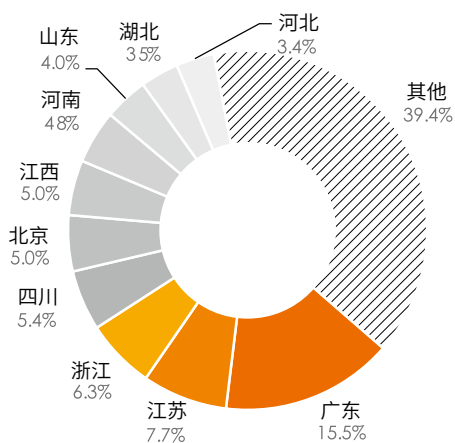


数据来源：绿盟科技威胁情报中心（NTI）和金山安全

4.6.2 中国 Bot 端省份分布

根据绿盟科技威胁情报中心（NTI）和金山安全的统计，僵尸网络 Bot 端主要分布在我国的广东（15.5%）、江苏（7.7%）、浙江（6.3%）、四川（5.4%）、北京（5.0%）等省份。相比 2016 年，江西省排名下降，四川、北京排名上升。

图 4.23 中国 Bot 端省份占比 Top 10



数据来源：绿盟科技威胁情报中心（NTI）和金山安全

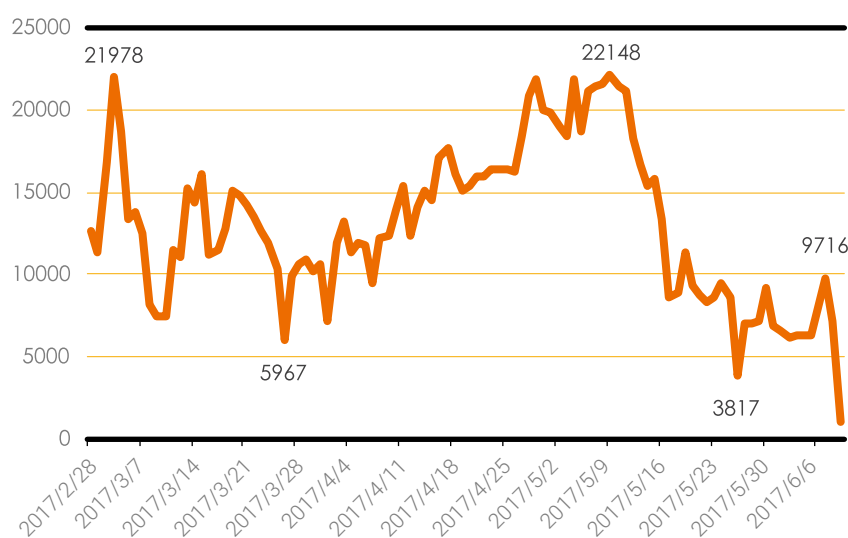
4.6.3 物联网僵尸网络

2016 下半年开始火遍全球的 Mirai，其活动仍在继续，我们的蜜罐系统监控了包括初版和变种 Mirai 的 10 个扫描端口（23、2323、7547、6789、5555、32、23231、3777、2222、19058），Mirai Bot 端扫描次数如图 4.20 所示，平均扫描次数 13193 次 / 日，相比去年下半年扫描活动下降明显。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，关于这点请详见今年年初绿盟科技与电信云堤联合发布的[《2016 年 DDoS 威胁报告》](#)中关于台风 DDoS 物联网僵尸网络的分析。

物联网僵尸网络的种类越发增多，用途也更为广泛。IBM 研究人员最近又发现了 Mirai 僵尸网络新变种，这次它拓展了自己的能力，还包括了比特币挖掘组件。这并不奇怪，在利益的驱使下攻击者总是愿意投入更多的时间、精力去寻求更多、更有效的攻击手段和攻击资源。

图 4.24 Mirai Bot 端扫描趋势图

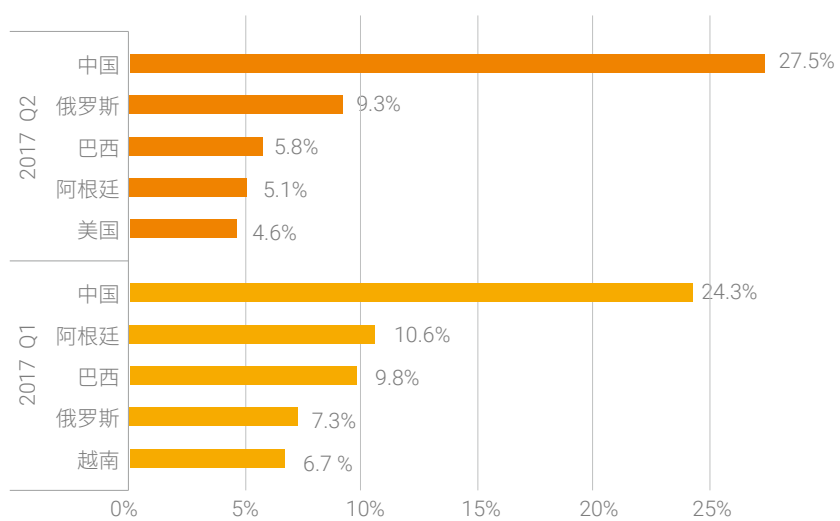


数据来源：绿盟科技威胁情报中心（NTI）

图 4.25 Mirai Bot 端全球分布图



图 4.26 Mirai Bot 端国家占比 Top 10



数据来源：绿盟科技威胁情报中心 (NTI)



有 82% 的网站在 2017 上半年曾遭受 Web 应用攻击，单个站点日平均被攻击次数为 21 次。

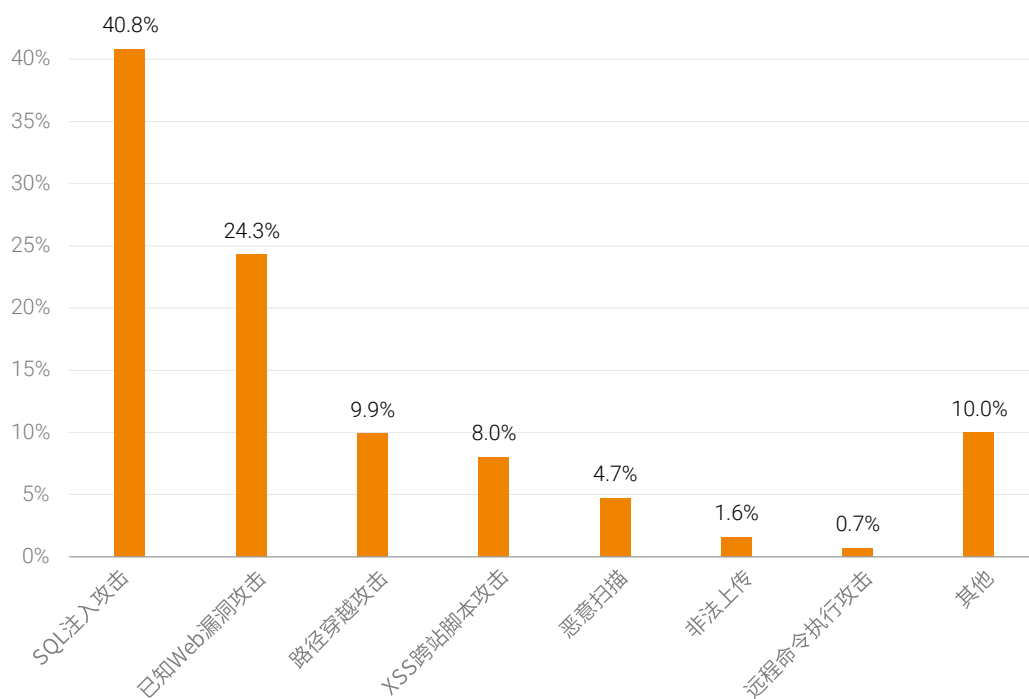
5. 2017 上半年 Web 应用攻击态势

5.1 Web 应用攻击类型分析.....	22
5.2 被攻击与未被攻击站点比例	23
5.3 攻击源情况分析	23
5.4 Web 应用各类攻击方式分析	25
5.5 Struts2 CVE-2017-5638 高危漏洞	31

5.1 Web 应用攻击类型分析

根据我们的统计，2017 上半年，针对 Web 应用的攻击占比如下图所示，其中 SQL 注入攻击占比最高，达 40.8%。其次是已知 Web 漏洞攻击，占比 24.3%。第三位是路径穿越攻击，占比 9.9%。

图 5.1 针对 Web 应用的各类攻击攻击次数占比

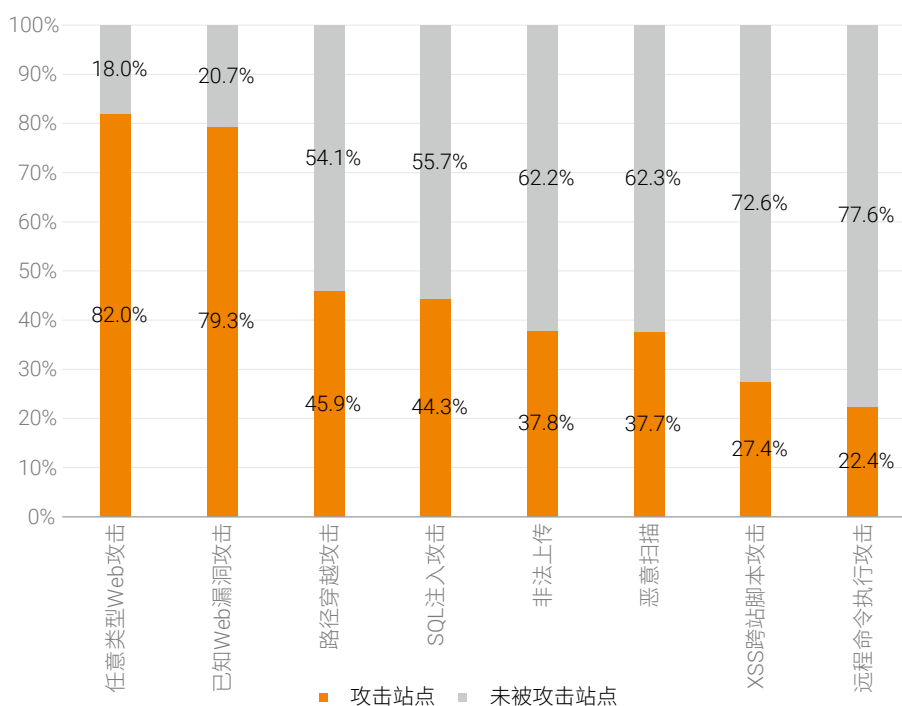


数据来源：绿盟科技可管理安全服务（MSS）

5.2 被攻击与未被攻击站点比例

2017 上半年我们保护的站点中，曾遭受到 Web 应用攻击的站点达到 82%。其中已知 Web 漏洞攻击的攻击范围最广，有 79.3% 的站点遭受了已知 Web 漏洞攻击。其次是路径穿越和 SQL 注入攻击，被攻击站点率分别为 45.9% 和 44.3%。

图 5.2 被攻击与未被攻击的 Web 站点比例



数据来源：绿盟科技可管理安全服务（MSS）

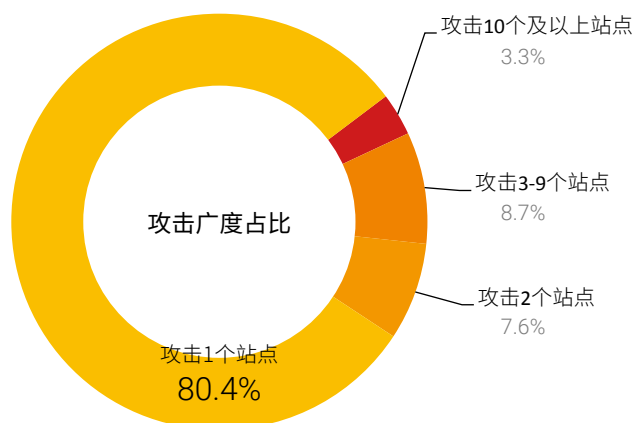
5.3 攻击源情况分析

5.3.1 攻击源 IP 攻击广度与其 IP 信誉

我们对所有攻击源 IP 的攻击广度进行了分析，发现有 19.6% 的 IP 曾经对 2 个及以上的 Web 站点发起过攻击；有 3.3% 的攻击源 IP 曾对 10 个或更多的 Web 站点发起过攻击；只攻击过一个 Web 站点的 IP 占 80.4%。

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，有 12% 的攻击源 IP 在 NTI 上有不良 IP 信誉记录，其中被标识为中、高危的占 55.2%；攻击过多个（2 个及以上）Web 站点的攻击源 IP 中，有 74.3% 的攻击源 IP 在 NTI 上有不良 IP 信誉记录，这部分源中被标识为中、高危的占比为 74.2%。表明攻击源 IP 攻击广度越高，攻击源活跃度越高，在 NTI 上被标识为异常的概率越大，属于高级别威胁的概率也越大。

图 5.3 攻击源 IP 攻击广度

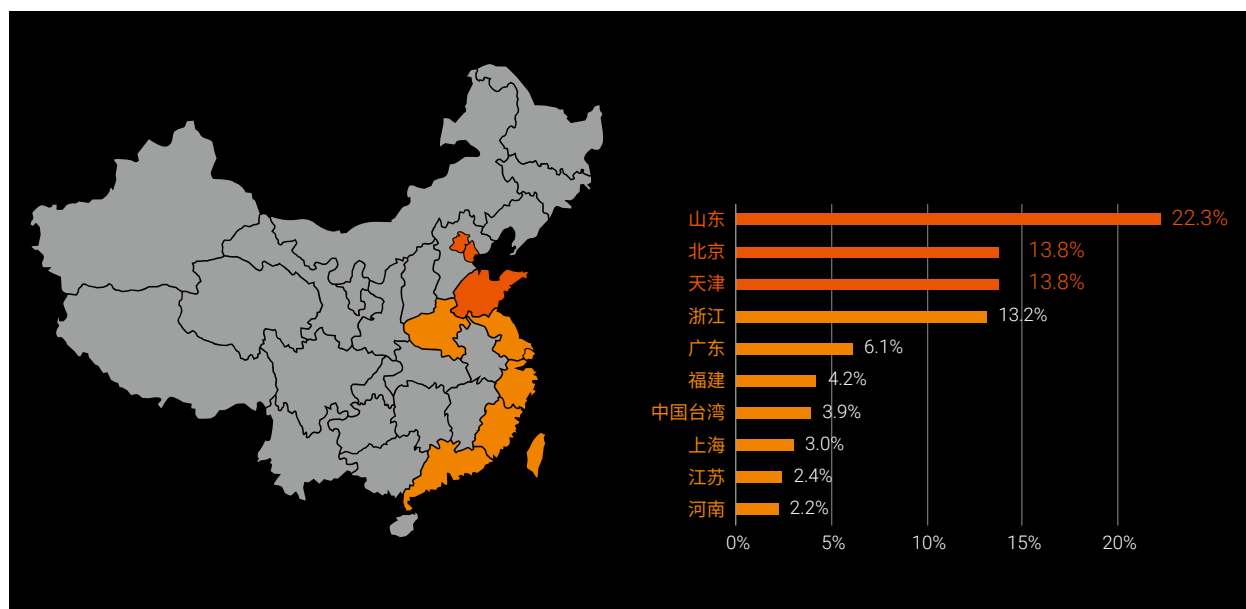


数据来源：绿盟科技威胁情报中心（NTI）

5.3.2 攻击源主机数在中国地区占比

攻击源主机数量在中国地区的分布情况如下图所示，沿海地区和发达地区的攻击源较多，山东、北京、天津排前三，分别占 22.3%、13.8%、13.8%。

图 5.4 攻击源主机数中国地区分布图及 Top 10



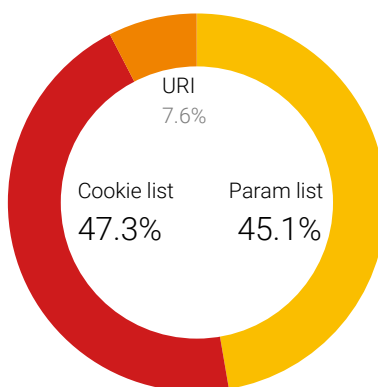
数据来源：绿盟科技可管理安全服务（MSS）

5.4 Web 应用各类攻击方式分析

5.4.1 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、路径穿越、XSS 跨站脚本、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 5.6 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）

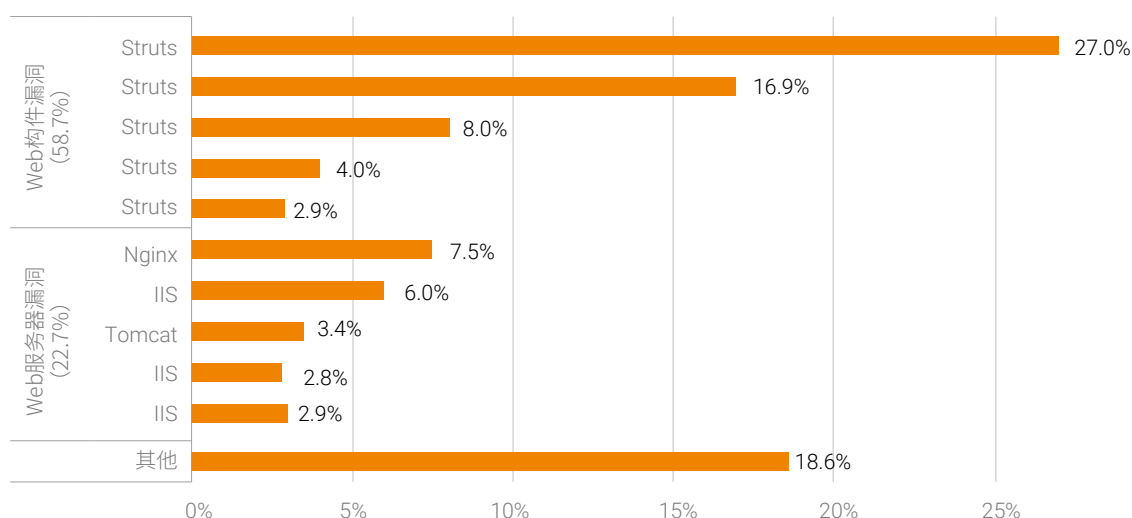
5.4.2 利用已知 Web 漏洞的攻击

在信息化的时代，企业的商业风险与其关键业务的 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[研究表明](#)，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，平均每个 Web 站点包含大概 5-32 个漏洞，大多数的 Web 站点在大部分时间内都是包含漏洞的，如不及时修复已知漏洞，网站将时刻面临巨大安全威胁。

我们这里所说的已知 Web 漏洞包含 Web 服务器漏洞和 Web 构件漏洞。Web 服务器漏洞主要存在于 Web 服务器程序中，如：IIS、Apache、Nginx、Tomcat、lighttpd；Web 构件漏洞主要集中在 Web 应用或重要的 Web 开发框架中，如：Struts、WordPress、phpBB、EmpireCMS、Xoops、Discuz!、ShopEx、vBulletin、phpcms、ECSHOP、DedeCms、phpMyAdmin、PHPWind、Php168 以上几种使用频率比较高的论坛、cms 系统等 Web 程序。

2017 上半年，针对 Web 应用发起的攻击中利用已知 Web 相关漏洞的 Top 10 如下图所示，我们分类进行展示：

图 5.7 Web 应用攻击利用漏洞 Top 10



数据来源：绿盟科技可管理安全服务 (MSS)

这些漏洞中，1 个为中级漏洞，其余 9 个均为高危漏洞。很多漏洞都是几年前的漏洞，但利用率仍然很高。

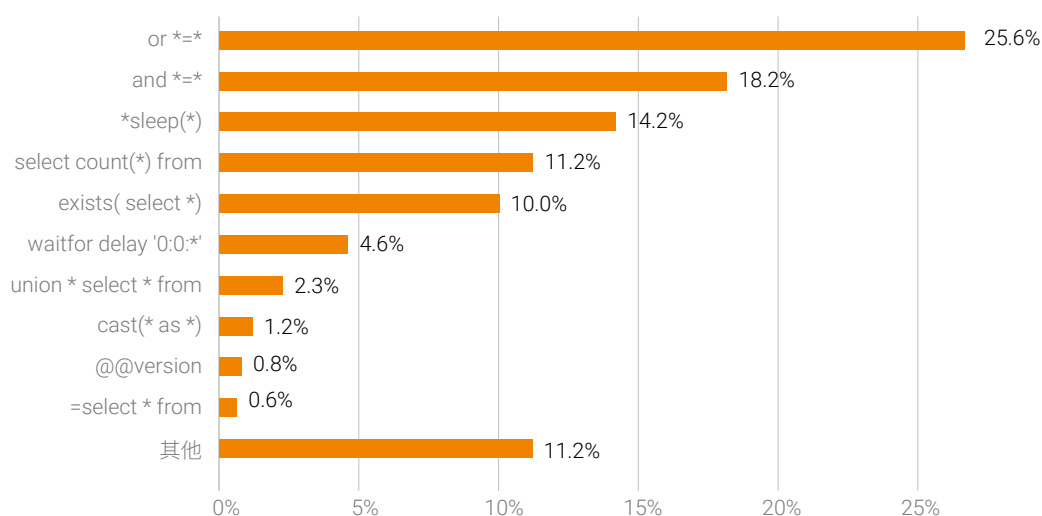
从图中也可看出，今年上半年针对 Web 应用的攻击利用已知漏洞 Top 10 中，Apache Struts2 相关漏洞是被利用最多的漏洞，占全部已知漏洞 Top10 的 58.7%。Apache Struts2 是世界上最流行的 Java Web 服务器框架之一，被广泛用于政府、企业组织、金融等行业的门户网站的底层模版建设，一旦出现漏洞，影响甚广。今年上半年 3 月 7 日爆发 Apache Struts2 CVE-2017-5638 的高危漏洞 (CVSS 评分 10)，占全部已知漏洞攻击的 8%，该漏洞攻击及影响面分析可见第 5.5 节。

5.4.3 SQL 注入攻击常见 Payload

所谓 SQL 注入，是通过把 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。具体来说，它是利用现有应用程序，将恶意的 SQL 命令注入到后台数据库引擎执行，它可以通过在 Web 表单中输入恶意 SQL 语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行 SQL 语句。

其主要原因是程序没有细致地过滤用户输入的数据，致使非法数据侵入系统。2017 上半年，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 5.8 SQL 注入常见攻击 Payload Top 10



数据来源：绿盟科技可管理安全服务（MSS）

1. or *=* 的插入语句最为常用，占全部攻击 Payload 的 25.6%，比如：or 53=3, OR 53=35, OR 53=4 等均合并到此项中。其次是 and *=*，占比达 18.2%，例如：and 1=1, and 1=2 等都合并到这个项中。
2. *sleep(*) 占比 14.2%，例如：(sleep(2);--, select pg_sleep(5)-- 等类似的语句都合并在这个选项中，常用于 MySQL、PostgreSQL 数据库基于时间的盲注，waitfor delay '0:0:x' 也是这个作用，常用于 MSSQL 数据库基于时间的盲注。
3. select count(*) from，占比为 11.2%，在 SQL 注入中，常与其他语句结合使用，用于判断某个表是否存在，或者猜测某个字段长度，猜测某个字符。

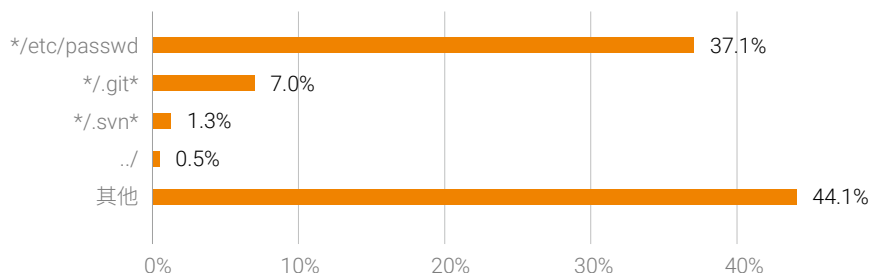
SQL 注入 Top 3 攻击 Payload 都是用于判断系统是否含有 SQL 注入漏洞的，发生在攻击初期对系统漏洞是否存在的探测踩点阶段。

5.4.4 路径穿越攻击常见 Payload

路径穿越攻击是指服务端对用户输入检查不严密，在涉及到文件路径操作时攻击者有可能利用绝对或相对路径来获取服务端关键路径访问的权限，造成攻击者获取服务端的敏感信息或系统的控制权限等。

我们统计了路径穿越攻击中常见的路径 Top 排名，如下图所示。

图 5.9 路径穿越攻击中常见的路径



数据来源：绿盟科技可管理安全服务（MSS）

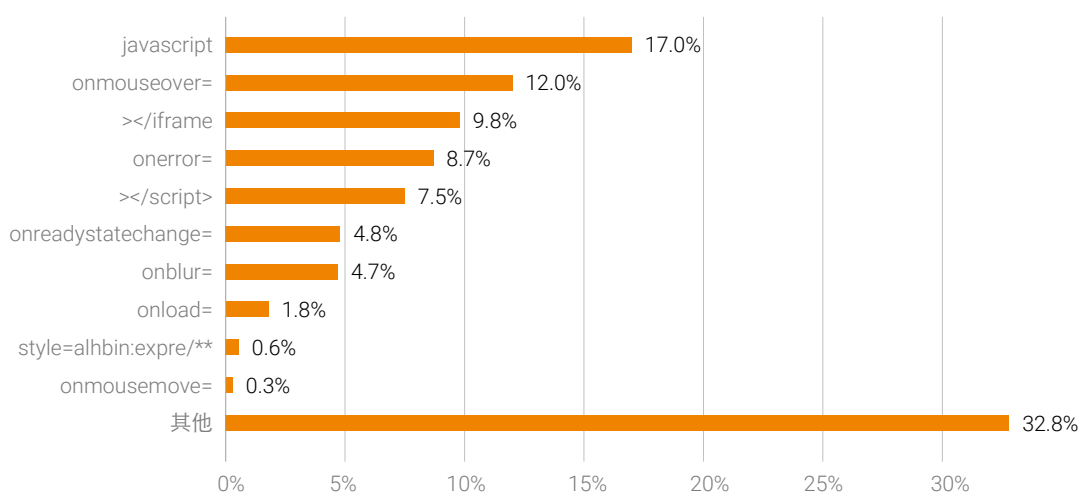
1. */etc/passwd 在路径穿越攻击中使用最多，占比 37.1%。在 linux 系统中，/etc/passwd 文件记录了每个用户的一些基本属性。系统管理员经常会接触到这个文件的修改以完成对用户的管理工作。这个文件对所有用户都是可读的。攻击者可以从这个文件中获取到系统的用户信息，从而加以利用。
2. 其次是 */.git*，占 7.0%。Github 是开源代码库以及版本控制系统，随着越来越多的应用程序转移到了云上，Github 已经成为了管理软件开发以及获取已有代码的首选方法。.gitignore 文件是 Git 项目中用于指定哪些文件要忽略。攻击者尝试从 /git 目录下获取或修改服务端源代码或 .gitignore 文件。
3. */.svn* 在路径穿越攻击中排名第三，占 1.3%。SVN 是 Subversion 的简称，是一个开放源代码的版本控制系统，多个人共同开发同一个项目，以达到共用资源的目的。攻击者企图通过 */.svn* 目录获取或修改服务端的资源（包括源代码）。
4. ../ 在路径穿越攻击中排名第四，占 0.5%。意思是回到上一层目录，攻击者可利用相对路径进行路径穿越。

5.4.5 XSS 攻击常见 Payload

XSS 全称为 Cross Site Scripting，即跨站脚本，发生在目标网站中目标用户的浏览器层面上，当用户浏览器渲染整个 HTML 文档的过程中出现了不被预期的脚本指令并执行时，XSS 就会发生。XSS 攻击是应用层常见的典型攻击类型，攻击者可提交精心构造的 XSS 攻击代码，在页面嵌入 HTML、JS 代码，使用户的浏览器端出现恶意的 HTML 元素或执行恶意的 JS 脚本，达到窃取用户 cookie、控制用户动作等特殊目的。

我们统计了 XSS 攻击中常见的攻击 Payload Top 10，如下图所示。

图 5.10 XSS 攻击常见攻击 Payload Top 10



数据来源：绿盟科技可管理安全服务（MSS）

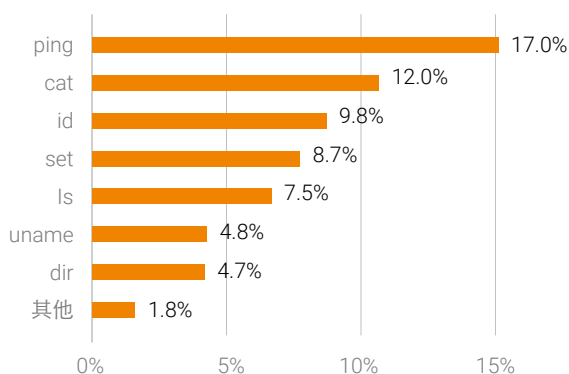
1. javascript 排第一，占 17.0%。javascript 是一种网络脚本语言，广泛应用于 Web 应用开发，为网页添加各式各样的动态功能，javascript 脚本是通过嵌入在 HTML 中来实现自身的功能的。
2. onmouseover 排第二，占 12.0%。所有主流浏览器都支持 onmouseover 属性，比如攻击者可以在 <input> 元素中插入 onmouseover 属性，当用户鼠标指针移动到元素上时就会触发攻击者插入的 XSS 攻击代码。
3. ></iframe 排第三，占 9.8%。所有浏览器都支持 <iframe> 标签，iframe 元素会创建包含另外一个文档的内联框架（即行内框架）。攻击者可通过在 iframe 元素中插入代码，实现 xss 攻击。

所有的 on* 事件内是可以执行 JavaScript 脚本的。

5.4.6 远程命令执行攻击常见 Payload

攻击者可通过提交经过特殊构造的系统命令，实现在服务端执行命令的目的，获得服务器的系统控制权。我们统计了远程命令执行攻击中常见的攻击 Payload Top 排名，如下图所示。

图 5.11 远程命令执行攻击常见 Payload



数据来源：绿盟科技可管理安全服务（MSS）

ping 命令常被用于测试网络中其他 IP 的联通性。

cat 命令用来显示文件内容。

id 用于显示用户的 ID，以及所属群组的 ID。

set 命令主要是显示系统中已经存在的 shell 变量，以及设置 shell 变量的新变量值。

ls 命令在 linux 系统下用来列出目录下的文件。

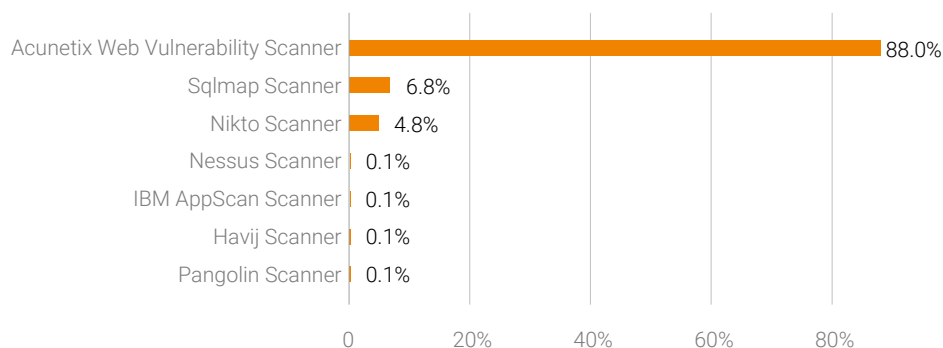
uname 用于获取电脑和操作系统的相关信息。

dir 命令在 dos 系统下用来列出目录下的文件。

5.4.7 恶意扫描常见扫描器 Top 统计

端口扫描是黑客发起攻击的前置步骤，黑客发送一组端口扫描消息，试图以此侵入某台计算机，并了解其提供的计算机网络服务类型，从而了解到从哪里可探寻到攻击弱点。我们从告警信息中分析扫描器指纹，统计出黑客最常使用的扫描器类型占比，如下图所示。

图 5.12 恶意扫描常用扫描器类型 Top 占比



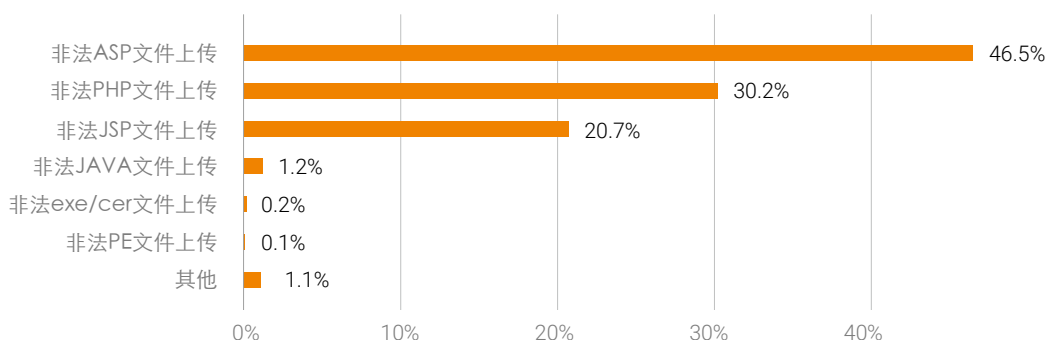
数据来源：绿盟科技可管理安全服务（MSS）

1. Acunetix Web Vulnerability Scanner 排名第一，占比高达 88%，它是一款商业的 Web 漏洞扫描程序，可以检查 Web 应用程序中的漏洞，如 SQL 注入、跨站脚本攻击、身份验证页上的弱口令长度等。它拥有一个操作方便的图形用户界面，并且能够创建专业级的 Web 站点安全审核报告。使用量 Top 1。
2. Sqlmap Scanner 是一款基于 SQLMAP 和 Charles 的被动 SQL 注入漏洞扫描工具。
3. Nikto Scanner 是一款开源的（GPL）网页服务器扫描器，它可以对网页服务器进行全面的多种扫描。
4. Nessus Scanner 是目前全世界最多人使用的系统漏洞扫描与分析软件
5. IBM AppScan Scanner。
6. Havij Scanner 胡萝卜，一款自动化的 SQL 注入工具，它能够帮助渗透测试人员发现和利用 Web 应用程序的 SQL 注入漏洞。
7. Pangolin Scanner 穿山甲，深圳宇造诺赛科技有限公司（Nosec）旗下的网站安全测试产品之一。

5.4.8 非法文件上传类型 Top 统计

攻击者为了达到长期控制网站服务器的目的，一般都会上传 Webshell 后门，排名前 3 的 ASP/PHP/JSP 都是现在最常用的 Webshell 后门格式。

图 5.13 非法文件上传常见类型 Top 占比



数据来源：绿盟科技可管理安全服务（MSS）

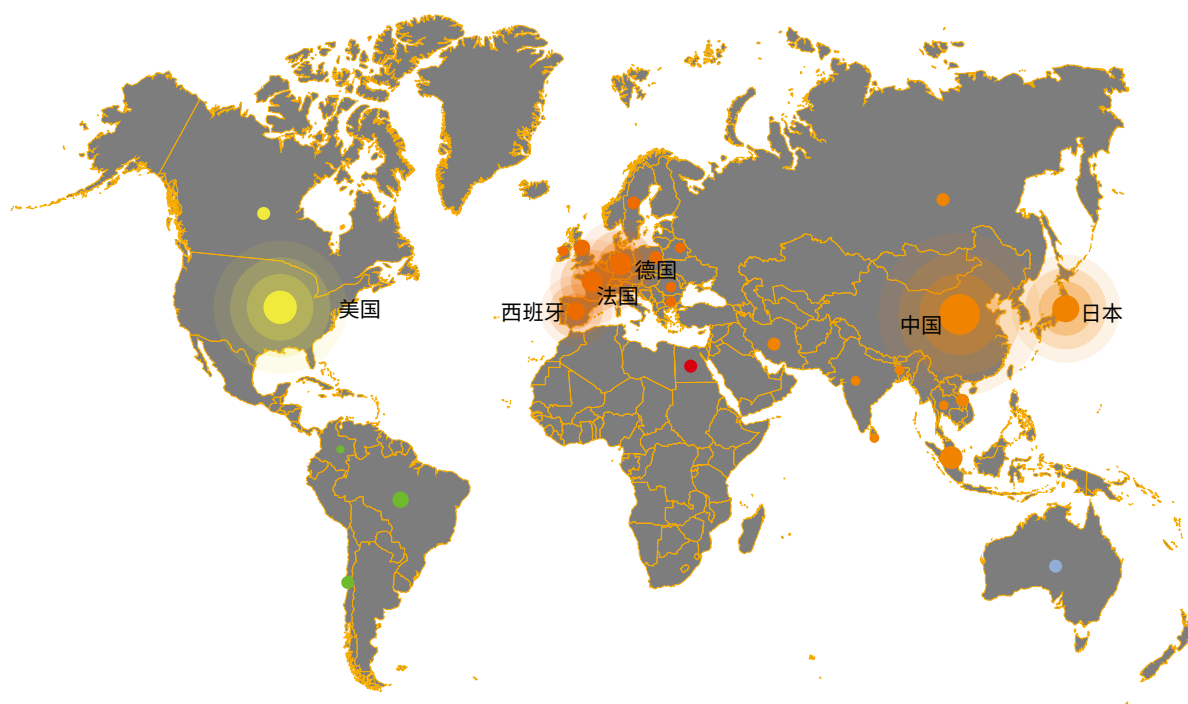
5.5 Struts2 CVE-2017-5638 高危漏洞

Apache Struts2 在今年 2017 年 3 月 7 日曝出一个高危漏洞——CVE 编号 CVE-2017-5638，其原因是由于 Apache Struts2 的 Jakarta Multipart parser 插件存在远程代码执行漏洞，攻击者可以在使用该插件上传文件时，修改 HTTP 请求头中的 Content-Type 值来触发该漏洞，导致远程执行代码。

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，一旦出现漏洞，影响甚广。

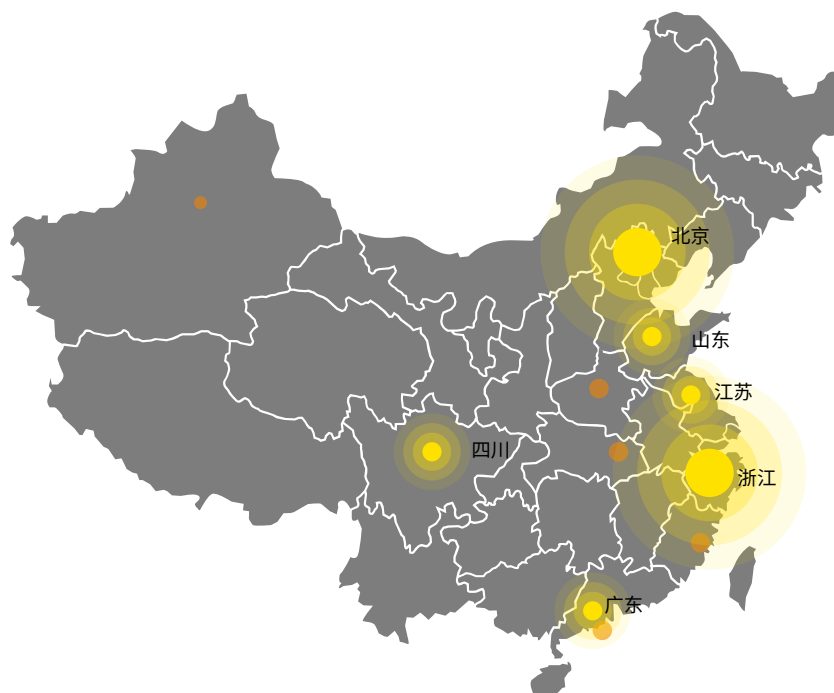
NSFOCUS 发布的《[【万年漏洞王】Struts2 受影响情况数据报告](#)》中给出了全球和中国地区互联网上开放的 Apache Struts 分布情况，如下图所示。

图 5.14 全球互联网上开放的 Apache Struts 分布



数据来源：绿盟科技威胁情报中心（NTI）

图 5.15 中国互联网上开放的 Apache Struts 分布

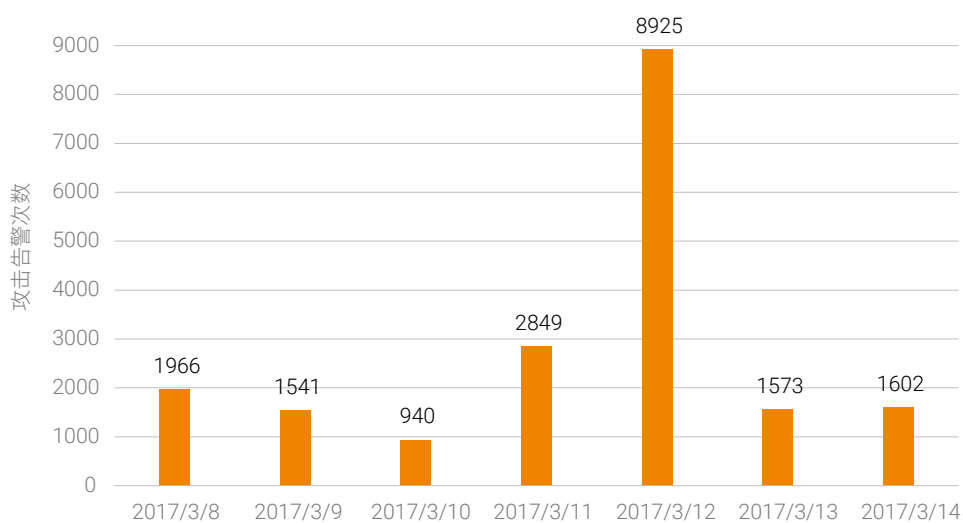


数据来源：绿盟科技威胁情报中心（NTI）

5.5.1 攻击次数趋势

我们对该漏洞爆出后一周内该漏洞的攻击次数进行统计，如下图所示。针对所有 NSFOCUS 监控的 Web 站点，一周内共发生 19,396 次该漏洞的攻击，平均每天 2,771 次攻击。在漏洞爆出的第 4 天为攻击高发期，共发生 8,925 次该漏洞的攻击。

图 5.16 CVE-2017-5638 Struts2 漏洞日攻击次数



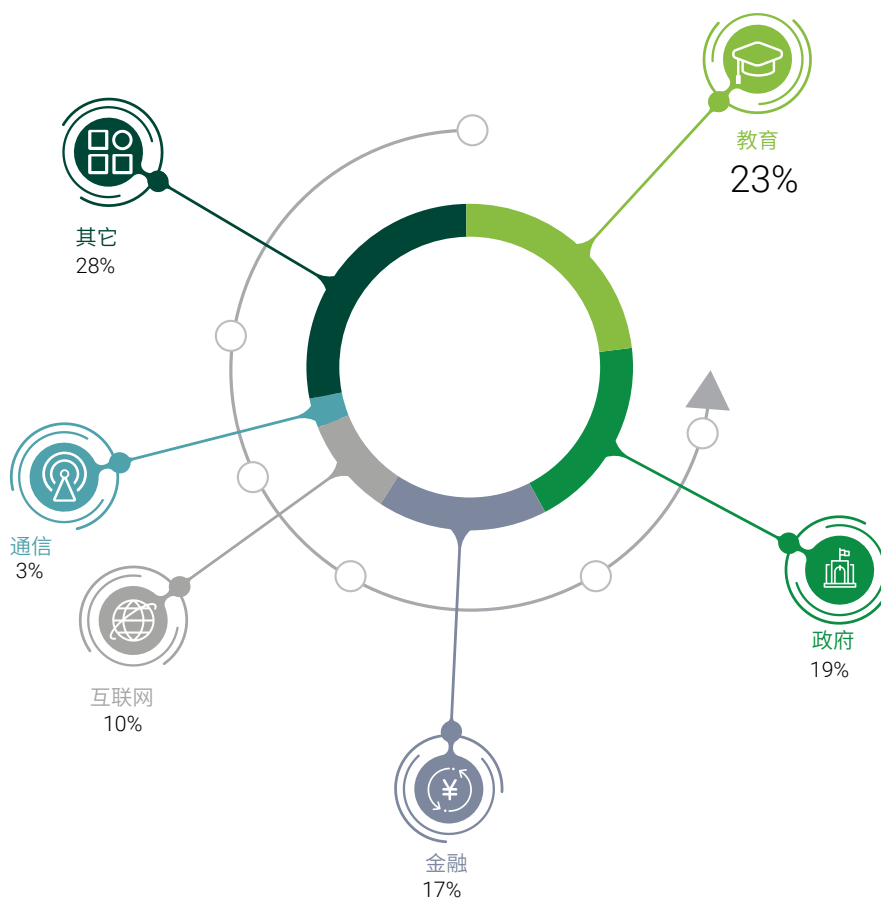
数据来源：绿盟科技可管理安全服务（MSS）

5.5.2 受影响行业和地域

从 3 月 7 日漏洞爆出到 3 月 9 日不到 36 个小时时间内，对使用绿盟云的 Struts2 紧急漏洞检测服务的网站进行统计分析。得出如下结果：

1、从检测数据来看，教育行业受 Struts2 漏洞影响最多，占 23%，其次是政府（19%）、金融（17%）、互联网（10%）、通信等行业（3%）。

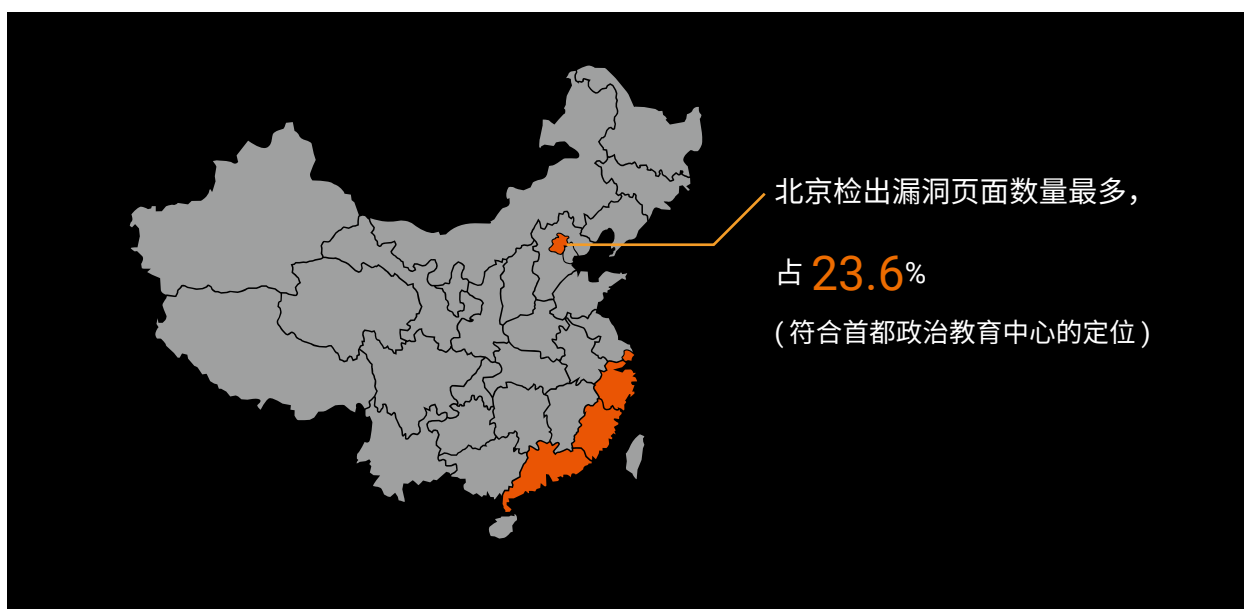
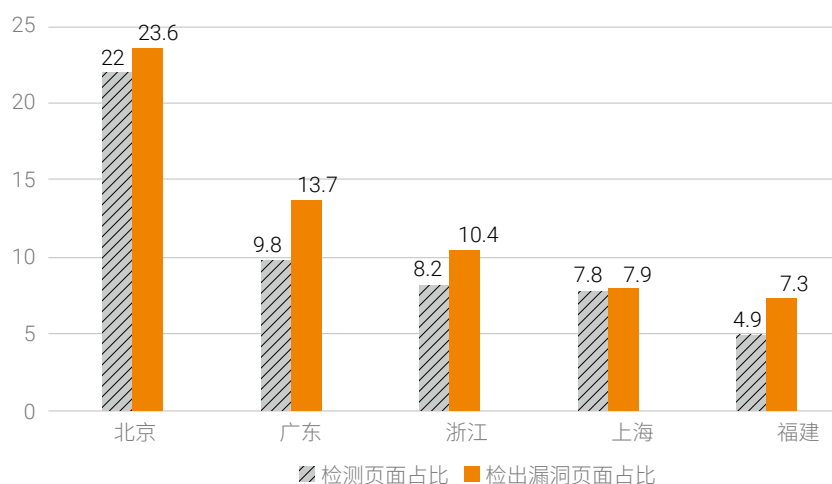
图 5.17 受 Struts2 漏洞影响行业



数据来源：绿盟科技威胁情报中心（NTI）

2、从地域来看，北、上、广、沿海城市等经济发达地区成为 Struts2 漏洞高发区，与此同时修复情况也最及时。其中北京最积极占 22%，其次是广东 9.8%，浙江 8.2%，上海 7.8%，福建 4.9%。这也符合“多检多得”的排序，北京检出漏洞页面数量最多，占 23.6%（符合首都政治教育中心的定位），广东 13.7%，浙江 10.4%，上海 7.9%，福建 7.3%。

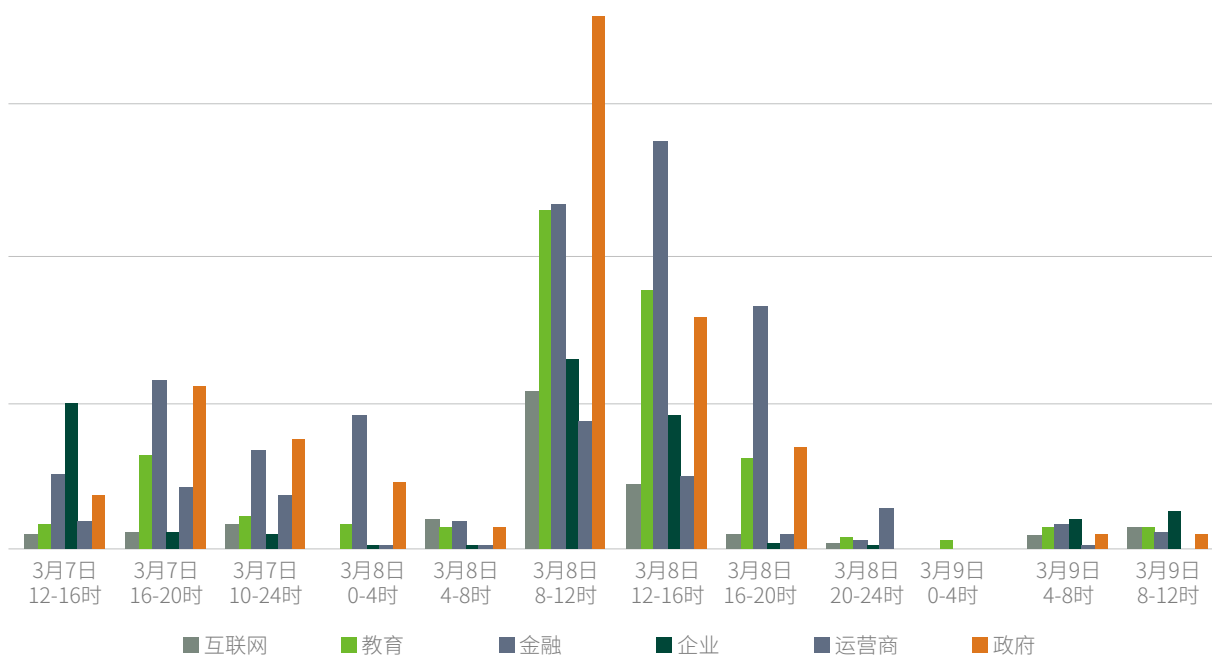
图 5.18 受 Struts2 影响的中国地区 Top 5



数据来源：绿盟云

3. 从应对漏洞积极性来说，金融、政府、教育位列前三甲。根据检测结果以及绿盟工程服务团队响应客户反馈统计，应对本次 Struts2 漏洞，金融行业应急响应最为迅速，在漏洞爆发后采取行动也是最迅速的，无论是自行升级漏洞软件还是联系厂商升级防护设备都走在其他行业前列，很多金融行业站点在几个小时之内再次扫描时已经将漏洞修补完成。

图 5.19 Struts2 漏洞各行业检测积极性



数据来源：绿盟云

绿盟云清洗服务

2016 年 6 月正式推出绿盟云清洗服务，在全国拥有 5 大高防机房，海外多地拥有云清洗中心，总清洗能力大于 3T，提供电信、联通、BGP 多线路同时清洗，可以帮助各类客户抵御大流量 DDoS 攻击上百次，最高攻击峰值超百 G。现与黑洞云清洗服务的多通道联动，围绕智能、敏捷、可运营这三大特性展开，以本地设备为探针，快速感知大流量 DDoS 攻击，智能联动云清洗服务，云端运营平台调集最佳清洗资源协防，抵御各类 DDoS 攻击于无形。

绿盟科技威胁情报中心（NSFOCUS Threat Intelligence, NTI）

定位于绿盟科技智慧安全战略的安全数据中枢，是绿盟科技依托自身在安全研究、安全产品、安全服务的长期积累，以及威胁情报应用实践，构建的集情报生产、消费、服务于一体的综合性威胁情报服务中心。NTI 聚焦威胁情报在提升安全能力方面的核心价值，以高质量的威胁情报为核心，通过数据共享、设备联动、服务定制等形式，为企业客户提供威胁情报驱动的安全解决方案，全面提升客户在安全响应和安全对抗中的主动性、及时性和有效性。

作者

绿盟科技 潘文欣、孙叶、彭元、何坤

编辑

绿盟科技 郝明 黄柱（平面设计）

同时感谢绿盟科技 IIS 技术团队和威胁情报中心的同事对本报告提供的帮助和支持



THE EXPERT BEHIND GIANTS 巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，
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。
在这些巨人的背后，他们是备受信赖的专家。

www.nsfocus.com