CERNET 中的 UDP DRDDOS 攻击

李刚，丁伟，夏震

(东南大学计算机科学与工程学院，江苏南京 211189)

摘要：UDP DRDDOS 攻击是一类利用应用层网络协议漏洞发动的反射式 DDOS 攻击。本文简述了这类 DDOS 攻击的原理，参考了 Arbor[5]的一份有关 UDP 反射攻击的报告，在一个面向流记录的网络管理平台—NBOS 上，对上述报告中提出的几种反射攻击在 CERNET 全网范围进行了检测，发现了大量活跃的被利用进行攻击的主机，并对检测的数据进行了统计分析。

关键词：UDP DRDDOS；流记录；NBOS；攻击分析

1 引言

UDP DRDDOS，也叫 UDP 反射 DDOS 攻击，是一类特殊的 DDOS 攻击形式。在此类攻击中，攻击者通过伪造被攻击主机地址，向网络上有漏洞的主机发送基于特定 UDP 服务的请求报文，这些请求的回复会被放大数倍后发送到被攻击主机从而达到攻击目的[1]。其攻击场景如图 1 所示：

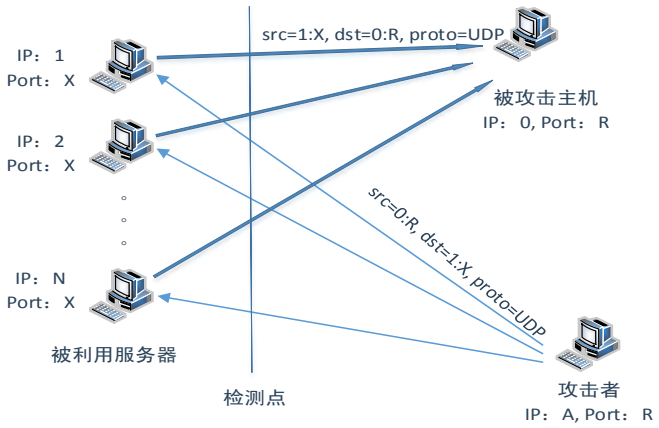

图 1 反射 DDOS 攻击场景

反射 DDOS 攻击不依赖于数量巨大的傀儡机，实现起来更方便、攻击源不易被追踪，并且攻击中表现出的流量放大特点使攻击效果比较理想，因此它已经成为互联网上最近非常活跃的一类攻击手段。

2 反射 DDOS 攻击的研究现状

早在 1996 年就有学者指出了字符发生器协议(Chargen，Character Generator Protocol)存在这方面的漏洞[2]。Paxson 于 2001 年对 TCP、UDP、IP 等常见协议中潜在的可被用来进行反射攻击的字段进行了系统性研究[3]，研究报告中的 DNS、SNMP 等协议在现阶段已经成为主流的反射攻击协议。2014 年，德国波鸿大学的一篇研究报告对 14 种 UDP 协议进行了实验性研究[4]，认为这些协议存在实施反射攻击的可能，并对攻击的危害程度进行了对比分析。

来自设备厂商 Arbor ATLAS 的一份报告显示， 5 种基于 UDP 的反射攻击在实际网络环境中是可见的，它们分别是 Chargen，SNMP，DNS，NTP 和 SSDP。攻击者利用上述协议的漏洞，通过扫描的方式确定服务的开放性，之后针对性地发动攻击。以上 5 种 UDP DRDDOS 攻击，我们利用布置在 CERNET 主节点网络边界提供的流记录数据，均可以检测到。

3 基于流记录的反射攻击行为主机检测

3.1 检测算法

针对 Chargen 反射攻击，文献[1]提出了一种基于端口匹配和流量阈值的检测算法，用于检测网内有反射攻击行为的主机。在该算法基础上，我们将其中的端口进行扩展，尝试覆盖 19 号、123 号、1900 号、161 号和 53 号端口。

3.2 算法实现

NBOS（Network Behavior Observation System）是 CERNET 华东北地区网络中心在国家科技支撑计划课题“新一代可信任互联网安全和网络服务”支持下开发的用于监控和管理 CERNET 网络服务质量和网络安全状态的新型网络管理系统，它基于流记录工作，以不同的时空尺度提供网络的基础运行数据。2014 年 NBOS 完成了一次升级，升级后的版本是 NBOS-S3.0，可以支持的数据源是 V5 或 V9 格式的 netflow 或 netstream，采用 B/S 结构工作。目前已经在 CERNET 全部 38 个主节点所管理的网络边界部署，稳定运行时间超过 1 年。

我们将上述反射攻击检测算法在 NBOS 平台上实现，并部署到 38 个主节点。在实际检测中我们发现，由于 NBOS 使用的分析数据源存在瑕疵[1]，影响到对 SNMP(161 端口)和 DNS（53 端口）两种反射攻击检测，尝试的几种补偿方案经实际环境检测准确率不能达到要求，因此目前正式运行的 NBOS 平台上的检测算法只覆盖针对 Chargen，NTP 和 SSDP 这 3 种协议的反射 DDOS 攻击。

部署在 38 个主节点的 NBOS 驻地节点检测出的被管网内攻击服务器相关信息除了存储在本节点数据库中，还周期性地汇报至 NBOS 总控节点汇总。本文第 4 节中的综合统计中的所有分析数据均是总控汇总后的结果。

4 检测结果的统计和分析

实际检测时，算法实际使用的阀值是在一个 5 分钟的 NBOS 时间粒度中，面向单个网外主机的网内主机上述端口 UDP 流量超过 20MB。针对 Chargen、NTP 和 SSDP 反射攻击，我们根据各主节点 NBOS 驻地系统在 2 月 10 日到 3 月 9 日这 28 天内发回总控的全网的攻击数据，形成下面的统计分析。

4.1 总体攻击情况数据统计

图 2 是主节点在统计时间内参与三种攻击的网内活跃主机数。需要说明的是在这个统计中我们滤掉了整个统计期间发送攻击流量少于 50MB 的主机，另外由于 pop15 节点的 19、123、1900 端口参与攻击的主机数量分别为 72、9、320 台，总数为 401 台，数量较其他节点多出 2 倍以上，为了不影响其他节点的显示精度，图中未显示该点数据。

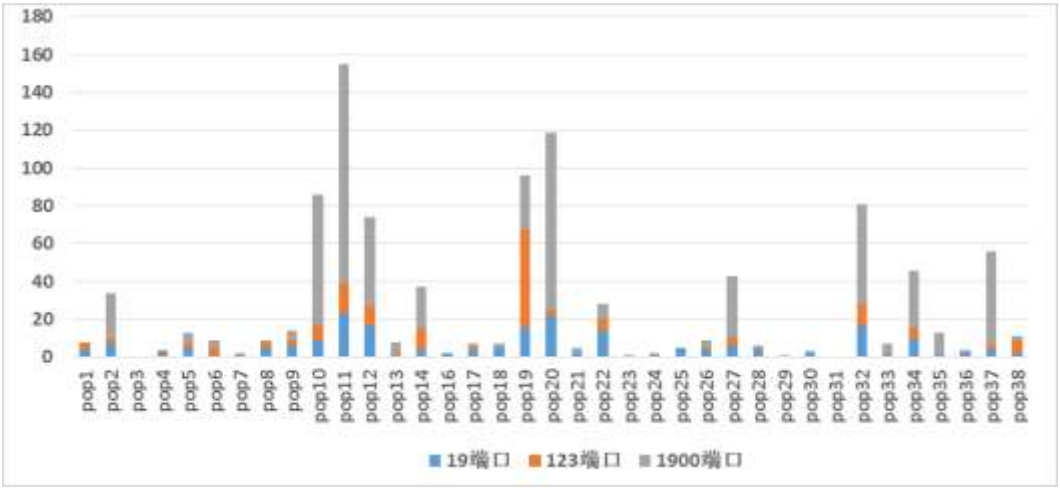

图 2 不同节点攻击主机数

从图中可以看到，CERNET 中存在一定数量的有 Chargen、NTP、SSDP 反射攻击行为的主机。

图 3-a 是三种攻击每天被攻击的主机数量，3-b 是三种攻击每天的发生次数，数据同样来自 2 月 10 日到 3 月 9 日 NBOS 总控的汇总信息，并分按被攻击 IP 的归属，分为国内和国外两方面进行统计。

图 3-a 被攻击主机数

图 3-b 攻击次数

从图中可以看出，被攻击主机和攻击次数在走向上总体保持一致，且针对国外地址的攻击不论在主机数量和攻击次数上都占据主要位置。

图 4 给出了统计时间段内，按天统计的 CERNET 全网范围内发起的三种攻击的总流量。从图中可以看出，面向 NTP 协议的攻击虽然参与的主机数量不多，但产生的攻击流量是最大的。其攻击流量在 2 月下旬的每一天里甚至达到十几 TB。而 Chargen 和 SSDP 反射攻击流量总体较低且数据较为平稳。

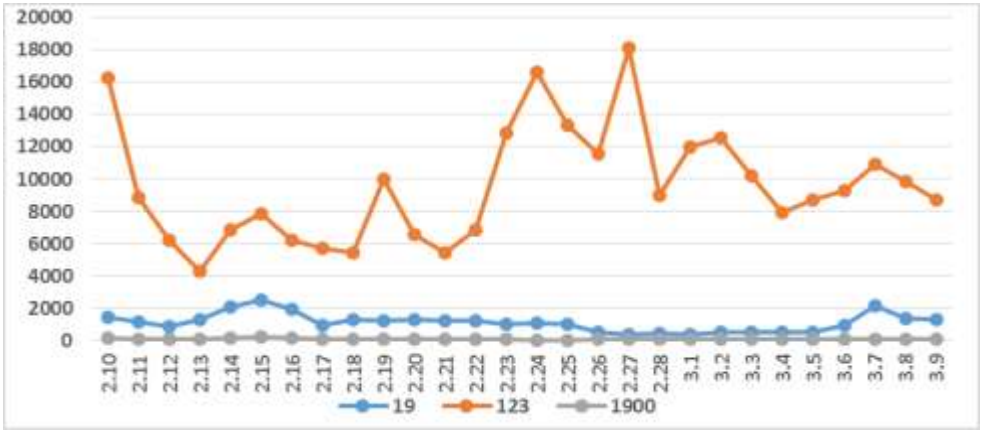

图 4 三种攻击流量统计（单位：GB）

表 1 给出了 2 月 10 日到 3 月 9 日期间，全网三种反射攻击的总体数据。

表 1 攻击数据汇总表

端口	攻击流量(GB)	攻击次数	参与攻击主机数	被攻击主机数
19	31346.9268	420189	280	44428
123	265464.0127	1446844	170	27706
1900	2936.0577	594205	956	18655

总体上，NTP 和 Chargen 反射攻击的在攻击流量上占据主要成分，特别是 NTP 反射攻击，虽然参与攻击的主机数量最少，但攻击总流量达到了 265TB，攻击的次数也居于首位。

4.2 攻击峰值情况

上节给出的流量和主机数据提供了攻击随时间的整体走向和在空间上的分布情况。本节将给出在统计时间段内发生的攻击中的一些峰值统计数据。

表 2-a、2-b 和 2-c 分别从被攻击者接收的流量最大、参与攻击主机发送的流量最大、参

与攻击主机的攻击次数最大三个角度，分别给出了三种攻击的对应数据：

表 2-a 接受攻击流量最大的网外主机

端口	攻击流量（GB）	参与攻击的 IP 数	被攻击服务器
19	119.56	4	95.136.48.119
1900	25.83	39	113.17.169.58
123	1939.23	98	208.98.54.137

表 2-b 发送攻击流量最大的网内主机

端口	参与攻击 IP	POP 节点	攻击总流量（GB）	攻击服务器数量
19	219.246.*.96	Pop 34	3816.0405	10379
1900	58.193.*.232	Pop 10	85.1839	3681
123	202.194.*.132	Pop 11	24872.6123	21777

表 2-c 参与攻击次数最多的网内主机

端口	参与攻击 IP	POP 节点	攻击流量（GB）	攻击次数
19	210.36.*.92	Pop 25	846.48	28058
1900	222.205.*.6	Pop 15	16.13	6019
123	202.112.*.18	Pop 22	11779.54	42246

所有的数据均表明，在三种反射攻击中，NTP 反射攻击是最严重的，其次是 Chargen 反射攻击，SSDP 的攻击效果则远小于前两者。

4.3 反射攻击的防范

最简单有效的方法是关闭端口，管理者应当尽可能地限制访问服务或者关闭服务端口。有关对反射攻击更具体的应对措施，由于篇幅的限制，我们将另文讨论。

需要说明的是目前在 CERNET 的所有主节点，均可以通过 NBOS 系统观测到所管理的网络范围内发生的上述 3 种类型的 UDP DRDDOS 攻击。在南京主节点，我们正在尝试通过 Chairs 系统，向有 UDP DRDDOS 行为的用户发送报告。

5 小结

本文在分析反射 DDOS 攻击原理的基础上，利用一种基于端口和阈值的检测算法，在 NBOS 平台上了针对 NTP、Chargen、SSDP 协议的反射 DDOS 攻击检测程序，并用其对 CERNET 中的此类攻击进行了观测和统计。从实际的观测结果来看，这三种反射攻击在 CERNET 中广泛存在，特别是 NTP 反射攻击，其攻击强度较大，应当引起足够的重视。协议本身的设计缺陷以及管理员对该类设备缺乏针对性的配置是造成攻击的主要原因。在实际应用中，应当限制或者关闭服务端口，或者对访问进行必要的限制，以降低发生此类攻击的可能。

参考文献

[1]赵煜,夏震,杨望,丁伟. Chargen 反射 DDOS 攻击检测[J].中国教育网络,2014,06:51-52.

[2]http://cve.scap.org.cn/CVE-1999-0103.html

[3]V. Paxson. An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks. In Computer Communication Review 31(3), July 2001.

[4]M Kührer,T Hupperich, C Rossow, T Holz. Amplification Hell: Revisiting Network Protocols for DDOS Abuse. USENIX Security Symposium, 2014 - usenix.org.

[5]http://www.freebuf.com/news/46514.html