SECURITY NSFOCUS

2014 绿盟科技 DDoS 威胁报告

2014 DDoS THREAT REPORT

2014 DDoS 威胁报告执行摘要

快速导读

本报告是 2014 年全年度 DDoS 报告。2014 年，DDoS 攻击方式中出现了新的 DDoS 反射式放大攻击形式，该攻击基于 SSDP 协议利用一些智能设备进行反射式攻击，攻击带宽放大倍数最高可达 75 倍。在国内，在线游戏已进入 DDoS 攻击目标的前 3。在 2014 年 DDoS 攻击事件中，某次攻击事件流量超过 100Gbps。

关键发现

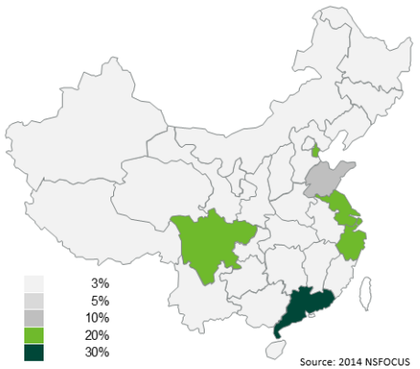
1. 智能设备发起 DDoS 攻击数量明显增多
2. 广东依然是最严重的受害区域
3. 18 点-23 点是 DDoS 开始攻击的主要时间段
4. UDP FLOOD 成为最主要的 DDoS 攻击方式
5. 在线游戏已进入 DDoS 攻击目标前 3
6. 93% DDoS 攻击发生在半小时内

预测 2015

1. DDoS 攻击峰值流量将再创新高
2. 反射式 DDoS 攻击技术会继续演进
3. DNS 服务将迎来更多的 DDoS 攻击
4. 针对行业的 DDoS 攻击将持续存在

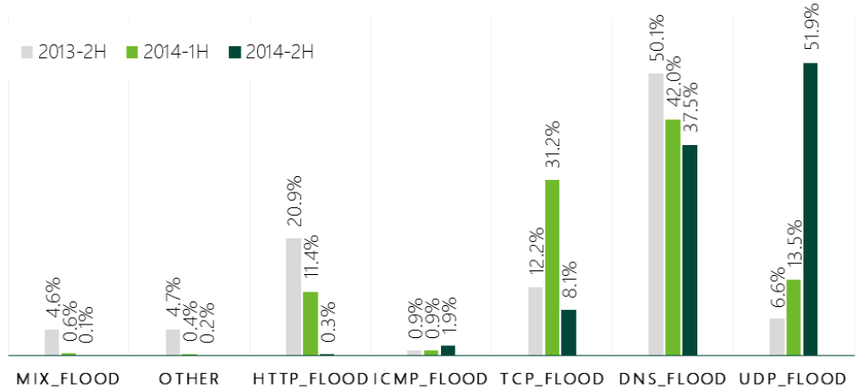
广东依然是最严重的受害区域

与 2014 上半年相比，广东省内被攻击的比例虽然下降，但是其下半年遭受攻击次数是上半年的一倍多。



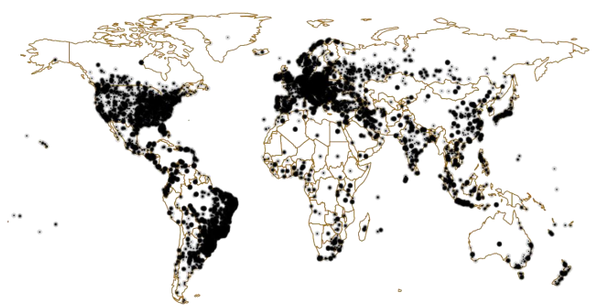
UDP FLOOD 成为最主要的 DDoS 攻击方式

UDP FLOOD 上升为重要 DDoS 攻击方式的原因之一，与反射式 DDoS 攻击有密切关系。此类攻击不需要占领大量的“肉鸡”，而且从被攻击者角度来看，所有数据包都是正常的，但海量数据最终严重损耗网络带宽资源。



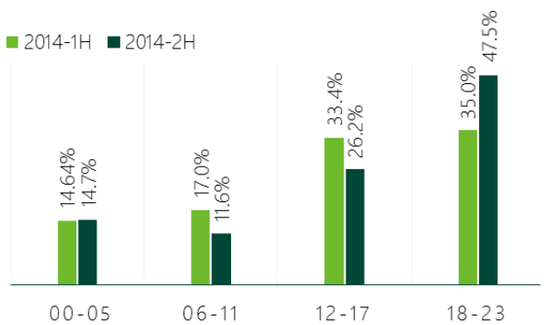
全球已发现 700 多万 SSDP 设备可能被利用进行 DDoS 攻击

由于一些基于 SSDP 协议的智能设备存在弱口令或者漏洞，且一般情况下防御薄弱，容易被攻击者利用，进而成为 DDoS 攻击源。



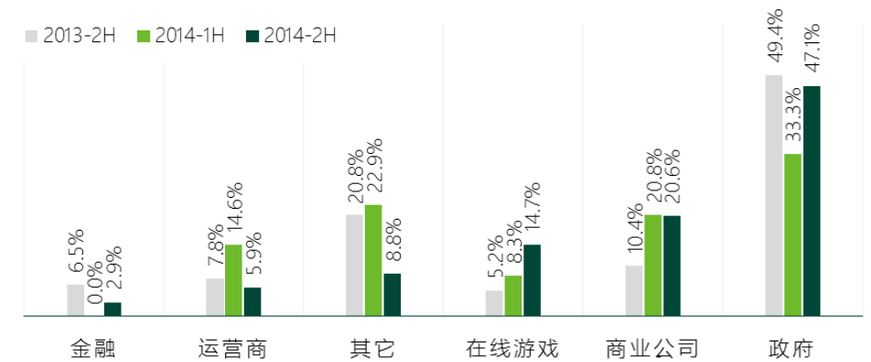
18 点-23 点是 DDoS 开始攻击的主要时间段

攻击者选择这个时间段开始进行攻击，因为这段时间电脑在线数量多，网络流量比较大，使得攻击效果会“事半功倍”。



在线游戏已进入 DDoS 攻击目标前 3

在线游戏运营商被攻击事件的急速上升，可能与攻击者通过勒索而牟取非法利益存在着联系，也有可能存在非正当商业竞争等原因。



报告下载 了解更多 DDoS 攻击防御信息 400-818-6868（7×24）

http://weibo.com/nsfocus

http://www.nsfocus.com.cn/4_research/4_6.html

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。

目录

4

报告内容

观点 1：智能设备发起 DDoS 攻击数量明显增多 4

事件 1：2014 年国内规模最大的 DDoS 攻击——1/3 攻击源是智能设备 4

观点 2：沿海省市是受攻击的集中地区，广东依然是最严重的受害区域 5

观点 3：18 点-23 点是 DDoS 开始攻击的主要时间段 6

观点 4：UDP FLOOD 成为最主要的 DDoS 攻击方式 7

事件 2：SSDP 反射式 DDoS 攻击实例分析 8

观点 5：在线游戏已进入 DDoS 攻击目标前 3 10

观点 6：93% DDoS 攻击发生在半小时内 10

11

预测 2015

DDoS 攻击峰值流量将再创新高 11

反射式 DDoS 攻击技术会继续演进 11

DNS 服务将迎来更多的 DDoS 攻击 11

针对行业的 DDoS 攻击将持续存在 11

作者和贡献者 12

关注 DDoS 威胁报告 13

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

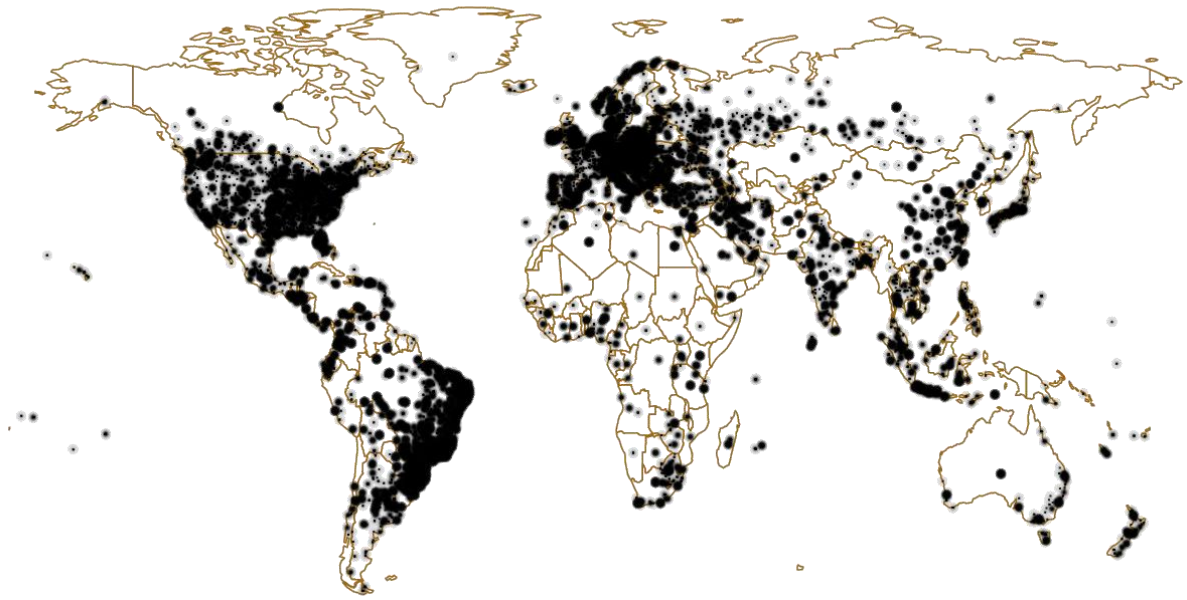
报告内容

观点 1：智能设备发起 DDoS 攻击数量明显增多

近年来已监测到多起由智能设备发起的 DDoS 攻击，并且次数在逐渐增多。 由于一些智能设备（例如网络摄像机）具有以下特点：

- 相对比较高的带宽
- 升级周期比较长，甚至可能自部署后从未升级
- 通常是 7*24 小时在线

如果这些设备存在弱口令或者漏洞，则容易被攻击者利用，进而成为 DDoS 攻击源。绿盟科技近期对世界范围内的智能设备进行了监控，已发现约 80 万该类设备可能被利用进行 DDoS 攻击，下图显示了其分布情况。



事件 1：2014 年国内规模最大的 DDoS 攻击——1/3 攻击源是智能设备

自 2014 年 12 月 10 日起，全球范围内 DNS 流量出现异常，针对该事件绿盟科技安全团队做出了快速的分析处理，此次 DNS 攻击事件波及全国大多数省份，从 10 日凌晨至 14 日，攻击在全国范围内依然时常发生。初步统计，此次攻击事件在全国范围内的攻击流量至少有 100G 以上，单节点高峰流量达到 70Gbps，其持续事件之长，攻击流量之大，属近年之最。经过样本分析发现，攻击者通过不断查询 a***k.org、n***c.com 等三个域名的随机二级域名的方法进行 DNS Flood 攻击。

这次 DDoS 攻击的基本方法是利用僵尸网络查询游戏网站的随机二级域名，企图攻击该游戏网站的权威域名服务器（即 DNS Slow Drip DDoS 攻击）。由于国内的宽带用户通常将其电脑的 DNS 选项设置为各省的递归服务器，在大量肉鸡发起攻击（请求）后，导致递归服务器需要向外递归查询游戏网站的随机二级域名，从而极大地消耗了这些服务器的系统资源，造成运营商核心解析业务受到严重影响。这次 DDoS 攻击有如下 3 点值得关注的地方：

- 攻击源中有 1/3 左右是智能设备

- 国内 DNS 递归服务器是因牵连而受到严重影响
- 被攻击域名均属于在线游戏网站

此外，以 2014 年 12 月为例回顾针对 DNS 服务的 DDoS 攻击事件（DNS FLOOD）

EVENT OF 2014 DDoS ATTACK

攻击对象	开始日期	攻击流量	持续时间	缓解方法
DNS Simple[①]	12 月 01 日	将近 25Gbps	约 11 小时	部署 20Gb 清洗设备 使用 Anycast 网络服务进行 DNS 流量清洗
1&1 Internet[②]	12 月 09 日		约 12 小时	
国内运营商	12 月 10 日	至少 100Gbps	4 天多	部署 DDoS 清洗设备
Telia[③]	12 月 11 日		1 天多	
朝鲜[④]	12 月 21 日		约 9.5 小时	
Rackspace[⑤]	12 月 22 日		约 12 小时	将 DDoS 清洗设备部署到 DNS 之前

Source: 2014 NSFOCUS DDoS Threat Report

上表中若干攻击事件可能存在关联。这些攻击能够频频得手充分说明，从攻击者角度看攻击 DNS 服务是实现攻击目的既有力又有效的手段，这种选择也间接体现了目前 DNS 的安全防护状况，毕竟 DDoS 攻击目的就是企图造成资源耗尽，因此需要找出攻击受害者的"软肋"。

如何读懂 DDoS 攻击事件报道中的流量

DDoS 攻击事件报道中提及攻击流量时，常见的流量单位是 pps（packets per second）或 bps（bits per second），前者还包括 Kpps、Mpps、Gpps 等，后者还包括 Kbps、Mbps、Gbps 等。无论前者还是后者，相邻两个单位之间的进率都是 1000，而不是 1024。例如：1000Kbps=1Mbps

观点 2 :沿海省市是受攻击的集中地区，广东依然是最严重的受害区域

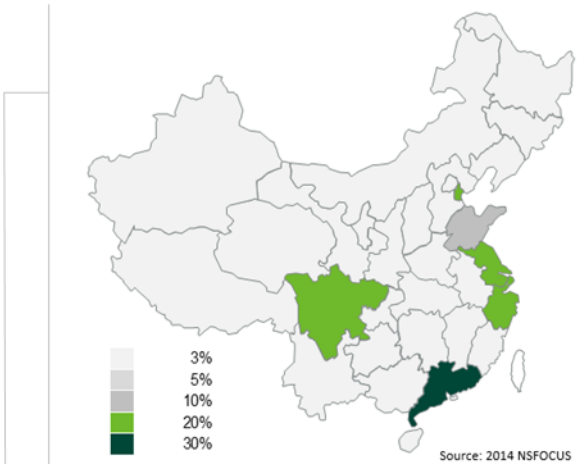
2014 下半年广东依然是最严重的受害区域。与 2014 上半年相比，广东占攻击的比例虽然下降，但是其下半年遭受攻击次数是上半年的 1 倍多，这充分反映了当前 DDoS 攻击活动的活跃程度。与 2013 下半年相比，变化最明显的是天津市，受害者数量不断上升，2013 年还在 10 名之外，到 2014 下半年已超过福建省位列第 4。在前 10 名受害区域中，除内陆省份陕西与四川外，其它受害区域均属沿海省市。

① http://blog.dnsimple.com/2014/12/incident-report-ddos/
② http://blog.1and1.com/2014/12/10/information-on-the-dns-outage-at-11-on-december-9-2014
③ http://www.telia.se/privat/driftinformation/2014/December/Problem-med-surf-och-digital-tv-avhj-lpt
④ http://www.northkoreatech.org/2014/12/23/north-koreas-internet-back-after-probable-attack/
⑤ https://status.rackspace.com/index/viewincidents?group=14&start=1419224400

BASED ON IN-REGION DDoS ATTACK STATISTICS

2014 H2广东依然是最严重的受害区域。与2014 H1相比，广东占全国受攻击的比例虽然下降，但是其下半年遭受攻击次数是上半年的一倍多。

2014 H2国内受攻击地区分布，绿色越深情况越严重



过去3个半年内，受攻击地区在国内各区域占比

	AH*	JX	BJ	HN	FJ	SX	XG	Other	SD	JS	SC	TJ	ZJ	SH	GD*
2013-2H	2.9	3.6	4.7	4.9	7.0	0.0	0.0	8.5	2.2	8.0	0.0	0.0	24.0	1.6	32.7
2014-1H	0.0	0.6	0.0	0.0	5.9	0.0	1.1	3.6	1.1	1.3	0.5	3.9	22.3	26.2	33.4
2014-2H	0.0	0.0	0.0	0.0	0.1	0.1	0.1	1.0	6.8	10.0	12.0	12.4	14.5	16.3	26.6

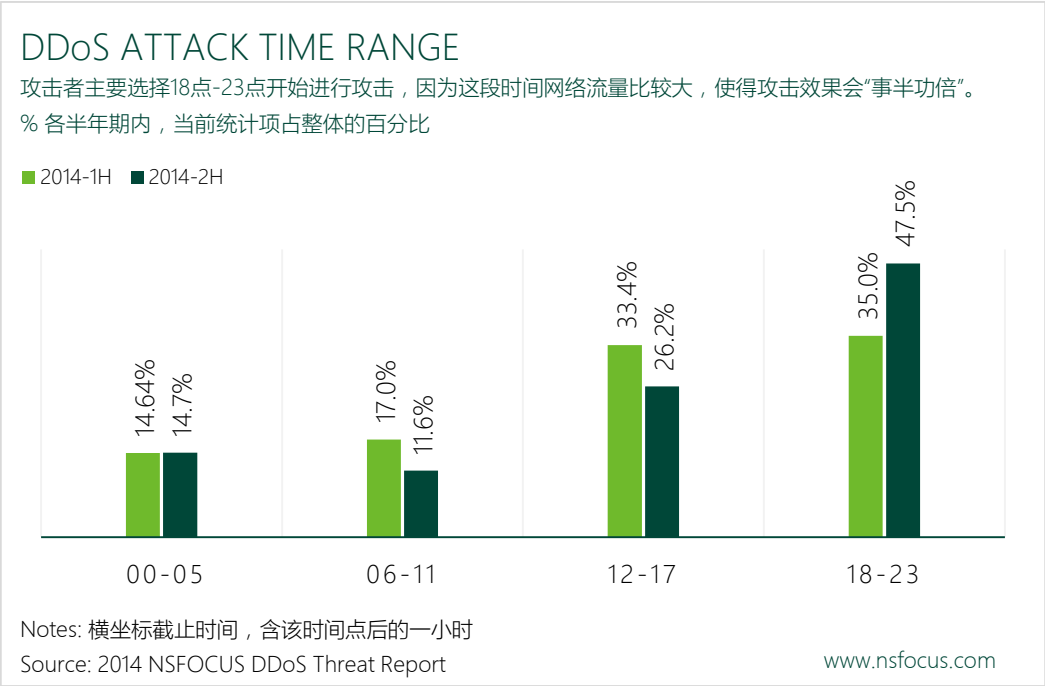
Notes: * 星号标注行均为省、直辖市、特别行政区等区域简拼

Source: 2014 NSFOCUS DDoS Threat Report

www.nsfocus.com

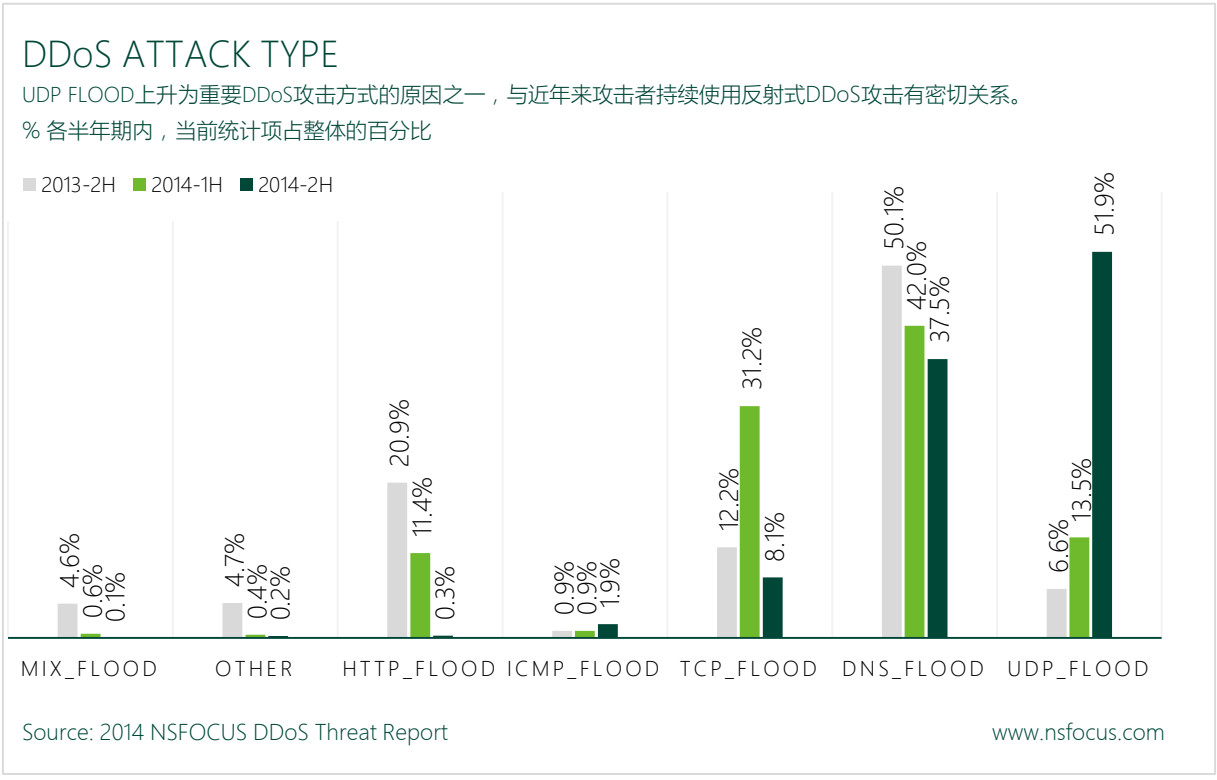
观点 3：18 点-23 点是 DDoS 开始攻击的主要时间段

下图表现了 2014 年 DDoS 攻击目标每半年的 DDoS 攻击开始时间。从中可以看出，在 2014 下半年 18 点-23 点（北京时间，GMT+8）是 DDoS 开始攻击的主要时间段（47.5%），其次是 12 点-17 点的时间段（26.2%）。攻击者主要选择 18 点-23 点开始进行攻击，这是因为这段时间网络流量比较大，使得攻击效果会"事半功倍"。



观点 4：UDP FLOOD 成为最主要的 DDoS 攻击方式

绿盟科技的监测数据显示，2014 下半年 UDP FLOOD 超越 DNS FLOOD 成为当前最主要的 DDoS 攻击方式，占总数的 51.9%。DDoS 攻击方式的变化反映了在网络攻防对抗中，不断动态演进的攻防技术发展，例如：攻击者对数据包到目标站点经过的各节点进行试探，在发现网络链路上的薄弱环节后再发动攻击。UDP FLOOD 上升为重要 DDoS 攻击方式的原因之一，与近年来攻击者持续使用反射式 DDoS 攻击有密切关系。



事件 2：SSDP 反射式 DDoS 攻击实例分析

在 2014 年下半年 SSDP 反射式 DDoS 攻击次数显著上升，这种攻击的基本过程如下图所示。首先攻击者将伪造 IP 地址的 M-SEARCH UDP 数据包发送给众多 UPnP 设备；然后这些 UPnP 设备向受害者 IP"返回"响应数据包；最后当受害者无法处理由于这些 UPnP 设备产生的反射攻击流量时，导致被攻击目标陷入拒绝服务状态。根据已监测到的 SSDP 反射式 DDoS 攻击数据，其攻击带宽放大倍数（BAF，即 UDP Payload 比值）在 30 左右。

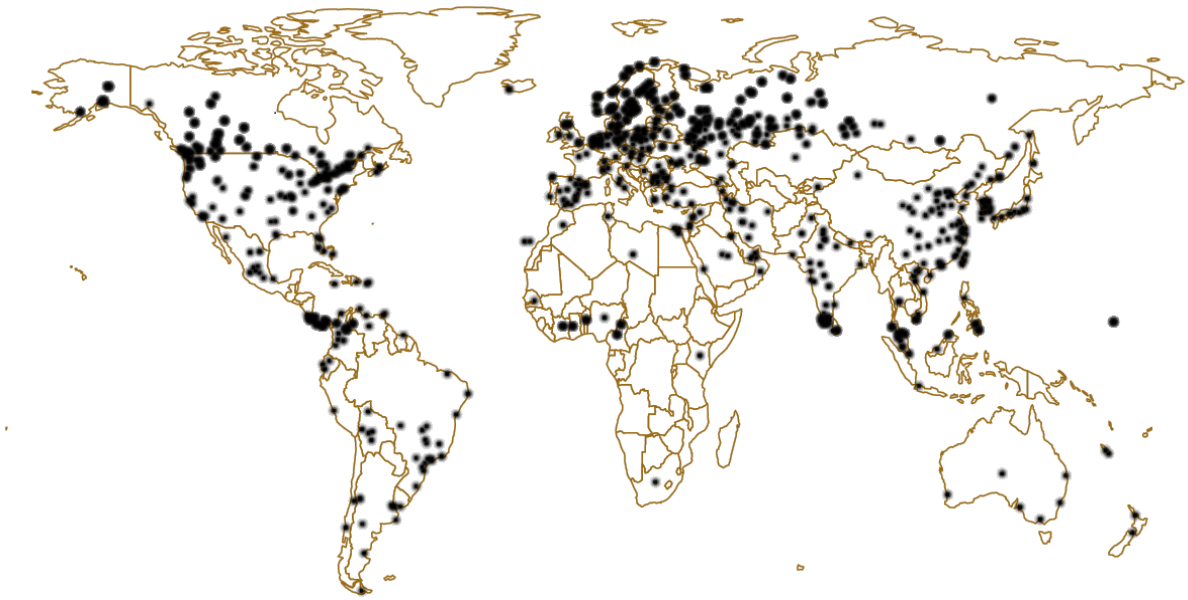
下图是在现网设备捕获到的 SSDP 反射式 DDoS 攻击（利用 SSDP 反射攻击 DNS 服务器）

2014-11-12 04:02:12	UDP-DNS-Flood	[redacted]	[redacted]	1900	53	DNS
2014-11-12 04:02:12	UDP-DNS-Flood	[redacted]	[redacted]	1900	53	DNS
2014-11-12 04:02:12	UDP-DNS-Flood	[redacted]	[redacted]	1900	53	DNS
2014-11-12 04:01:40	UDP-DNS-Flood	[redacted]	[redacted]	1900	53	DNS

攻击的请求报文样例：

```
Hypertext Transfer Protocol
  M-SEARCH * HTTP/1.1\r\n
  Host: [redacted]:1900\r\n
  Man: "ssdp:discover"\r\n
  MX: 5\r\n
  ST: ssdp:all\r\n
  \r\n
  [Full request URI: http://[redacted]:1900*]
  [HTTP request 1/10]
  [Response in frame: 2]
```

从上图可以看到，攻击者向 UPnP 设备发送 M-SEARCH 请求，并将 ST（Search Target）设置为 ssdp:all （即搜索所有设备和服务）。如果考虑到全球可被利用的 UPnP 设备数量，则很容易看出这种反射式 DDoS 攻击会给互联网带来非常巨大的影响。绿盟科技近期对世界范围内的 SSDP 服务进行监控时，发现 700 多万台 SSDP 设备（Controlled Device）能够被利用进行 SSDP 反射式 DDoS 攻击。



根据统计结果，SSDP 协议的平均带宽放大倍数（BAF）是 37，最常见的放大倍数是 24 和 32；SSDP 协议的平均包放大倍数（PAF）是 8.7。对 SSDP 设备放大倍数按升序排序，则前 10% SSDP 设备的平均带宽放大倍数是 14，而后 10% SSDP 设备的平均带宽放大倍数是 75。

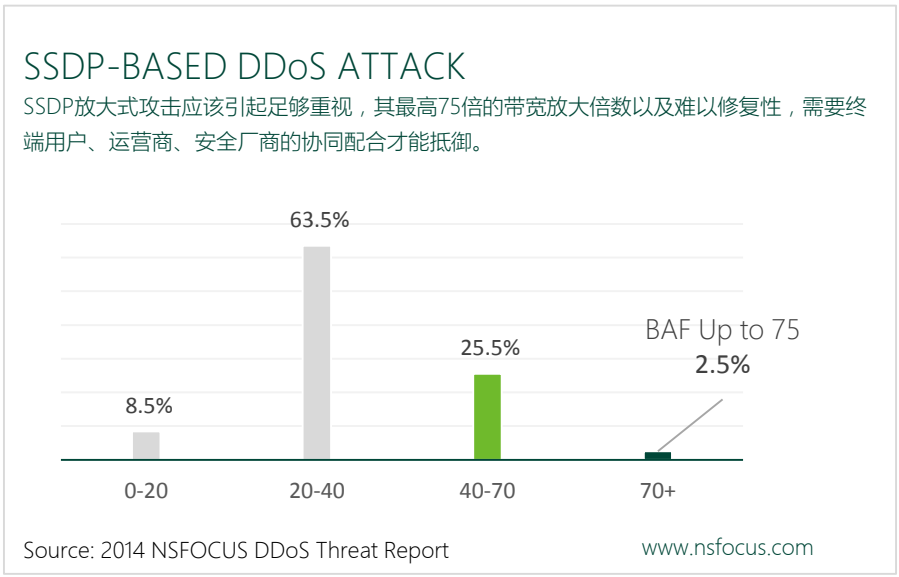
BAF 及 PAF 在本报告中的计算方式

BAF= 服务器向受害者发送 UDP 包的 payload / 攻击者向服务器发送 UDP 包的 payload

PAF= 服务器向受害者发送 IP 包的个数 / 攻击者向服务器发送 IP 包的个数

Notes: 上式中服务器是指可被利用进行反射攻击的 NTP、DNS、CharGen、SSDP 等。
如果有任何疑问，请致函 zhaogang@nsfocus.com

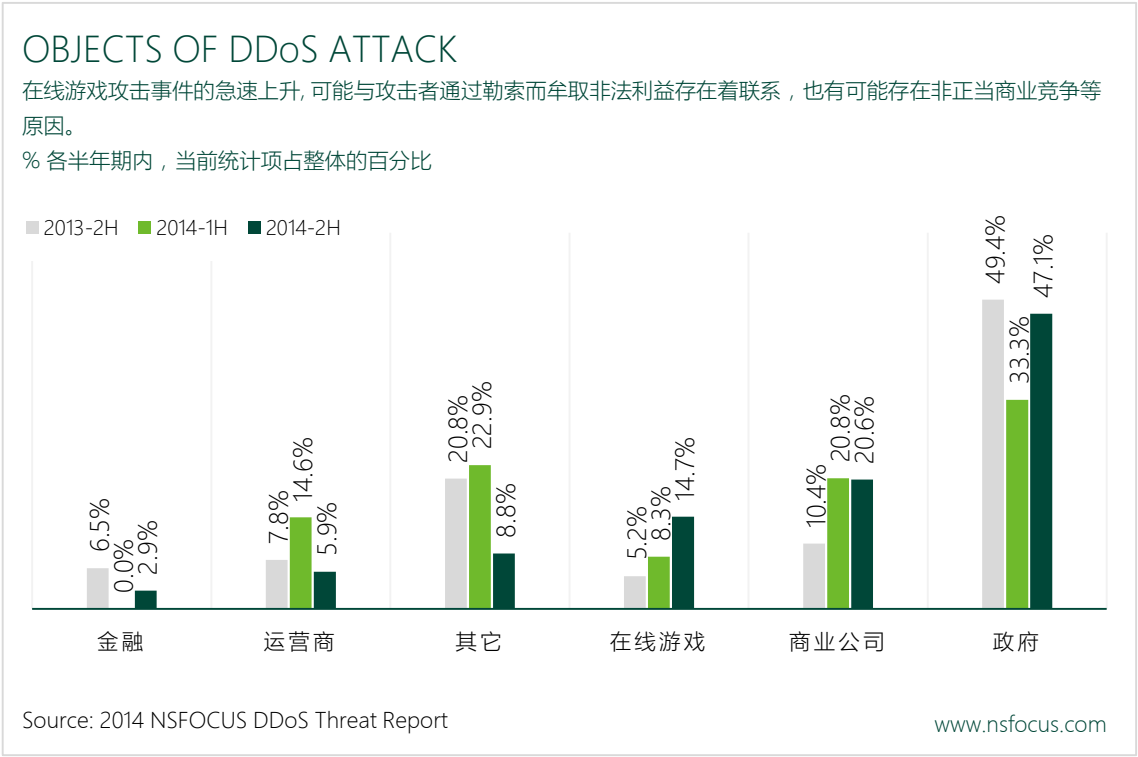
这些 SSDP 设备的放大倍数分布状况如下：



基于 SSDP 协议的反射攻击在很长时间内将难以修复。由于影响的设备范围广，手段多样以及攻击效果明显，可以预见的是越来越多的攻击者会利用/改进这种攻击的手段和方式。从应对反射攻击的思路上看，这种类型攻击需要终端用户、运营商、安全厂商协力配合，从各个层面阻击才能最大程度的保证用户业务的可靠性。

观点 5：在线游戏已进入 DDoS 攻击目标前 3

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 下半年政府网站依然是 DDoS 攻击最主要的目标，占总数近一半，其次则是针对商业公司的攻击。与 2014 上半年相比，运营商受到的攻击比例有所下降，而在线游戏和金融行业则有所上升。与 2013 下半年相比，最明显的区别是针对在线游戏的 DDoS 显著增加，游戏行业一直是 DDoS 攻击的主要目标之一，这是因为在线游戏对于游戏服务器的服务质量要求很高，在 DDoS 攻击影响游戏正常运行时，玩家常会责怪游戏服务器"太慢、易掉线"，如果频繁出现这些状况，玩家极有可能选择离开，从而直接导致该款游戏在线盈利能力下降。攻击者之所以喜欢将在线游戏作为攻击目标，这可能与攻击者通过勒索而牟取非法利益存在着联系，也有可能存在非正当商业竞争等原因。

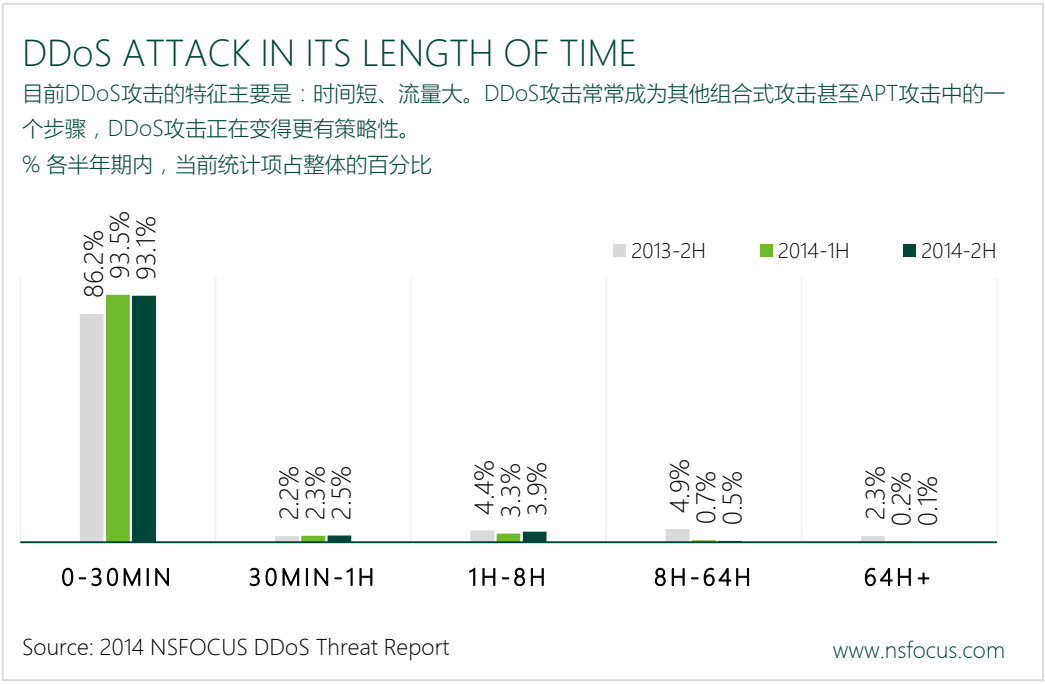


观点 6：93% DDoS 攻击发生在半小时内

从 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。目前 DDoS 攻击的重要特征是：持续时间短、但攻击流量大。攻击者采用这种攻击策略的目的至少有：

1. 闪电战：试图在检测发现攻击至启动清洗服务的时间间隔内进行攻击，以更有效率地对目标实施 DDoS 攻击；
2. 干扰战：对攻击目标进行 DDoS 攻击，只是吸引攻击目标 IT 工作人员的注意力，掩护攻击者采取其它攻击方式；
3. 游击战：通过长期 DDoS 攻击网站，意图恶意阻碍网站的正常访问，常常是"打一枪就走"。

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 下半年，绿盟科技云安全运营中心监测到持续最久 DDoS 攻击长达 70 个小时。



预测 2015

现状值得我们去分析，是因为它是未来的先兆。如果 2015 年不会出现颠覆性的技术变革，或是重大的政治宗教冲突。那么，我们可以对 DDoS 的数量、方法和对象提出一些预测。其中反射式 DDoS 攻击尤其值得重视，所以本节从技术和威胁角度给出了更详细的分析。

DDoS 攻击峰值流量将再创新高

DDoS 攻击峰值流量逐年上升,这一方面是由于攻击技术的不断发展，另一方面也是由于网络带宽等可利用资源显著上升。 因此预期 2015 年 DDoS 攻击峰值流量较 2014 年将有明显增长，甚至可能会进入 1Tbps 时代。

反射式 DDoS 攻击技术会继续演进

从防护角度看反射式 DDoS 攻击易于检测与缓解，这是因为攻击数据包的源端口相对固定；然而从攻击角度看，这种 DDoS 攻击方式具有隐匿攻击者真实身份、攻击者无需组建僵尸网络、对攻击者的网络带宽要求小等优势。在 2014 年下半年，基于 SSDP 协议 DDoS 反射式攻击次数显著上升。预计这种高效、低成本的 DDoS 攻击技术还将为攻击者提供更多的攻击选项。

DNS 服务将迎来更多的 DDoS 攻击

2014 下半年多次重大 DDoS 攻击中都使用了 DNS FLOOD，这主要是因为 DNS 协议设计存在安全缺陷、许多 DNS 服务器运维存在安全隐患等导致，从而使得 DNS 服务器自然而然地成为攻击者瞄准的重要攻击对象。

针对行业的 DDoS 攻击将持续存在

近年来针对金融、能源等行业的 DDoS 攻击时有发生，一些行业甚至长期面临 DDoS 攻击的困扰。虽然目前各种缓解 DDoS 的技术不断发展，但是从攻击者角度看 DDoS 攻击简单易行，只要其行之有效则会持续存在。

结束语

拒绝服务攻击存在的根源是 Internet 架构自身缺陷，正如 RFC 4732 所说，"由于最初 Internet 架构未考虑拒绝服务攻击，从而导致几乎所有 Internet 服务均易遭受拒绝服务攻击"。纵观近 5 年 DDoS 攻防双方的对抗交锋，攻击方技术不断演进，将"以大欺小"（流量型攻击）与"以小搏大"（资源耗尽型）两种攻击方式组合起来，利用逐渐提高的网络带宽增强攻击力等；而防守方则通过流量清洗设备等多种手段予以应对。

从绿盟科技长期跟踪与分析的 DDoS 数据可以看出，攻击者行为是在不断变化，网络环境的演进使得攻防的战场更为复杂。相信报告中所述观点，对于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。

"能因敌变化而取胜，谓之神"，面对 DDoS 攻击目前所呈现的不断演变与浪潮冲击，您做好准备了吗？

您还想看什么内容？

您可以联系报告作者，将您的见解与我们分享，如果您有更多想看的内容，也可以告诉我们，在这里先行致谢！

请致函 zhaogang@nsfocus.com

作者和贡献者

作者

赵刚，绿盟科技 Email：zhaogang@nsfocus.com

绿盟科技威胁响应中心研究员，主要研究领域为态势感知和信息安全事件分析。

马乐乐，绿盟科技 Email：malele@nsfocus.com

绿盟科技北京研发中心研发工程师，主要进行 DDoS 攻防相关的研究。

贡献者

何坤，绿盟科技 Email：hekun2@nsfocus.com

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

赵刚库，绿盟科技 Email：zhaogangku@nsfocus.com

张振风，绿盟科技 Email：zhangzhenfeng@nsfocus.com

DDoS 威胁报告

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

关注 DDoS 威胁报告

如果您希望与我们一起持续关注这个项目，请关注：

- 访问更多 DDoS 安全报告：http://www.nsfocus.com/4_research/4_6.html
- 绿盟科技威胁响应中心微博：http://weibo.com/threatresponse
- 绿盟科技官方微博：http://weibo.com/nsfocus
- 绿盟科技官方微信：搜索公众号 绿盟科技

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