doi:10.3969/j.issn.1000-436x.2014.z1.007

基于 NTP 反射放大攻击的 DDoS 追踪研究

姜开达，章思宇，孙强
（上海交通大学 网络信息中心，上海 200240）

摘 要：提出了一种利用 NTP 反射型放大攻击的特点，通过对中国大陆开放公共 NTP 服务的主机定期发起主动探测（执行 monlist 指令），利用返回信息对全球范围 NTP 反射类 DRDoS 攻击事件进行长期追踪观察和统计分析。追踪从 2014 年 2 月开始，初始探测范围为大陆近 1.4 万台 NTP 服务主机，每隔 2 h 一个周期持续进行了 164 天，观测到了针对数十万个 IP 地址的疑似 DDoS 攻击行为。

关键词：NTP；反射型放大攻击；DDoS；DRDoS；行为追踪
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2014)Z1-0031-05

Research on tracking DDoS based on NTP reflection amplification attack

JIANG Kai-da, ZHANG Si-yu, SUN Qiang
（Network and Information Center，Shanghai Jiaotong University, Shanghai 200240, China)

Abstract: Based on characteristics of NTP reflection amplification attack, proposes a method of regularly launching active detection to hosts of public NTP services in Chinese mainland (execution of monlist instruction) and doing a long-term follow-up observation and statistical analysis of global NTP reflection DRDoS attacks based on the return information. The track began in February 2014, the initial detection range covered 14 000 NTP servers in China mainland, and detection period is 164 days with two hours for each cycle, observed suspected DDOS attacks against hundreds of thousands of IP addresses.

Key words: NTP; reflection amplification attack; DDoS; DRDoS; behavior tracking

1 引言

DDoS(distributed denial of service)攻击每时每刻都在互联网上频繁发生，是目前网络安全领域已知威力最强，同时也最难防御的攻击方式。早期 DDoS 攻击以发大网络流量，耗尽网络带宽资源引发目标不可访取胜，主要表现为 UDP/ICMP Flood 等，后来发展到利用协议和应用软件漏洞的低速流量攻击，主要方式有 Slowloris 慢攻击、PHP Hash 冲突碰撞攻击、HTTP Header 攻击等。如今有威胁的 DDoS 主流攻击方式大多是混合型，例如 SYN Flood、DNS 放大攻击、SNMP 反射放大攻击、NTP(network time protocol)反射放大攻击等。

随着以 Zmap 为代表的互联网大规模扫描技术发展和全球互联网带宽的增加，各种简单易用的 DDoS 工具扩散和僵尸网络的传播，以及庞大的用户终端和服务器群体存在漏洞等因素，实施 DDoS 的门槛和成本越来越低，并且对于分布式的反射型攻击事件，追踪溯源及其困难。这些攻击不仅长期困扰 IDC 服务提供商，也给互联网安全运行带来不稳定因素。

2013 年 11 月以来，全球范围内 NTP 反射放大攻击事件频发，成为 2014 年上半年 DDoS 的最典型攻击手段，并且超过百 G 的攻击流量屡有出现，严重影响了互联网的正常安全稳定访问。2014 年 2 月，美国知名云安全公司 CloudFlare 公布其持续遭受史无前例的 400 Gbit/s 流量 NTP Flood 攻击[1]，CNCERT（国家互联网应急中心）也在 3 月发布的预警报告中称中国电信 2014 年 2 月初国际出入口的 NTP 攻击流量最高达到 300 Gbit/s[2]。

收稿日期：2014-10-15

本文对DRDoS（分布式反射攻击）类型的主流攻击方式-NTP 反射放大攻击机制进行了论述，并通过长期的主动探测手段和后期数据分析来对相应DDoS攻击事件进行持续追踪和深入研究。

2 NTP反射放大攻击机制

2.1 反射型原理

DDoS 反射攻击是指利用路由器、服务器等设施对大量请求产生应答，从而产生反射攻击流量并同时隐藏攻击来源的一种流行 DDoS 手段[3]。NTP可以提供高精度的时间校正服务，使用开放123端口的 UDP 协议。客户端发送请求查询分组到服务端，服务端返回相应响应分组给客户端，由于UDP是面向无连接的协议，所以过程中请求分组的源IP很容易伪造。如果把请求分组中的源IP修改为攻击目标IP，服务端返回响应分组就会大量涌向攻击目标，形成反射型攻击。

2.2 高放大倍数

在提供NTP服务的ntpd低版本（4.2.7p26之前均存在CVE-2013-5211漏洞）下，远程请求monlist指令可以获取和NTP服务端曾进行请求的最后600个客户端IP地址列表等相关信息[4]。发送一个很小的请求分组（小于235 byte，例如：ntpdc -n -c monlist ntpserver's IP address），就能获取到一组由大量活动IP 地址组成的连续 UDP 分组(表 1 为上海电信某NTP 服务器部分返回内容示例)，每个响应分组内含6个最近请求的IP信息，根据请求NTP服务端的繁忙程度，每次最多可以返回100个分组（每个分组为440 byte）。攻击者通过伪造源IP地址，并向NTP服务端持续发送精心构造的monlist请求分组，可以将攻击流量放大到556.9~4 670倍[5]。恶意攻击者可以通过编写自动化攻击脚本来继续降低构造的请求分组长度，也能够随机伪造不同源 IP 地址来迅速填满NTP服务端的最近600个访问IP地址空间，并同时向大量的可利用公共NTP服务器发起频繁请求，以获得高放大比攻击效果。

由表 1 可见排名前 8 位的远程访问 IP 地址（remote address）对应的源端口（port）都是80或8 080，这是常用的Web服务端口，同时其最近请求统计分组数（count）也显著偏高，因此可以判定NTP服务器101.227.12.9被利用作为反射源放大攻击这些Web服务器。排名第9~12位的IP地址对应来源国家分别为匈牙利、法国、美国、英国，虽然其源端口并非常规Web端口，但是也不是正常NTP客户端所常用的123端口，并且统计次数也表明其被非正常高频访问，仍然可以综合判断是被不当利用进行放大攻击。

2.3 同类型攻击

DDoS 放大攻击是一种特殊类型的反射型攻击，其利用需要满足一系列前提条件。首先响应数据流量要显著大于请求触发的数据流量，只有拥有足够高的反射比，以小搏大的攻击效果才会明显。其次攻击利用的协议不能要求认证和握手，因为反射型攻击需要伪造攻击目标的IP地址来发起请求，所以绝大多数利用的都是无连接的 UDP 协议来完成。最后存在漏洞且可以被远程利用的反射设备要

表 1 **客户端执行 monlist 命令请求返回内容**

remote address	port	local address	count	m	ver	rstr	avgint	lstint
87.78.66.249	80	101.227.12.9	9 596	7	2	0	0	0
64.15.129.232	80	101.227.12.9	6 480	7	2	0	0	0
108.17.9.156	80	101.227.12.9	7 523	7	2	0	0	0
46.165.210.131	80	101.227.12.9	350	7	2	0	0	0
46.165.210.148	80	101.227.12.9	1 186	7	2	0	0	2
71.203.68.184	8 080	101.227.12.9	219	7	2	0	21	5
173.32.98.151	80	101.227.12.9	164	7	2	0	3	6
107.170.223.127	80	101.227.12.9	131	7	2	0	15	83
37.221.210.15	27 226	101.227.12.9	11 676	7	2	0	0	223
91.121.60.36	3 306	101.227.12.9	1 622	7	2	0	0	233
192.210.150.174	27 226	101.227.12.9	942	7	2	0	3	245
86.19.247.107	5 223	101.227.12.9	10 878	7	2	0	0	671

在互联网上广泛存在，只有足够的规模才存在被利用的价值。

同时满足这些条件的除了 NTP 放大，还有 DNS 放大、SNMP 放大、CHARGEN 放大等，这两年来已成为混合型 DDoS 攻击的主要利用手段。2013 年 3 月，欧洲反垃圾邮件组织 Spamhaus 对外宣称受到了 300 Gbit/s 流量的 DNS 反射放大攻击，这些攻击流量据报告来自近 31 000 台开放 DNS 服务器[6]。

3　基于全网扫描的 NTP 服务识别

3.1　Zmap 端口扫描

Zmap 是由美国密歇根大学开发的开源 Internet Scanner，可以在短时间内高效完整扫描全球 IPv4 地址空间[7]。其不仅仅只是个寻找活跃主机的端口扫描器，还可以配合扩展应用探测模块，完成需要交互的网络应用识别和远程信息搜集。

本文研究扫描针对的范围为中国大陆地区的 3.3 亿个 IPv4 地址，数据来源于 APNIC（亚太互联网络信息中心）在其官方网站 2014 年 2 月份公布的大陆地址段信息，使用 CIDR（classless inter-domain routing）格式传递给 Zmap 的扫描配置文件。通过 Zmap 初级扫描，把研究访问的 IP 地址数量（仅判断是否响应 UDP 的 123 端口）从 3.3 亿降低到了 1 219 万。为了使结果尽可能接近真实情况，在不同时间段进行了 3 次扫描，最终取其并集进一步研究。

3.2　Nmap 应用扫描

Nmap 是一个历史悠久的用于网络发现和安全审计的开源 Network Scanner，是系统管理人员和网络管理人员常用工具。Nmap 可以判断网络中的主机存活、进行操作系统识别、检测开放端口服务类型和防火墙使用等。Nmap 允许使用 script 脚本插件来扩展应用识别功能，ntp-info 插件支持返回同步时间信息、服务端版本号、CPU 类型、其他系统信息等。ntp-monlist 插件支持返回上游时间源服务器地址和最近请求访问的客户端地址列表等信息。

利用 Zmap 的前期扫描结果（开放 UDP 123 端口）作为数据源，在 2014 年 2 月 20 日，通过 Nmap 配合相关插件进行二级扫描，把研究的 NTP 服务器范围从疑似的 1 219 万降低到了接近真实的 181 万（标准是有返回时间信息，表明提供公开 NTP 服务），同时确认存在支持 monlist 指令的只有 1.4 万，大大降低了研究对象数量级，便于后期针对性分析。

3.3　存在漏洞的 NTP 服务统计

181 万台公开 NTP 服务器返回统计信息如表 2 所示。虽然利用 Nmap 扫描判定的支持 monlist 放大，存在漏洞的比例不到 1%，但是由于基数太大，1.4 万台的绝对数量仍然非常可观。

表 2　Nmap 扫描大陆地区 NTP 服务器返回信息

NTP 服务器	数量
有返回时间信息	1 806 173
有返回版本信息	43 813
有返回系统信息	183 034
有返回 CPU 类型	43 498
支持 monlist 指令	13 628

4　追踪方法和分析

4.1　原始数据来源

从表 1 中可以看出，如果向被利用反射的 NTP 服务器发出 monlist 指令，会得到一系列返回信息。分析 remote address、port、local address、count、m、ver、rstr、avgint、lstint 等返回值，可以获知最近请求的 600 个源 IP 地址（或对应域名）、对应源地址最后一个分组的请求源端口、NTP 服务本地监听 IP 地址、从对应源地址收到的分组数、请求协议分组的模式、请求协议分组的版本号、限制标志位、从对应源地址收到的数据分组平均间隔、从对应源地址收到最近的数据分组间隔[8]。

基于这个原理，面向存在漏洞的 NTP 服务器群体定期发送特殊 monlist 探测分组，收集返回值并汇聚分析，会得出一系列有价值的结论。追踪从 2014 年 2 月 25 日正式开始，到 8 月 7 日结束，持续进行了 164 天。初始探测范围为 2 月中旬扫描探测得到的中国大陆当时仍然存在 NTP 反射放大漏洞主机（约 1.4 万台），以每隔 2 h 为一个周期对这些 NTP 服务器发起轮询请求（相当于每 2 h 对攻击利用情况做一次快照），共获得了 2 589 199 组返回数据（每组最大返回 600 条地址相关信息），近 3.8 亿条原始信息，观测到了针对数十万个 IP 地址的疑似 DDoS 攻击行为。

为了使返回 remote address 值为规整的数字 IP 格式，使用了 ntpdc -n -c monlist 参数来取回相应信息，避免了出现返回域名的现象。为了解决高并发的快速查询，使用了 Golang 语言来底层实现请求，并把返回结果定期记录到本地文件。后期的数据分

析使用了 PostgreSQL 关系型数据库和 awk/sort/grep/wc 等 Linux 脚本语言来实现。

4.2 反射 NTP 主机数量变化趋势

在不同的历史阶段，被利用的反射 NTP 主机数量是在动态变化的。由于有了长期的数据积累，就可以定量地来描述这个变化过程。图 1 是 2014 年 2 月~7 月期间被利用反射 NTP 主机数量变化趋势。

从图 1 中可见，在 2014 年 2 月末到 3 月初，反射 NTP 主机数量有两阶段明显剧减的过程，这主要和几方面因素相关。首先 NTP 系统管理人员安全意识提高并主动采取了更新 ntpd 版本，限制访问范围，修改配置文件等诸多增强安全措施；其次国内基础电信运营商在全国主干网采取了措施来限制 123 端口的 UDP 访问，这个效果非常明显，从监测上看一两天之内相应主机数量直线下降。

从 2014 年 3 月中旬开始，反射 NTP 主机数量开始缓慢的递减，呈现了长尾效应。不过在 6 月开始，反射主机数量又有了新的小幅反弹，这显示仍然不断有新的反射主机在加入，但总体上看数量相对还是比较稳定，没有出现剧烈震荡。随着反射主机数量的减少，利用其发起 DDoS 的攻击效果相对 3 月以前已经有所下降，但由于基数仍然不低，还是能保持相当的攻击强度。

4.3 数据误差分析

从原始数据处理后的 3.5 亿条有效记录当中，仍然存在有正常的 NTP 访问，为了避免干扰分析，这些正常请求数据需要被尽量剔除。数据清洗依照以下几条原则依次进行。

1) 返回 remoteip 为不应在全球互联网上出现的保留地址、私有地址、D 类地址、E 类地址[9]都不认为是 DDoS 攻击行为。这些数据有 41 311 599 条，大约占总数据量的 11.73%。

2) 返回请求分组数 count 小于 3 的数据由于数量太小，不构成 DDoS 攻击威胁，这些请求可能是正常的 NTP 请求，也可能是攻击者为了达到攻击效果最大化，填满 600 个地址空间而发的少量随机源 IP 地址请求。这些数据有 44 424 897 条，大约占剩余总数据量的 14.29%。

3) 返回请求源端口为 123，且请求协议分组模式 *m* 不等于 7，请求协议分组版本号 ver 不等于 2，这些请求可能是正常的 NTP 请求。这些数据有 5 754 666 条，大约占剩余总数据量的 2.16%。

4) 返回源地址收到的数据分组平均间隔 avgint 大于 60 s，且请求协议分组模式 *m* 不等于 7，请求协议分组版本号 ver 不等于 2，这种频率的请求也不足以产生 DDoS 威胁。这些数据有 3 091 588 条，大约占剩余总数据量的 1.19%。

经过多轮清洗之后，最终形成了供分析 DDoS 的 2.6 亿条最终数据。

4.4 攻击目标分布

通过分析 monlist 返回信息中的源端口，可以了解攻击者的利用方式。表 3 所示为排名前 10 的放大攻击利用源端口分布。

由表 3 可见，针对 80 端口的反射放大攻击占比超过 50%，利用次数最频繁，被攻击 IP 目标也最多。由于反射放大攻击是和端口无关的流量型攻击，所以其他端口同样可以被利用。根据相关数据统计分析，最常见的 Top5 端口可以覆盖 70.3%的攻击行为，最常见的 Top10 端口可以覆盖 75.9%的攻击行为，这些数据对 DDoS 攻击的抑制提供了直接参考。

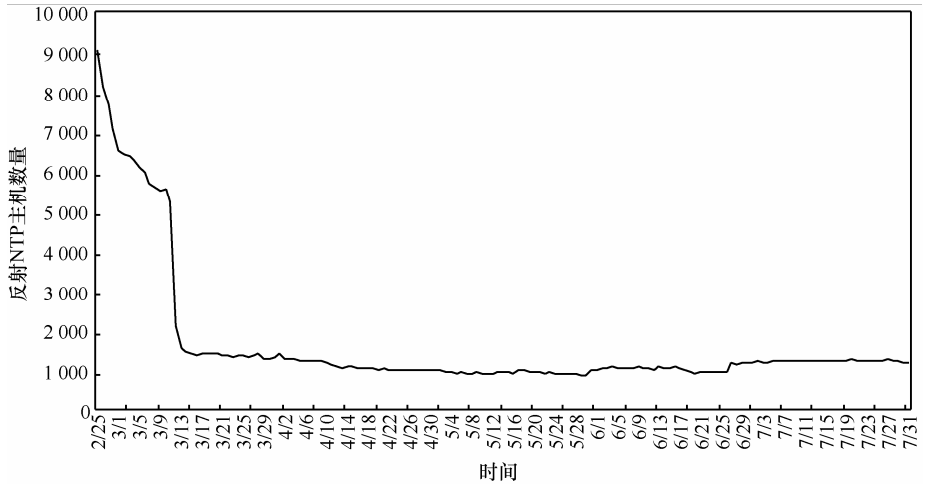


图 1 中国大陆地区 2014 年 2 月~7 月反射 NTP 主机数量变化趋势

表 3　NTP 放大攻击利用源端口分布

源端口	出现次数	百分比/%	对应不同 IP 数量
80	139 138 322	54.01	261 023
3 074	21 937 198	8.52	68 604
5 223	9 486 832	3.68	25 845
53	6 151 737	2.39	21 727
22	4 394 336	1.71	6 224
25 565	4 308 035	1.67	6 286
123	3 009 873	1.17	43 476
3 040	2 451 088	0.95	3 101
27 015	2 418 990	0.94	3 063
8 080	2 261 423	0.88	6 629

以攻击 80 端口的典型 DDoS 为例，波及的 26 万个网站服务器 IP 对应的地域分布如表 4 所示，可见互联网数据中心业务高度发达的北美和欧洲是被攻击的重灾区。3074 端口也是常见发起 DDoS 的源端口，涉及的近 7 万个网站服务器 IP 对应区域分布也和表 4 类似，前 10 名排序依次为美国（54.68%）、英国（10.74%）、法国（8.42%）、加拿大（6.93%）、澳大利亚（4.36%）、德国（2.97%）、墨西哥（2.41%）、西班牙（1.38%）、新西兰（1.00%）、荷兰（0.86%）。端口的差异意味着可能使用了不同的攻击工具，这 2 种常见源端口的攻击目标统计分布还是高度重合的。

表 4　被 DDoS 攻击 80 端口的网站地域分布

网站 IP 数量	国家/地区	百分比/%
95 028	美国	36.41
24 067	法国	9.22
19 369	英国	7.42
15 144	加拿大	5.80
12 565	德国	4.81
10 852	澳大利亚	4.16
8 701	巴西	3.33
8 073	荷兰	3.09
5 930	俄罗斯	2.27
4 167	波兰	1.60

5　结束语

DDoS 对全球互联网的安全有着长期和深远的影响，只有更深入了解其产生和发展全过程，才有可能预测其未来走向，并针对性的采取各种可行措施来降低其威胁程度。这不仅仅要依靠各种被动的异常监测系统，也需要进行一系列主动安全探测来发现，基于 NTP 反射放大的 DDoS 追踪正成为其中的一个方向。

参考文献：

[1] Matthew prince, technical details behind a 400 Gbit/s NTP amplification DDoS attack[EB/OL]. http://blog.cloudflare.com/technical-details-behind-a-400gbit/s-ntp-amplification-ddos-attack

[2] CNCERT. 关于警惕近期多发 NTP 反射放大攻击的预警通报[EB/OL]. http://www.cert.org.cn/publish/main/10/2014/20140314085001237248948/20140314085001237248948_.html, 2014.
CNCERT. On guard against recent multiple NTP reflection/ amplification attacks alert notification [EB/OL]. http://www.cert.org.cn/publish/main/10/2014/20140314085001237248948/20140314085001237248948_html, 2014.

[3] 洪海. DDoS 放大攻击原理及防护方法[EB/OL]. http://www.nsfocus.com/images/6_about/journal/12_20_023_j.pdf, 2013.
HONG H, DDoS amplification attacks principles and protective methods [EB/OL]. http://www.nsfocus.com/images/6_about/journal/12_20_023_j.pdf, 2013.

[4] KUHRER M, HUPPERICH T, ROSSOW C, *et al*. Exit from hell? reducing the impact of amplification DDoS attacks[A]. 23rd USENIX Security Symposium[C]. San Diego, California, 2014.

[5] Christian Rossow, amplification hell: revisiting network protocols for DDoS abuse[A]. 21st Network and Distributed System Security Symposium[C]. San Diego, California, 2014.

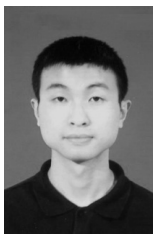
[6] JENKINS Q. Answers about recent DDoS attack on spamhaus [EB/OL]. http://www.spamhaus.org/news/article/695/answers-about-recent-ddos-attack-on-spamhaus,2013.

[7] DURUMERIC Z, BAILEY M J, HALDERMAN A. An internet-wide view of internet-wide scanning[A]. 23rd USENIX Security Symposium[C]. San Diego, California, August 2014.

[8] WALT KELLY P. ntpq-standard NTP query program[EB/OL]. http://www.eecis.udel.edu/~mills/ntp/html/ntpq.html, 2012.

[9] IANA. IANA IPv4 address space registry[EB/OL]. http://www. iana.org/assignments/ipv4-address-space/ipv4-address-space.xml,2014.

作者简介：



姜开达（1980-），男，安徽池州人，上海交通大学工程师，主要研究方向为网络与信息安全。

章思宇（1989-），男，上海人，上海交通大学助理工程师，主要研究方向为网络与信息安全。

孙强（1975-），男，山东郓城人，上海交通大学助理工程师，主要研究方向为系统运维和网络安全。