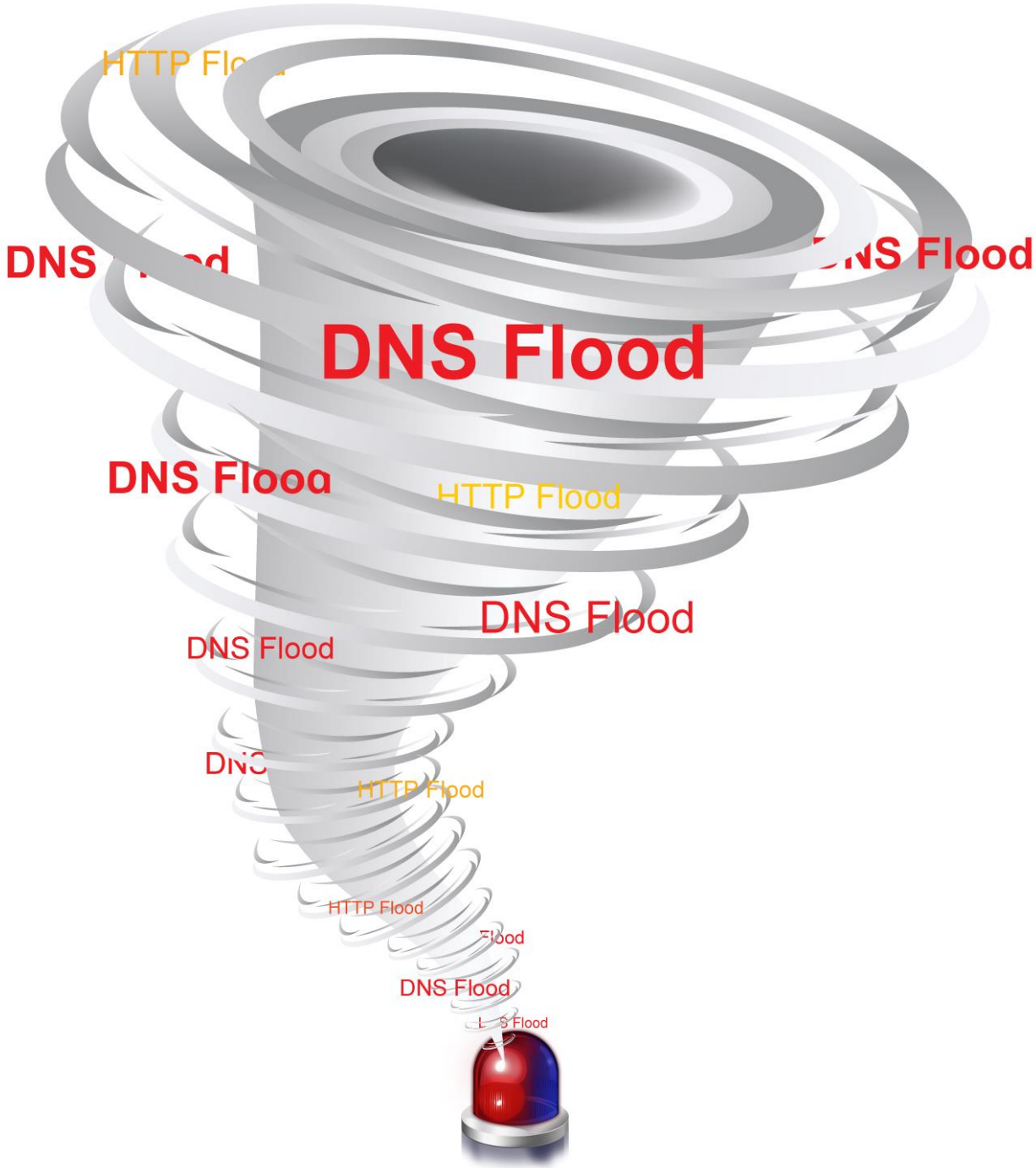
SECURITY NSFOCUS

NSFOCUS
H1 2014 DDoS THEATS REPORT

2014H1 绿盟科技 DDoS 威胁报告



执行摘要

持续关注趋势

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，绿盟科技的防护产品和监测系统会发现数以千计的 DDoS（分布式拒绝服务）攻击危害客户安全。为了快速反馈关于这类攻击的信息，绿盟科技发布《2014 H1 DDoS 威胁报告》。本报告为 2014 年半年报，用于快速跟踪及反馈 DDoS 威胁的发展态势。如果您需要了解全年报告《2014 DDoS 威胁报告》的情况，请跳转到该章节。

关键发现

本次报告包括以下关键观点：

[政府网站依然是最主要的攻击对象，攻击者选择目标具有“潮流性”

广州、上海和浙江是最集中的受害区域，受攻击的地区有越来越集中的趋势

四成的受害者遭受 2 次或以上 DDoS 攻击，40 位中会有 1 位遭受 10 次以上

DNS FLOOD 依然是最主要的 DDoS 攻击方式，HTTP FLOOD 持续减少

30 分钟内的 DDoS 攻击始终占总数的 90%左右

大流量高速的攻击正越来越多]

特别声明

本次报告中涉及的所有数据，来源于绿盟科技的自身产品、网络监测和合作伙伴的提供。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，均不会出现在报告中。

关于本文档

在本文档中你可以尝试体验检索、搜索及共享操作。

点击本图标可以打开 Adobe Acrobat 中的查找功能。

随时注意页面左侧的这些图标，点击它们可供分享内容。

推荐软件

Adobe Acrobat 7.0 及以上版本

报告内容

“

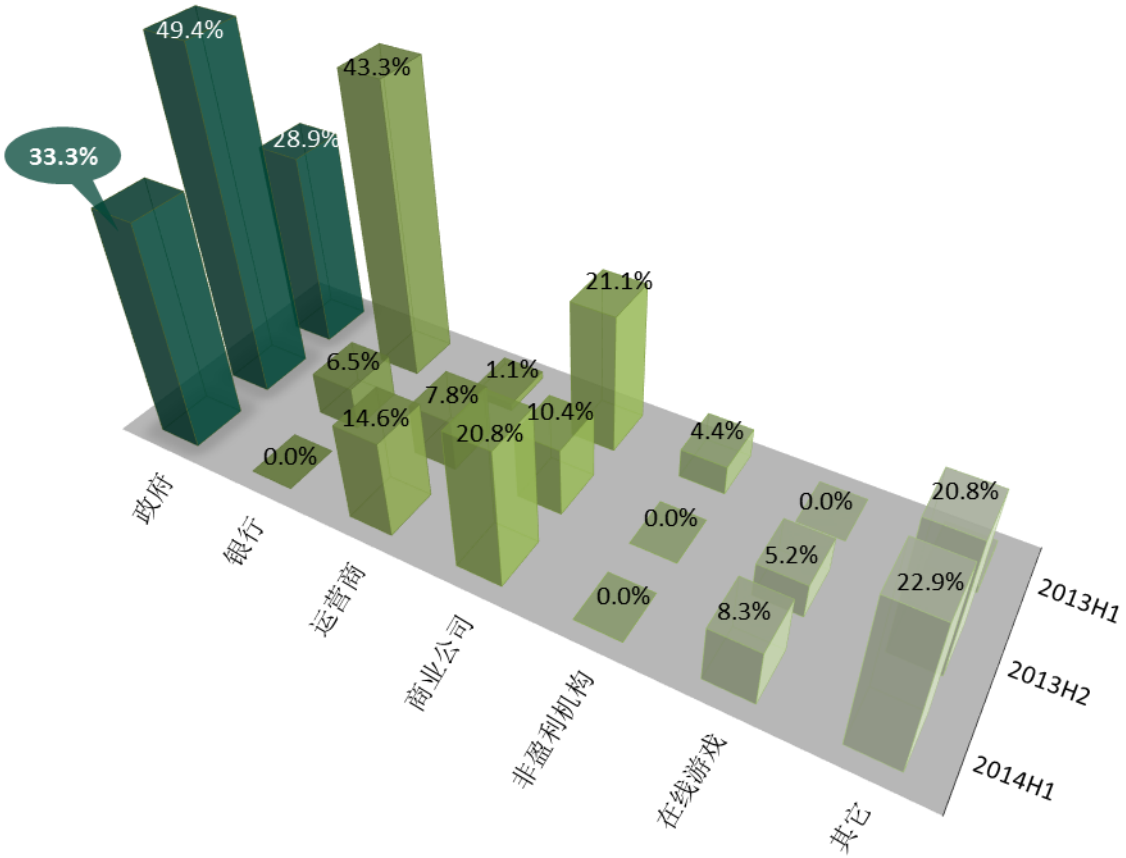
绿盟科技威胁响应中心，每天都在持续追踪

DDoS 威胁的发展态势

33.3%

观点 1 :政府网站依然是最主要的攻击对象，攻击者选择目标具有“潮流性”

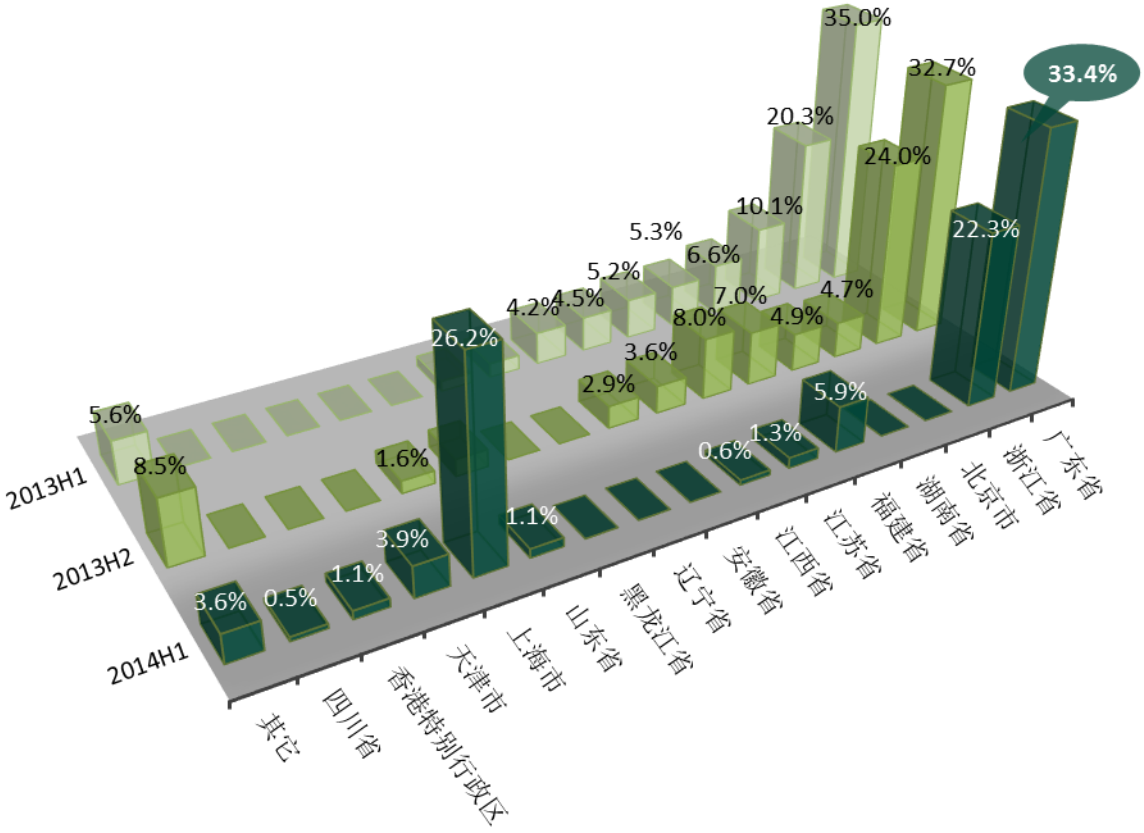
绿盟科技收集了 2013 至 2014 年全球发生的重大 DDoS 攻击事件。在这些攻击事件中，[2014 上半年政府网站依然是 DDoS 攻击最主要的目标，占总数的三分之一，其次则是针对商业公司的攻击。与 2013 下半年相比，政府网站和在线游戏受到的攻击比例有所下降，而运营商和商业公司则有所上升。与 2013 上半年相比，最明显的区别是针对银行的 DDoS 急剧减少。] 这体现了攻击者除了具有“逐利性”以外，对目标选择其实同其他商品一样具有的“潮流性”。



	2013H1	2013H2	2014H1
政府	28.9%	49.4%	33.3%
银行	43.3%	6.5%	0.0%
运营商	1.1%	7.8%	14.6%
商业公司	21.1%	10.4%	20.8%
非盈利机构	4.4%	0.0%	0.0%
在线游戏	0.0%	5.2%	8.3%
其它	1.1%	20.8%	22.9%

观点 2：广州、上海和浙江是最集中的受害区域，受攻击的地区有越来越集中的趋势

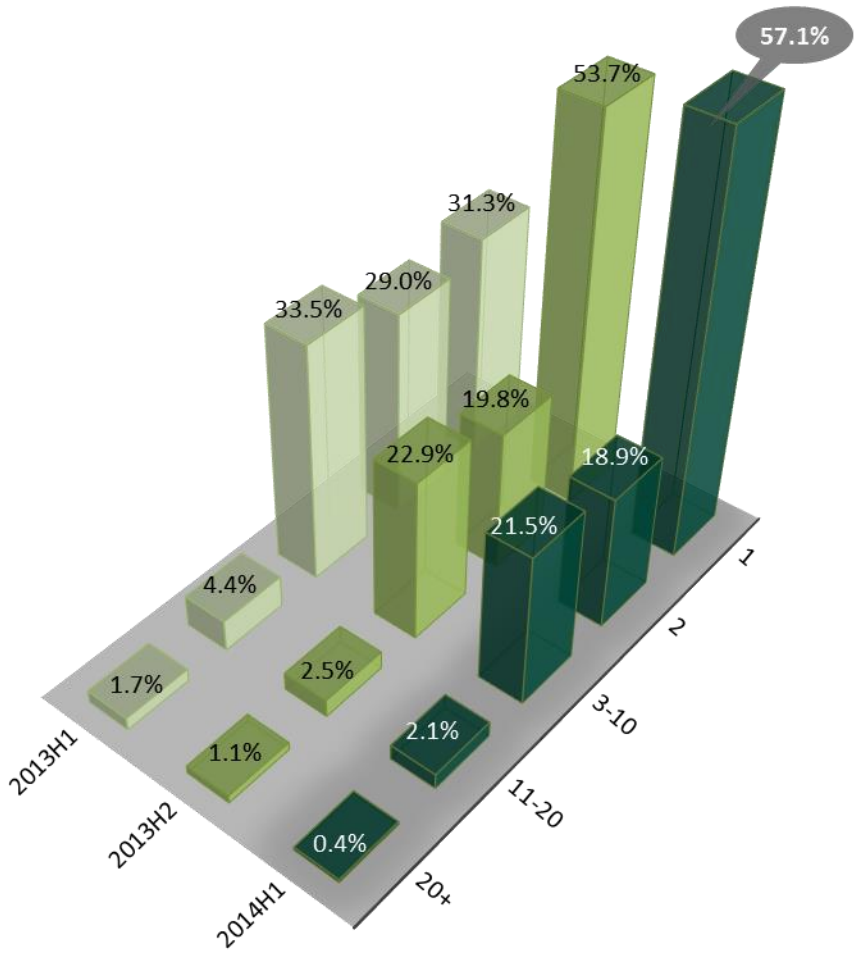
2013 至 2014 年 DDoS 攻击目标在中国国内的地理分布变化明显。从下图可以看出，[2014 上半年广州、上海和浙江是最集中的受害区域。受害区域有越来越集中的趋势，2013 前三位的地区共占攻击的 65%左右，而在 2014 上半年则上升到 82%。其中变化最明显的事北京市，受害者数量逐年减少，2013 上半年位列第三，到 2014 就已经跌出了前十。]



	广东省	浙江省	北京市	湖南省	福建省	江苏省	江西省	安徽省	辽宁省	黑龙江省	山东省	上海市	天津市	香港特别行政区	四川省	其它
2013H1	35.0%	20.3%	10.1%	6.6%	5.3%	5.2%	4.5%	4.2%	1.8%	1.4%	0.0%	0.0%	0.0%	0.0%	0.0%	5.6%
2013H2	32.7%	24.0%	4.7%	4.9%	7.0%	8.0%	3.6%	2.9%	0.0%	0.0%	2.2%	1.6%	0.0%	0.0%	0.0%	8.5%
2014H1	33.4%	22.3%	0.0%	0.0%	5.9%	1.3%	0.6%	0.0%	0.0%	0.0%	1.1%	26.2%	3.9%	1.1%	0.5%	3.6%

观点 3：四成的受害者遭受 2 次或以上 DDoS 攻击，每 40 位中会有一位遭受 10 次以上

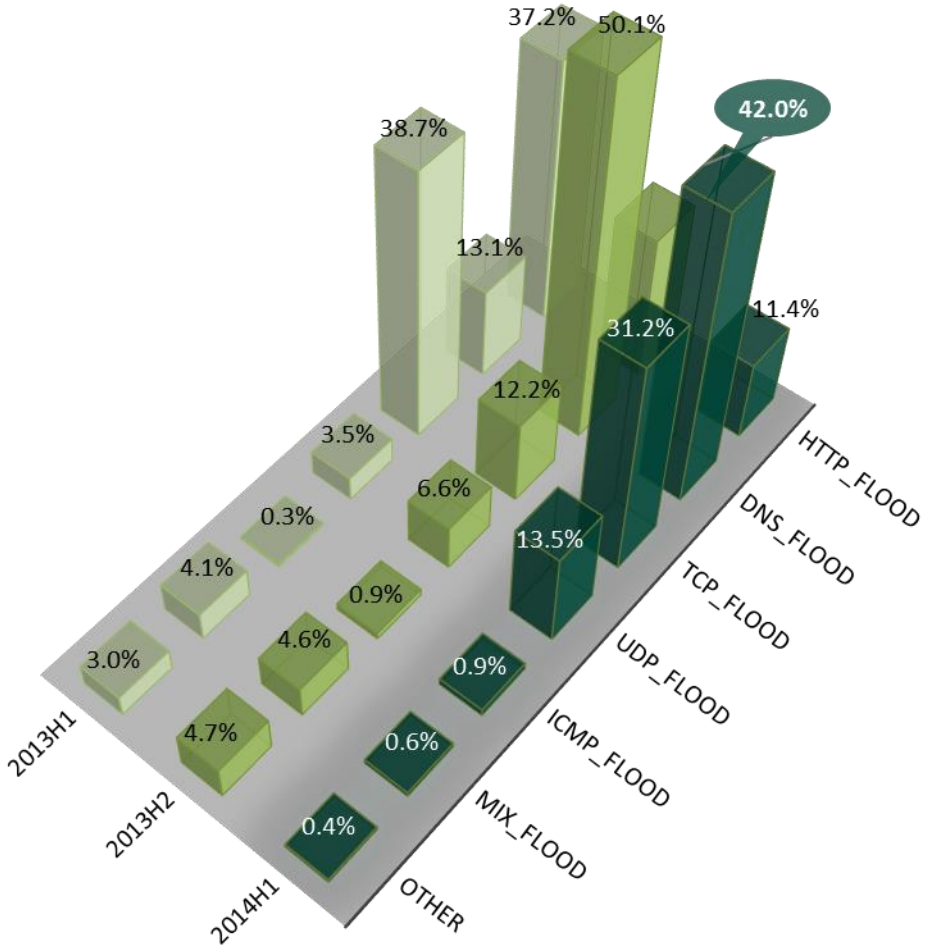
下图表现了 2013 至 2014 年 DDoS 攻击目标每半年受到的 DDoS 攻击次数。从中可以看出，[2014 上半年中四成的受害者（42.9%）遭受过 2 次或以上的 DDoS 攻击，而每 40 个受害者中会有一位遭受 10 次以上的攻击，半年内单一目标最多遭受过 68 次攻击。整体现象与 2013 下半年基本一致。而与 2013 上半年相比，情况已经有所改善，当时有超过三分之二的受害者遭受过 2 次或以上 DDoS 攻击。]



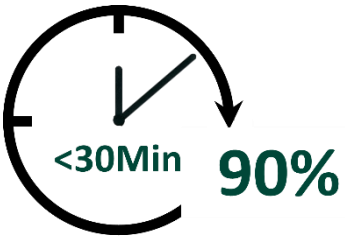
	1	2	3-10	11-20	20+
2013H1	31.3%	29.0%	33.5%	4.4%	1.7%
2013H2	53.7%	19.8%	22.9%	2.5%	1.1%
2014H1	57.1%	18.9%	21.5%	2.1%	0.4%

观点 4：DNS FLOOD 依然是最主要的 DDoS 攻击方式 ,HTTP FLOOD 持续减少

[2014 上半年绿盟科技的监测数据显示，DNS FLOOD 依然是最主要的 DDoS 攻击方式，占总数的 42%，其次是 TCP FLOOD，UDP FLOOD 和 HTTP FLOOD。与 2013 下半年相比，DNS FLOOD 和 HTTP FLOOD 的数量有所减少，而 TCP FLOOD 则大幅上升。与 2013 上半年相比，DNS FLOOD 的上升和 HTTP FLOOD 的下降最为显著。**]**

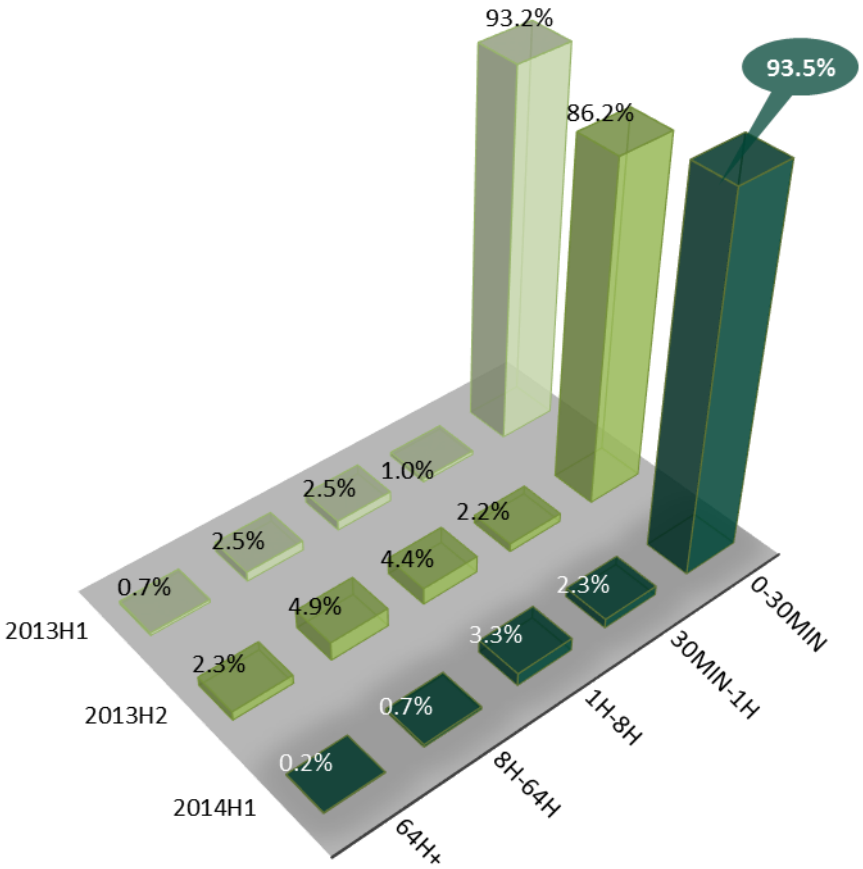


	HTTP_FLOOD	DNS_FLOOD	TCP_FLOOD	UDP_FLOOD	ICMP_FLOOD	MIX_FLOOD	OTHER
2013H1	37.2%	13.1%	38.7%	3.5%	0.3%	4.1%	3.0%
2013H2	20.9%	50.1%	12.2%	6.6%	0.9%	4.6%	4.7%
2014H1	11.4%	42.0%	31.2%	13.5%	0.9%	0.6%	0.4%

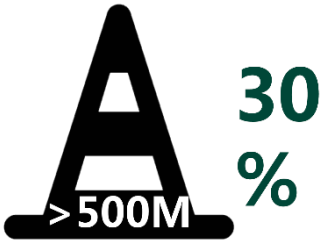


观点 5：30 分钟内的 DDoS 攻击始终占总数的 90%左右

[2013 年以来的数据显示，DDoS 攻击时间的分布一直比较稳定，30 分钟内完成的攻击始终占 90%左右。由此可见，对于 DDoS 的缓解而言，从检测发现攻击到启动清洗的响应速度会成为评判缓解效果的关键因素之一。此外，长期连续的 DDoS 攻击虽然少见但依然存在，2014 上半年绿盟科技监测到持续最久 DDoS 长达 228 个小时。]

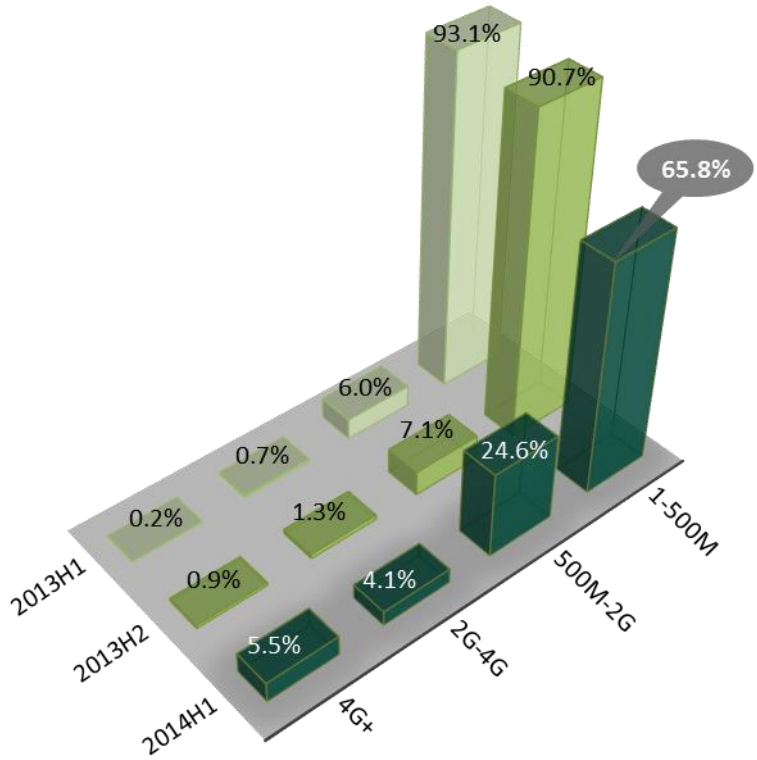


	0-30min	30min-1h	1h-8h	8h-64h	64h+
2013H1	93.2%	1.0%	2.5%	2.5%	0.7%
2013H2	86.2%	2.2%	4.4%	4.9%	2.3%
2014H1	93.5%	2.3%	3.3%	0.7%	0.2%

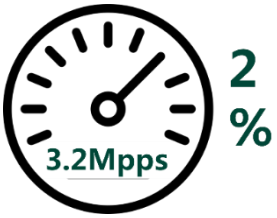


观点 6：大流量、高速率的攻击正越来越多

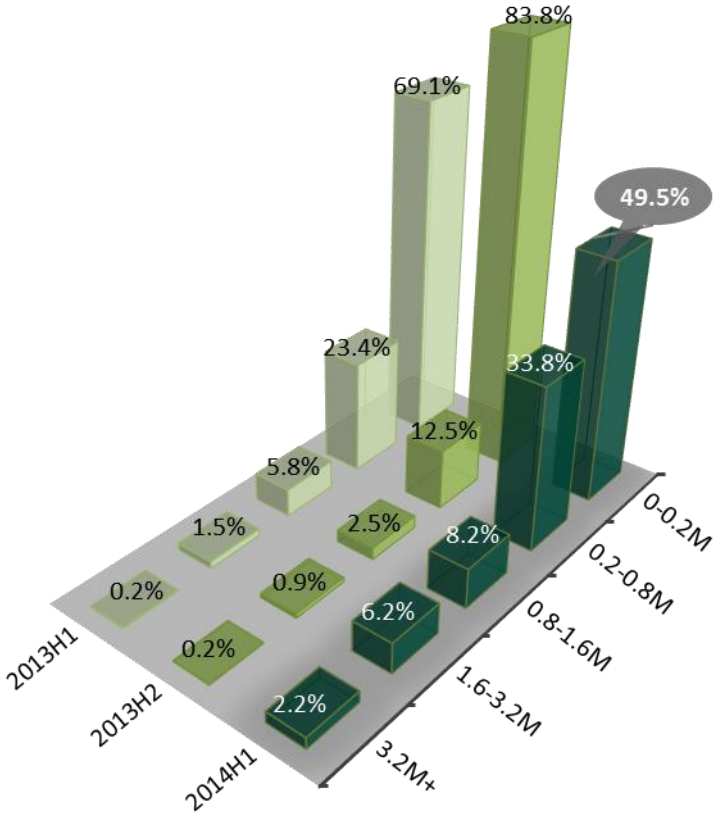
[2013 年，大部分 DDoS 的实际流量并不大，500M 以下的攻击占 90%以上。然而，2014 上半年的数据显示，DDoS 的攻击流量开始整体上升，500M 以上的攻击已占总数的三分之一，4G 以上则超过了 5%。绿盟科技在此期间内监测到的攻击流量最高达到 45G。**]**



	1-500M	500M-2G	2G-4G	4G+
2013H1	93.1%	6.0%	0.7%	0.2%
2013H2	90.7%	7.1%	1.3%	0.9%
2014H1	65.8%	24.6%	4.1%	5.5%



[与流量提升同步，DDoS 攻击的包速率也在全面加快。0.2Mpps 以上的已经超过一半，而在 2013 下半年这个数字还仅为 16%。 超过 3.2Mpps 的攻击也超过了 2%，最快速率达到了 23Mpps，高速攻击的时代正在来到。**]**



	0-0.2M	0.2-0.8M	0.8-1.6M	1.6-3.2M	3.2M+
2013H1	69.1%	23.4%	5.8%	1.5%	0.2%
2013H2	83.8%	12.5%	2.5%	0.9%	0.2%
2014H1	49.5%	33.8%	8.2%	6.2%	2.2%

结束语

回顾 4 年来 DDoS 的跟踪数据以及更早期的研究成果，我们会发现其发展并不平稳。从一些角度看，攻击者在行为在不断变化，例如受害行业和攻击方法；而从另一些角度，似乎存在比较明显的趋势，例如受害者的地域分布和攻击的流量时长。

引发这些现象的原因包括了技术自身的发展，网络环境的演进，以及利益格局的变化。技术发展为攻击者提供了越来越多的工具选择，但这并不是关键的因素。网络环境的演进使得攻防的战场更为复杂，可用的战术多样化的同时，也有一些高效原则开始被普遍接受。

最后，也是最重要的，**[** 大部分 DDoS 攻击者依然以获利为目的，网络中自身利益格局的变化，对攻击行为的影响是最大的。事实表明，这个观点正是得益于绿盟科技长期跟踪及分析 DDoS 数据。相信这些观点对于大家预测未来的攻击形态，以及进一步完善企业及组织的解决方案，是有价值的。**]**

“知己知彼，百战不殆”，面对阴影中凶狠而狡猾的敌人，您做好准备了吗？

DDoS 威胁报告

SECURITY

网络安全威胁正在变得日益复杂，各类攻击目标、手段及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态势，以便能够理解与预测未来可能遭遇的恶意攻击，进而应对复杂变化所带来的挑战。

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，绿盟科技威胁响应中心对此予以重点及持续关注，同时定期发布《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

但随着 DDoS 攻击的日益加剧，年度报告已无法快速呈现其发展态势，故绿盟科技从 2012 年起，增发 DDoS 威胁报告半年报。本次报告即为 2014 年上半年 DDoS 威胁报告，在年底前后绿盟科技威胁响应中心将会发布《2014 DDoS 威胁报告》的年度安全报告。

如果您希望与我们一起持续关注这个项目，都可以联系我们：

- 点击左侧打印机图标，将本报告打印出来，便于在旅途中阅读。
- 点击左侧邮件图标，将本报告发送给您的朋友，与他们分享。
- 访问更多 DDoS 安全报告：http://www.nsfocus.com/4_research/4_6.html
- 点击左侧微博按钮，与绿盟科技的官方微博在线互动：http://weibo.com/300369

作者和贡献者

作者：

鲍旭华，绿盟科技　　Email：baoxuhua@nsfocus.com

博士，绿盟科技战略研究部研究员，主要研究领域为信息安全事件分析、安全智能和态势感知。

洪海，绿盟科技　　Email：honghai@nsfocus.com

绿盟科技安全研究部研究员，主要进行网络攻防和漏洞相关研究。

贡献者：

刘永刚，绿盟科技　　Email：liuyonggang@nsfocus.com

刘亚，绿盟科技　　Email：liuya@nsfocus.com

王晓晖，绿盟科技　　Email：wangxiaohui@nsfocus.com

您可以点击左侧邮件图标，联系报告作者，将您的见解与我们分享！先行致谢！

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。

巨 人 背 后 的 专 家

THE EXPERT BEHIND GIANTS