DOI: 10.3969/j.issn.1009-6868.2015.06.013
网络出版地址：http://www.cnki.net/kcms/detail/34.1228.TN.20151109.1437.002.html

超大异常流量攻击的防御思路探讨

Defense of Massive Anomalous Traffic Attack

中图分类号：TN929.5 文献标志码：A 文章编号：1009-6868 (2015) 05-0054-005

刘东鑫/LIU Dongxing
何明/HE Ming
汪来富/WANG Laifu
（中国电信股份有限公司广州研究院，广东 广州 510630）
(Guangzhou Research Institute of China Telecom Co., Ltd, Guangzhou 510630, China)

摘要： 提出了应对超大异常流量攻击的防御思路，该思路中将防御策略分为短期策略和长期策略。短期措施主要在现有异常流量防护措施的基础上，进一步提升对超大异常流量攻击的防护能力；而长期策略试图从虚假源地址过滤、开放服务的协议方面进行改进。随着可利用的DNS、NTP等公共服务器资源将逐步减少，攻击者将转为挖掘新的可用于流量反射放大的应用协议。由于以“反射、放大流量”为特性的超大异常流量攻击仍将保持发展，对它的安全防御仍有待在实践中检验和不断完善。

关键词： 异常流量；放大攻击；流量清洗

Abstract: In this paper, we propose a solution for ISPs to deal with massively anomalous traffic. This solution includes short-term protection and a long-term strategy. The short-term protection is mainly based on the existing abnormal flow detection but enhances the protection capabilities. The long-term strategy aims to improve the IP source address spoofing filtering and the protocols of the open service, such as DNS and NTP. With the decrease of the available known resource for attackers, new application protocols are used to make areflected and amplified anomalous traffic. For the sustained improvement of attacker skills, the defense of massively anomalous traffic need to be continuously tested and improved in practice.

Key words: anomalous traffic; amplified attacks; traffic cleaning

异常流量攻击是分布式拒绝服务（DDoS）攻击的一种，其本质上是带宽型攻击，它通过在网络中发送大流量的数据包，消耗极大的网络带宽资源。

随着互联网的快速发展，攻击手段不断演进，超大异常流量攻击方式已经呈现蔓延趋势。2013年3月，欧洲反垃圾邮件组织Spamhaus遭受了有史以来最大的异常流量攻击，被《纽约时报》称为“前所未有的大规模网络攻击”，其攻击强度达到300 Gbit/s，攻击强度以3倍以上快速增长，如图1所示。2014年2月，欧洲云计算安全公司CloudFlare遭遇的攻击流量的峰值超过了400 Gbit/s，快速大幅地刷新了异常流量攻击的相关历史记录。

文中探讨的超大异常流量攻击主要包含以下特征：攻击者主要利用了互联网中基于用户数据报协议（UDP）开放服务作为流量攻击的反射器；理论上，全球互联网中开启了开放服务的公共服务器都可以被攻击者使用，而公共服务器的数量惊人；反射器的流量放大效果可以高达上千倍，效果非常明显。从以上的3个特征我们可以看出，超大异常流量攻击属于反射型流量攻击的其中一种，而后两个特征是导致异常流量攻击纪录呈现出快速增长趋势的重要原因。

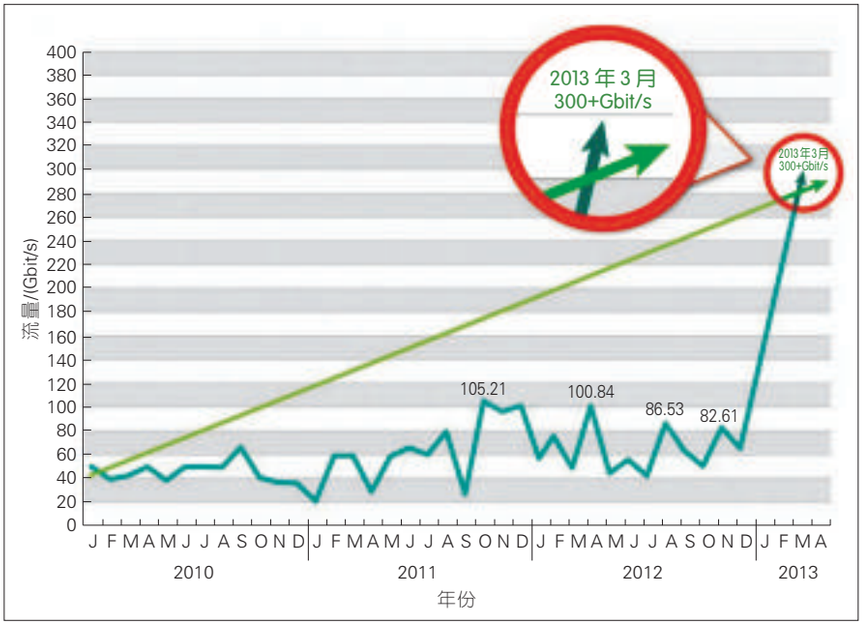
收稿日期：2015-09-02
网络出版时间：2015-11-09

1 超大异常流量攻击的特征分析

1.1 典型案例分析

2013年3月，欧洲反垃圾邮件组织Spamhaus遭受了时间长达1周、流量峰值高达300 Gbit/s的异常流量攻击，甚至影响到了整个欧洲互联网的正常运营。在这次攻击事件中，攻击者向互联网上开放的域名系统（DNS）服务器发送对ripe.net域名的解析请求，并将源IP地址伪造成Spamhaus的IP地址。DNS请求数据的长度约为36字节，而响应数据的长度约为3 000字节，这样攻击者利用DNS服务器就可以轻松地将攻击流量放大近100倍。进一步地，攻击者使用了约3万台开放DNS服务器，再加上一个能够产生3 Gbit/s流量的小型僵尸网络，就完成了一次创纪录的异常流量攻击事件。最后，借助云安全公司CloudFlare位于全球的20多个彼此独立的流量清洗中心，才得以

D:\MAG\2015-12-125/VOL21\Wide1.VFT——5PPS/P1



▲图 1 2010—2013 年全球异常流量攻击的流量峰值统计

缓解此次攻击。

本次攻击事件让业界意识到：如 DNS 等公共服务的协议漏洞是互联网的巨大安全隐患，如果不加以治理，未来可能会爆发更大规模的 DDoS 攻击。令人遗憾的是，这一担忧很快成为现实。

2014 年 2 月，CloudFlare 公司遭受峰值流量高达 400 Gbit/s 的异常流量攻击，这导致该公司在欧洲的业务受到严重干扰，甚至使美国互联网的一些基础设施也受到了影响。与 Spamhaus 遭受的异常流量攻击类似，攻击者利用一个小型的僵尸网络伪造 CloudFlare 公司的 IP 地址，向互联网上数量众多的开放网络时间协议（NTP）服务器发送请求时钟同步请求报文。CloudFlare 公司在事后披露，这些 NTP 服务器共有 4 529 个，遍布于全球 1 298 个不同的运营商网络中，如图 2 所示。为了增加攻击强度，发送的请求报文被设置为 Monlist 请求报文，反射流量的放大效果最大可提升至 700 倍。最后也是通过 Anycast 技术将攻击流量分散到全球不同的流量清洗中心，才得以逐步遏制攻击流量。

本次攻击事件再一次震惊业界，并抛出了令安全人员无奈的问题：类似 Spamhaus 和 CloudFlare 所遭受的超大异常流量攻击是否还会出现？如果出现，那么当一个目标用户遭受的异常攻击流量超出现网防护能力时，该如何面对？

1.2 超大异常流量攻击的实施机制

基于以上攻击案例分析，我们对超大异常流量攻击的实施机制做进一步的深入分析。在传统攻击方法中，攻击者需要想尽各种办法、耗费大量资源来构建一个大规模的僵尸网络，而超大异常流量攻击方法对僵尸网络的要求门槛大幅度降低，攻击者的准备工作主要集中在对互联网上公共服务器的扫描、基于 UDP 开放服务的选择，力求实现最大的反射流量放大效果，如图 3 所示。攻击者通过扫描、搜索引擎等方法就可以轻易地获取互联网上大量的公共服务器 IP 地址，最后根据攻击目标，选择一个或者几个基于 UDP 协议的开放服务用于攻击流量的放大，企图实现最大化的攻击效果。

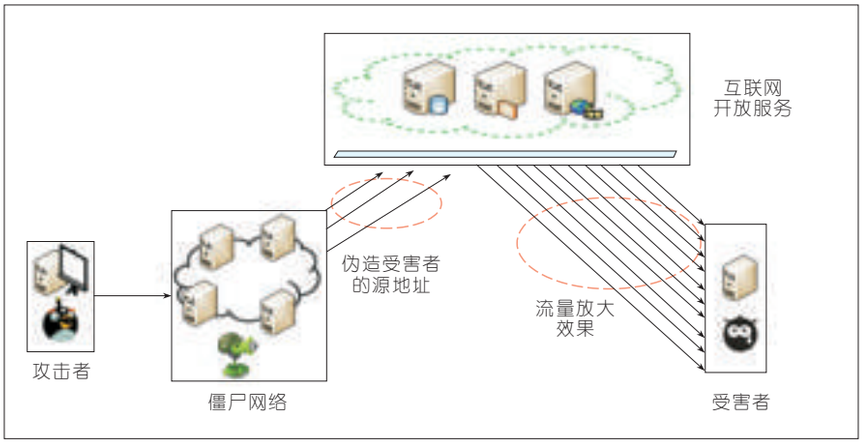
攻击者选择基于 UDP 协议的开放服务的原因是：这些开放服务往往无 session 状态、不需要认证过程，随时响应查询报文，而且返回的结果报文会自然产生流量放大效果。为了方便比较，我们采用带宽放大因子（BAF）来衡量各种不同开放服务的流量放大效果。

常见基于 UDP 协议的开放服务的流量放大效果对比如表 1 所示[1]。其中，BAF 受软件版本，客户端请求类型字段的影响，部分开放服务的 BAF 呈现较大的变化区间。

从表 1 可以看出，只要扫描到足够多的公共服务器，选择适当的应用协议，辅以一个小型的僵尸网络，就可以“四两拨千斤”地构建出一场轰动的异常流量攻击事件。其中，DNS 和 NTP 协议的流量放大效果最好，并且互联网上开放的域名系统和开放网络时间协议服务器最多，故攻击两

▲图 2 被利用的 NTP 服务器的地理分布

D:\MAG\2015-12-125/VOL21\Wide1.VFT——5PPS/P2



▲图3 超大异常流量攻击流程

▼表1 常见基于UDP协议的开放服务的流量放大效果对比

开放服务应用协议类型	UDP端口号	BAF	协议简介
DNS	53	29~98	域名解析
NTP	123	556~4670	网络时钟同步
SNMPv2	161	6~11	网络设备管理
NetBios	137	3~5	局域网通信的API
SSDP	1900	30~75	检测UPnP主机
CHARGEN	19	359	字符串发生器

API：应用程序编程接口　DNS：域名系统　SNMP：简单网络管理协议
BAF：带宽放大因子　NTP：开放网络时间协议　SSDP：简单服务发现协议

个案例可以快速刷新攻击流量的历史纪录。

2 现网异常流量防护措施的不足

在骨干网或城域网等现网的大规模异常流量防御技术体系中，通常采用部署异常流量清洗设备[2]，进行异常流量牵引、清洗和正常流量的回注。随着集中网管系统的逐步完善、异常流量清洗设备关键性能的不断提升，运营商对异常流量的清洗能力和攻击溯源能力大幅提高。但是，在现有的防护措施下，异常流量清洗设备作为最后的关键一环，却难以应对如以上案例中的超大规模攻击流量。总的来说，现有防护措施难以应对超大异常流量攻击的原因包括：

（1）流量清洗设备的处理能力难以匹配快速增长的攻击流量。一方面，由于攻击者广泛利用了来自全球不同自治系统（AS）内不同应用协议的公共服务器，导致攻击流量在AS的边界路由器就已经很大了，甚至可以超过流量清洗设备的处理能力。另一方面，现网的AS边界路由器在配置端口过滤等流量过滤手段时需要遵循严格的管理流程，这个时间差也给了攻击者探测攻击效果，逐步加大攻击强度的试验时间。最终，一些小运营商的边界路由器可能被攻击流量瘫痪，这点在案例1中表现得尤为明显。

（2）全球范围内广泛存在的公共服务器可以轻易被攻击者扫描获取并利用，而对公共服务器的安全加固则需要世界各国管理员的快速响应和协作配合。据估计，2014年初互联网上开放UDP 123端口的NTP服务器约有80万台[3]，开放式递归DNS服务器数量超过500万台，其他如CHARGEN、简单网络管理协议v2（SNMPv2）等公共服务器的数量可达数十万以上。

（3）向公共服务器发起查询的僵尸网络因为规模较小，发送的查询流量也较小，往往难以被溯源发现。在Spamhaus被攻击的案例中，为了达到300 Gbit/s峰值流量的攻击效果，攻击者只需要在全球范围内构建一个可发送3 Gbit/s流量的小型僵尸网络，来向全世界的DNS服务器发起查询请求。假设该僵尸网络有3万台主机，那么每台主机发起的流量仅仅是100 kbit/s。如此小的流量，难以被现网中基于Netflow的溯源技术发现，这也是造成超大异常流量攻击持续时间长的重要原因。

（4）作为初步的有效防护手段，虚假源地址过滤技术依然难以广泛部署。对于DDoS的反射型攻击，虚假源地址过滤是安全防护的有效手段，但虚假源地址过滤仍然是业界的一大难题。目前，针对虚假源地址问题，现网中常用的防护措施是在接入网层面采用访问控制列表（ACL）和反向路径过滤（RPF）等功能配置。受网络扁平化和业务发展影响，如IPv4地址回收、复用等，若在接入网层面全面配置ACL，则日常的配置、管理任务极其繁重，故实际中ACL在虚假源地址过滤方面的应用并不多；而RPF功能需要设备支持，不同厂家的支持力度不同，从而导致RPF应用范围有限。

3 超大异常流量攻击的防御思路

已有的攻击案例表明：现有的异常流量防护措施存在不足之处，业界亟需研究新的防御思路。现网的异常流量防护措施注重“快速检测、及时响应”阶段的能力建设，而超大异常流量攻击的有效防护应在“预防”阶段，体现在对开放式公共服务器的安全加固、网络边缘的虚假源地址过

D:\MAG\2015-12-125/VOL21\Wide1.VFT——5PPS/P3

滤等。文中按实施难度，将防御策略分为短期措施和长期策略，详细探讨对超大异常流量攻击的防御思路。其中，短期措施主要包含精细化的防护措施，在现有异常流量防护措施的基础上，进一步提升对超大异常流量攻击的防护能力；而长期策略试图从虚假源地址过滤、开放服务的协议改进，彻底杜绝超大流量攻击的“生长土壤”。

3.1 短期措施

超大异常流量攻击非常容易制造超大流量，对互联网基础网络的可用性造成威胁。实践证明：仅依赖流量清洗设备难以防御，更重要的是在超大的攻击流量发生时，需要尽快在网络上游直接过滤攻击流量，避免下游的网络拥塞。总的来说，短期内运营商应重点采取以下措施：

（1）排查自己网内的公共服务器，包括DNS、NTP、SNMP和CHARGEN等服务器，关闭不必要的公共服务器。对于开放的公共服务器，可在服务器前面部署源地址请求过滤，保证只接受本AS或本运营商内的源地址查询请求，避免沦为攻击外部网络的流量放大器。

（2）在开放的公共服务器部署查询限速和大包回应过滤技术。超大异常流量攻击的攻击特点是：回应报文长度远大于正常业务报文，源自受害者IP地址的查询速率快于正常的业务请求。例如，在DNS业务中，大部分的Reply报文不超过512字节，也很少有源自同一地址的查询速率超过300个/秒；而在NTP业务中，通常的NTP报文都很短，而攻击者所利用的monlist请求报文特别长，速率也特别快。这些都可以形成安全规则，在公共服务器进行过滤。

（3）尽快升级公共服务器端的软件和协议版本，关闭不必要的功能端口。例如，在DNS的软件版本中，只有最流行的互联网系统协会（ISC）BIND支持查询限速的功能配置，这将有助于减轻对安全防护设备的依赖（如防火墙）；而在最近备受关注的NTP反射攻击中，应尽快把NTP服务器升级到4.2.7p26，关闭现在NTP服务的Monlist功能，并在ntp.conf相关的配置文件中增加“disable monitor”选项。

（4）完善数据中心出口处的DDoS防护措施。过去，数据中心只关注Inbound DDoS攻击，但近两年已经开始出现数据中心的服务器中了僵尸木马后向外发送大流量DDoS攻击，Outbound DDoS攻击呈现出快速上升的势头。数据中心的服务器一旦被用作流量反射放大器，将成为Outbound DDoS攻击的一种，极容易导致上行链路拥塞，严重影响数据中心的正常业务。Outbound DDoS的防御技术与Inbound DDoS防御技术具有较大差别，建议在数据中心的网络边缘密切关注出口带宽变化、防范Egress流量的虚假源地址。

（5）对全网的异常流量清洗中心进行Anycast部署，提高抵御超大型流量攻击的能力，同时为增强流量清洗能力，也需要对流量清洗设备保持同步的扩容建设。通过利用多设备集群、负载均衡、资源管理及调度等技术，构建用于单个清洗节点的资源池；而基于统一流量控制中心的资源感知及调度技术，可实现多清洗节点资源协同，同时利用诸如云信令等技术实现本地网侧及骨干网侧流量清洗能力联动，最终达到高性价比的防护效果。

（6）在国际出入口和互联互通层面对NTP、DNS和SNMP等开放服务的流量进行监测和控制，并可通过ACL的方式进行过滤，降低来自网外的超大异常流量攻击威胁。例如，代表NTP协议的UDP 123端口、代表DNS协议的UDP 53端口以及代表CHARGEN协议的UDP 19端口等等。

（7）最后，对于遭受超大异常流量攻击的用户，在运营商边缘（PE）侧可通过流量牵引，对用户流量进行清洗。异常流量清洗中心可增加以下异常流量特征：NTP的monlist请求、DNS的ANY类型查询、SNMPv2的GetBulk请求等，以提高清洗效率。

以上几个措施必须同时配合，否则按照互联网中现有的DNS、NTP等公共服务器数量估算，攻击者依然可以发起超大流量攻击。随着业界的高度重视和共同配合，预计以DNS/NTP反射攻击为代表的超大异常流量攻击不断疯涨的强劲势头将会得到很大程度的遏制。

3.2 长期策略

超大异常流量攻击的泛滥，根本原因是互联网应用协议、网络体系等在设计之初，对安全问题考虑不足。运营商作为互联网产业的一个关键链条，应对相关的技术标准演进保持密切关注，及时推动网络技术的投资建设；同时，应加强与其他运营商、国家网络安全中心等部门的网络安全态势信息共享，提高对未知攻击的及时响应能力。长期来看，建议采取以下策略：

（1）密切关注包括IPv4和IPv6在内的源地址过滤技术发展动态，如BCP38/84、源地址验证架构（SAVI）等。低成本、易维护、易管理的虚假源地址过滤技术一直是运营商的关注焦点，有助于从根本上消除反射型的流量攻击。

（2）联合产业链的其他厂商，推动现有各种基于UDP的公共服务应用协议的标准修改，降低公共服务器沦为攻击放大器的风险。修改的思路包括：在现有基于UDP的应用协议基础上构建session状态，改善流量的对称性，加入或增强认证能力以实现一定程度的访问控制。最终，使得应用协议的BAF极大地降低，超大异常流量攻击从而将不再具有“超大流量”属性。

超大异常流量攻击所代表的是一个跨行业、跨地区、跨国界的复杂安全问题，不可能由哪一方面单独解

D:\MAG\2015-12-125/VOL21\Wide1.VFT——5PPS/P4

决。互联网及其基础设施的安全运行依赖于产业链条上每个参与者的长期共同努力和紧密配合。

4 结束语

近年来，随着基于云计算的超大型互联网数据中心（IDC）的纷纷落地，巨大的流量汇聚特性已经给网络设备带来较大的扩容和异常流量防护压力，而在如 Spamhaus、CloudFlare 所遭受的超大异常流量攻击面前，互联网基础设施所面临的防护压力被极度放大。随着产业界对开放式公共服务器的安全加固，攻击者可利用的公共服务器资源将逐步减少，其攻击思路将转为挖掘新的可用于流量反射放大的应用协议，例如 BitTorrent、Kad 等等。以“反射、放大流量”为特性的超大异常流量攻击仍将在攻与防的矛盾中不断发展，对它的安全防御仍有待在实践中检验和不断完善。

致谢

感谢中国电信网络安全实验室的肖宇峰、罗志强和沈军等同事的帮助，他们对文章的撰写给予了充分的支持和中肯的建议。

参考文献

[1] CHRISTIAN R. Amplification Hell: Revisiting Network Protocols for DDoS Abuse [C]// Network and Distributed System Security Symposium, San Diego, California, 2014
[2] 王帅等. 超宽带网络安全体系及关键技术研究[J]. 电信科学, 2013, (8): 257–261
[3] 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/8/2014/20140314085001237248948/20140314085001237248948_.html

作者简介

刘东鑫，现任中国电信广州研究院工程师；主要从事网络与信息安全的研发工作，在身份认证和访问控制等方面具有较丰富的经验；曾获得 CCIE 和 CISSP 认证；发表论文3篇。

何明，现任中国电信股份有限公司广州研究院高级工程师；主要从事网络安全方面的研发及技术支撑工作。

汪来富，现任中国电信股份有限公司广州研究院高级工程师；主要从事大数据安全、云安全、网络安全研究工作。

综合信息

中国首次提出的物联网编码国家标准正式发布

由中国物品编码中心(以下简称编码中心)主导完成，中国首次提出的自主可控的、物联网编码国家标准《物联网标识体系物品编码 Ecode》国家标准委正式发布，标准号为 GB/T31866–2015。该国家标准的发布有利于将物联网物品标识解析服务实现自主可控，对促进中国物联网产业发展具有重要意义。

在互联网中，各类网络资源，如 web 网页、音视频文件及应用软件等，均采用基于 DNS 系统的 URL 来进行标识。这样以来，各类互联网应用之间就可以通过 URL 对各类网络资源实现统一访问，从而确保各类互联网应用能实现便捷的互联互通。与互联网中的 URL 一样，物联网也为不同的物品分配了标识，并进而通过标识对物品进行寻址。

由于每种物联网标识的编码格式以及解析协议间存在差异，如果不能研发出一种兼容解析各类异构物联网标识的通用解析方法，就会导致采用不同物联网标识的物联网应用间无法实现互联互通，并因此而导致物联网信息孤岛现象，进而阻碍物联网的进一步发展。实现物联网标识兼容解析的第一步就是要准确识别各类异构物联网标识，也就是说当接收到一个物联网标识时，需能识别出该标识具体属于哪种物联网标识标准，进而才能实现异构物联网标识的寻址和兼容解析。

对物联网标识进行识别大致有两种方法：基于物联网标识标准的信息进行识别，即从文本信息中提取出物联网标识的编码规则，进而通过规则匹配来实现物联网标识识别；构造物联网标识编码样本并通过机器学习的手段进行识别。

近年来，物联网产业飞速发展，原来局限在一种物联网标识寻址体系内部的闭环物联网应用逐渐走向开环。在这种背景下，研发一种能兼容解析各类异构物联网标识的统一解析方法就变得迫在眉睫。而作为当中关键的一环，实现对各类异构物联网标识的准确识别是实现物联网标识兼容、统一解析的基础。为实现物联网应用的互联互通，很有必要加大对物联网标识识别这一基础共性技术的研发力度。我们相信，一旦开发出高效、准确的物联网标识识别技术定能进一步推动物联网产业从目前的闭环运行走向更加开放、繁荣的未来。（转载自《中国信息产业网》）

D:\MAG\2015-12-125/VOL21\Wide1.VFT——5PPS/P5