



分布式 DNS 反射 DDoS 攻击检测及控制技术

罗志强, 沈 军, 金华敏

(中国电信股份有限公司广州研究院 广州 510630)

摘 要: 分布式 DNS 反射 DDoS 攻击已经成为拒绝服务攻击的主要形式之一, 传统的基于网络流量统计分析和网络流量控制技术已经不能满足防护需求。提出了基于生存时间值(TTL)智能研判的 DNS 反射攻击检测技术, 能够准确发现伪造源 IP 地址分组; 基于多系统融合的伪造源地址溯源阻断技术, 从源头上阻断攻击流量流入网络。

关键词: DNS 反射攻击; DDoS 攻击; 虚假源地址; 网络安全

doi: 10.11959/j.issn.1000-0801.2015270

Detection and Control Technology of Distributed DNS Reflective DDoS Attack

Luo Zhiqiang, Shen Jun, Jin Huamin

(Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China)

Abstract: Distributed DNS reflective DDoS attack has become one of the main forms of denial of service attacks, and traditional security technology based on network traffic analysis and network traffic control technology can't meet the needs of protection. Detection technology of DNS reflection attack based on time to live (TTL) value intelligent judgments was proposed, and the detection technology can accurately detect spoofed source IP address of the packet. The control technology based on multi system fusion can block attack traffic flow into the network in the source.

Key words: DNS reflective attack, DDoS attack, fake source address, network security

1 引言

随着拒绝服务攻击 (DoS) 的方式和手段不断发展变化, 近年来, 互联网面临的分布式反射型拒绝服务攻击日趋频繁。据有关单位报告, 2013 年 3 月, 欧洲反垃圾邮件组织 Spamhaus 对外宣称遭受 300 Gbit/s 流量的分布式 DNS (domain name system, 域名系统) 反射型 DDoS (distributed denial of service, 分布式拒绝服务) 攻击^[1]; 2014 年

12 月中旬, 阿里云在微博上发布一则声明, 称 12 月 20-21 日, 部署在阿里云上的某知名游戏公司遭遇了全球互联网史上最大的一次 DNS 反射型 DDoS 攻击, 攻击峰值流量超过 450 Gbit/s^[2]。众多 DDoS 攻击事件表明, 分布式 DNS 反射 DDoS 攻击已经成为拒绝服务攻击的主要形式之一。

2 分布式 DNS 反射 DDoS 攻击技术原理

分布式 DNS 反射 DDoS 攻击是一种基于带宽耗尽型

收稿日期: 2015-06-16; 修回日期: 2015-10-09

论文引用格式: 罗志强, 沈军, 金华敏. 分布式 DNS 反射 DDoS 攻击检测及控制技术. 电信科学, 2015270

Luo Z Q, Shen J, Jin H M. Detection and control technology of distributed DNS reflective DDoS attack. Telecommunications Science, 2015270



攻击方式。根据 DNS 协议(RFC2617 文档)的特点,DNS 应答报文一般是查询报文的几倍甚至几十倍,通过开放 DNS 递归服务器的流量反射,相当于攻击数据分组增加了数十倍,达到了攻击流量放大的效果。

DNS 域名服务器的开放递归服务和源 IP 地址伪造技术是成功实施分布式 DNS 反射 DDoS 攻击的必要条件。攻击者在进行分布式 DNS 反射 DDoS 攻击之前,会在被控制的某些权威域名服务器上先发布大字节的 TXT 资源记录。然后,攻击者向大量开放递归服务的 DNS 服务器发送带有扩展字段 OPT RR(伪资源记录)的 DNS 查询请求分组,并将该 DNS 查询请求分组的源 IP 地址伪造成攻击目标 IP 地址。由于 DNS 域名服务器不对查询请求分组的源 IP 地址进行真实性验证,因此 DNS 服务器会对所有的查询请求都进行解析查询应答,并将大范围域名查询的响应数据发送给攻击目标。由于请求数据比响应数据小得多,攻击者就可以利用该技术有效地放大其掌握的带宽资源和攻击流量,这样,大量的 DNS 应答分组将汇聚在受害者端,堵塞受害者的网络而最终造成 DDoS 攻击。

例如,在 2013 年 Spamhaus 攻击事件中,攻击者向 30 000 多个开放 DNS 服务器发送了对 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 byte,而响应数据的长度约为 3 000 byte,这意味着利用 DNS 反射能够产生约 100 倍的放大效应。Spamhaus 攻击事件中,大量开放 DNS 服务器的响应数据产生了大约 300 Gbit/s 的攻击流量,因此,攻击者只需要掌握和控制一个能够产生 3 Gbit/s 流量的僵尸网络,就能够进行 300 Gbit/s 流量的大规模攻击。

在分布式 DNS 反射 DDoS 攻击过程中,开放递归的 DNS 服务器在不知情的情况下也参与了进攻,对 DNS 系统资源也有一定的消耗,同时经过放大后的攻击流量也会对流经的运营商网络性能产生一定影响,变相造成网络堵塞。

3 分布式 DNS 反射 DDoS 攻击检测及控制技术

目前,业界应对分布式 DNS 反射 DDoS 攻击主要是采用基于网络流量统计分析^[3]和网络流量控制^[4]的技术、基于机器学习和支持向量机算法^[5]的检测技术、基于网络流量行为时间序列的 DDoS 检测技术^[6]。

在基于网络流量统计分析和网络流量控制的技术方法中,检测 DNS 拒绝服务攻击之前,需要能够描述 DNS 服

务器正常运转情况下的网络流量信息和正常行为分布规律,通过分析 DNS 服务器的正常流量信息特征和正常行为分布规律,建立 DNS 服务器所在网络的正常状态和异常状态模型,通过设定异常状态阈值实现 DNS 恶意流量攻击行为的异常检测。此类检测技术常用的检测特征包括了域名解析失败率发生突然大幅增长、DNS 服务器所在网络流量迅速增大、随机域名出现有规律的均匀分布等重要检测特征。虽然流量统计分析方法具有一定的检测能力,但是随着攻击流量的隐蔽性增强和攻击形式的层出不穷,流量统计方法的误判率大幅度上升。

基于机器学习和支持向量机算法的检测技术是大规模、高带宽网络环境下实现对 DNS 网络攻击智能检测的重要手段,系统把服务器收到的正常数据流和 DDoS 攻击流当成一个分类问题进行运算,利用机器学习和支持向量机算法建立模型来进行判断,并对检测结果进行预警。此类技术的优点是利用支持向量机在解决小样本、非线性及高维问题时所具有的良好性能,实现对 DNS 攻击行为的高速检测。但是此类技术存在攻击流检测环境中多个检测器的协作问题,需要结合集成学习、人工免疫等新兴技术来提高检测系统的检测精度和顽健性。

在基于网络流量行为时间序列的 DDoS 检测技术中,主要是采用统计分析、关联分析等多种技术手段周期性检测域名服务器端对用户发送和接收的流量行为中的异常模式,判断其是否满足 TCP 和 UDP 行为的时间同步性,识别攻击者和正常用户,从而发现异常行为。

随着 DNS 攻击流量的隐蔽性增强和攻击形式的层出不穷,现有技术方法的误判率大幅度上升,多个检测器的协作问题也是安全性能提升的制约因素。为应对日益严峻的分布式 DNS 反射 DDoS 攻击安全形势,本文提出了基于生存时间值(time-to-live,TTL)智能研判的分布式 DNS 反射 DDoS 攻击检测技术和基于多系统融合的伪造源地址溯源阻断技术,在 DNS 服务器端检测到 DDoS 攻击后,通过网络通信的方式通知运营商边界路由器等网络边界基础设施,启用流量清洗过滤源 IP 地址伪造分组,从源头上阻断 DNS 攻击流量流入网络。

4 基于生存时间值智能研判的 DNS 攻击检测技术

正常来说,同一个客户端发送的 DNS 查询请求数据分组在一定时间内经过基本固定的路由到达 DNS 服务

器,也就是说在一段时间内,从同一个用户端发给 DNS 服务器的 DNS 请求数据分组的 TTL 值应该是稳定的。由于攻击者发动 DNS 反射攻击时,需要僵尸网络多台傀儡机同时发送伪造源地址的 DNS 请求分组,攻击者虽然可以伪造发向 DNS 服务器的数据分组中的源 IP 地址、TTL 等任何字段的信息,但是由于傀儡机通常分布在不同地区,因此,攻击者很难正确伪造真实 IP 地址对应的主机发送的数据分组到达 DNS 服务器的跳数,因此,基于 TTL 值智能研判的 DNS 攻击检测技术主要是对来自同一个源 IP 地址的 DNS 请求数据分组 TTL 值进行实时比对,对同一源 IP 地址 TTL 值频繁变动的 DNS 请求分组实施无递归的本地解析或直接丢弃的抑制方法。由于 IP 地址伪造技术是成功实施分布式 DNS 反射 DDos 攻击的必要条件,利用本方法能够准确发现伪造源 IP 地址分组并抑制域名反射放大攻击,有效解决了原有技术中漏判率和误判率严重的问题。

如图 1 所示,基于 TTL 值智能研判的 DNS 攻击检测技术主要包括了 DNS 攻击行为检测和伪造源地址域名查询智能抑制两部分。

在 DNS 攻击行为检测中,DNS 系统的检测研判模块分光 DNS 查询流量,实时分析进入 DNS 节点的查询数据分组,将每个查询数据分组的源 IP 地址和 TTL 值进行实时比对,当单位时间(5 s~1 min 可调)内同一个源 IP 地址的 TTL 值比对不相同,用新检测的 TTL 值替代原有的 TTL 值,同时针对该记录的计数器加 1,频繁变动的 TTL 值将导致计数器计数超过安全门限,从而发出抑制指令。

在伪造源地址域名查询智能抑制中,域名服务器根据抑制指令,对该域内的所有来自该伪造源 IP 地址的 DNS 请求分组实施无递归的本地解析或直接丢弃。

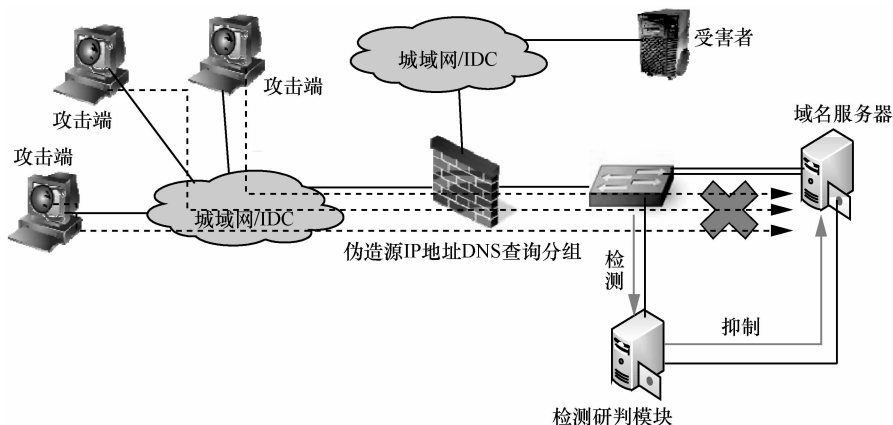


图 1 基于生存时间值智能研判的 DNS 攻击检测技术

5 基于多系统融合的伪造源地址溯源阻断技术

基于多系统融合的伪造源地址溯源阻断技术主要是通过运营商现有的域名安全分析系统、攻击溯源系统和流量清洗设备之间的融合联动,在 DNS 服务器端检测到 DDos 攻击后,通过网络通信的方式通知运营商边界路由器等网络边界基础设施启用流量清洗过滤源 IP 地址伪造分组,从源头上阻断攻击流量流入网络,这种在边界上过滤的方式比在 DNS 服务器端过滤更有效。

如图 2 所示,多系统融合的虚假源地址溯源阻断过程包括自动化的攻击行为检测、伪造源地址攻击分组溯源和伪造源地址攻击分组清洗 3 部分。

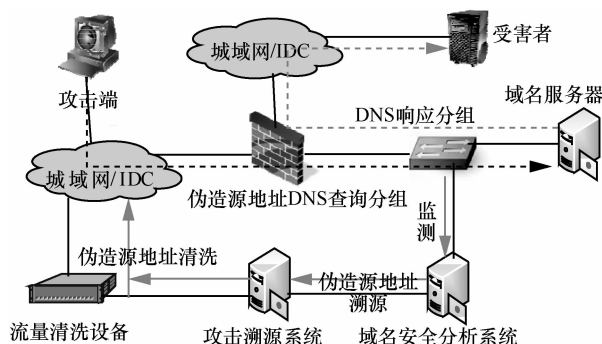


图 2 多系统融合的虚假源地址溯源阻断过程

- 自动化的攻击行为检测：域名安全分析系统分光 DNS 查询流量，实时分析进入 DNS 节点的查询数据分组，基于上文介绍的基于 TTL 值智能研判的 DNS 攻击检测技术，发现伪造源地址的 DNS 攻击分组，域名安全分析系统将攻击分组源地址参数发送给攻击溯源系统。



- 伪造源地址攻击分组溯源:攻击溯源系统根据源地址参数溯源攻击路径,结合采集存储原始 NetFlow 流量信息、路由器端口信息、路由拓扑信息、城域网 IP 地址等多维参数进行关联分析,通过多元广度遍历算法,快速回溯攻击流量穿越路径及流量分布特征,可对伪造源地址发起的 DNS 攻击进行实时监测,并通知流量清洗设备在相关网段阻断伪地址攻击流量。
- 伪造源地址攻击分组清洗:流量清洗设备在伪造源地址的城域网发布 BGP 细路由,将包括伪造源地址的 DNS 查询流量牵引到流量清洗设备,当连续一段时间内 DNS 查询流量的速率超过阈值时,流量清洗设备启动源认证防御,在源认证过程中清洗设备会触发客户端以 TCP 报文发送 DNS 请求,能够发送 TCP DNS 请求的客户端被认证为合法源。流量清洗设备只把来自合法源的 DNS 请求分组返回给 DNS 服务器,有效阻断伪造源地址的 DNS 查询请求。

6 检测技术可行性验证

为了验证本文提出的基于 TTL 值智能研判的 DNS 攻击检测技术的可行性,在中国电信网络安全实验室搭建了一个伪造源 IP 地址攻击网络环境,如图 3 所示。被攻击目标采用了一台 Windows7 64 位服务器,IP 地址为 192.168.0.4,在被攻击目标同一网段部署了一台协议分析仪(Sniffer 设备),连接到被攻击目标的镜像端口实时采集网络流量;DNS 服务器采用了一台 Windows2008 R2 版 64 位服务器,IP 地址为 172.18.16.11,在该服务器 C:\Windows\SysWOW64\dns 目录下安装了 BIND9.9.3 开源软

件,实现 DNS 功能,在 DNS 服务器的镜像端口上部署了计数器模块,实时分析 DNS 服务器的 DNS 查询流量;攻击者则由 SmartBits 6000C 测试仪表担任,测试仪表将模拟 1~10 个攻击客户端发送针对多个不同域名的正常 DNS 查询分组,其中所有攻击客户端发出的 DNS 查询分组的源 IP 地址均伪造为 192.168.0.4,每个攻击客户端的 TTL 初始值设置互不相同,启动所有 10 台攻击客户端时共有 10 个不同的 TTL 初始值。测试过程中,每台攻击客户端固定以 1 000 Hz 的速率发送 DNS 查询数据分组。

表 1 展示了在以上试验环境中,不同数量的攻击客户端向 IP 地址为 172.18.16.11 的 DNS 服务器发送源 IP 地址被伪造为 192.168.0.4 的 DNS 查询分组流量,进行多个不同域名的正常查询,记录了攻击峰值总流量、接收峰值总流量、检测率的统计结果。

验证过程中,当未启用本检测技术(不设置计数器最大门限值)时,由于每台攻击客户端所发送的 DNS 查询攻击数据分组为正常查询多个不同域名的 DNS 查询分组,这些源 IP 地址被伪造为 192.168.0.4 的查询分组流量符合 DNS 服务器的正常流量信息特征和正常行为分布规律,因此原有基于流量的统计分析无法根据 DNS 服务器所在网络流量迅速增大、随机域名出现有规律的均匀分布等重要检测特征检测出 DNS 查询攻击流,IP 地址为 192.168.0.4 的目标主机收到了大量的 DNS 回应分组流量,从而导致对目标主机的反射流量攻击。启用本检测技术后,首先在计数器最大门限值设置为 1 000 次/s 的条件下展开测试,测试数据显示,当只启动一台攻击机发送伪造源 IP 地址的 DNS 查询数据分组时,由于计数器检测到的 TTL 值一直保持不变,因此 IP 地址为 192.168.0.4 的目标主机仍然

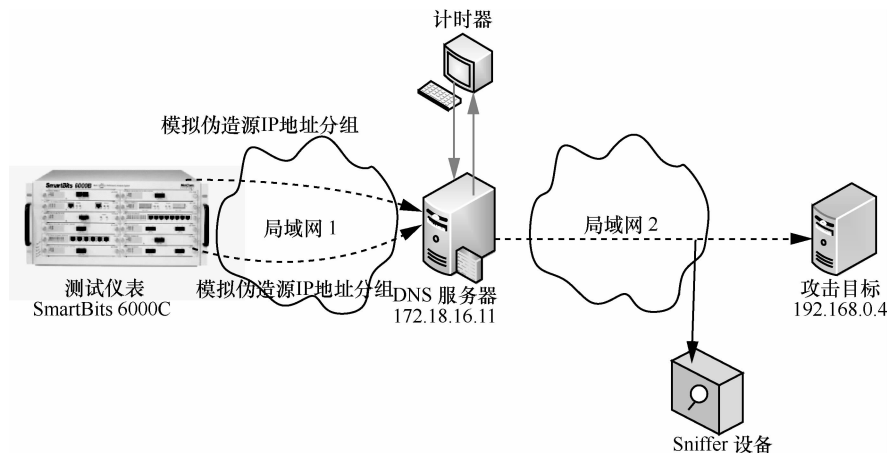


图3 伪造源 IP 地址攻击网络环境

表 1 基于不同 TTL 变化门限值的分布式 DNS 反射攻击检测率对比结果

计数器最大门限值变化次数/s	僵尸网络攻击端数目/个	攻击峰值总流量/pps	接收峰值总流量/pps	检测率
不启用	1	1 000	1 000	0.00%
	2	2 000	2 000	0.00%
	5	5 000	5 000	0.00%
	10	10 000	9 998	0.02%
1 000	1	1 000	1 000	0.00%
	2	2 000	1 635	18.25%
	5	5 000	1 356	72.88%
	10	10 000	1 082	89.18%
200	1	1 000	1 000	0.00%
	2	2 000	474	76.30%
	5	5 000	332	93.36%
	10	10 000	228	97.72%

会收到大量的 DNS 回应分组流量；当分别启动 2 台、5 台和 10 台攻击机发送伪造源 IP 地址的 DNS 查询数据分组时，由于不同攻击机发出的 DNS 查询分组 TTL 值均互不相同，计数器检测到源 IP 地址为 192.168.0.4 的 TTL 值频繁变动，导致计数器门限值计数会迅速累加，当门限值累计到 1 000 时，计数器将发送抑制指令，IP 地址为 172.18.16.11 的 DNS 服务器根据抑制指令，对所有源 IP 地址为 192.168.0.4 的 DNS 查询数据分组直接丢弃，测试数据可以看出，随着攻击机数目的增加，目标主机接收到的峰值流量占比迅速下降，检测率从 18.25% 提升到了 89.18%。又在计数器最大门限值设置为 200 次/s 的条件下展开测试，测试数据显示，由于最大门限值的降低，计数器能够更快发送抑制指令，随着攻击机数目的增多，检测率从 76.30% 提升到了 97.72%。

从可行性测试结果可看出，相对于传统的基于网络流量统计分析的检测方法，本文提出的基于 TTL 值智能研判的检测方法对检测僵尸网络产生的伪造源 IP 地址 DNS 反射攻击流量有明显效果，僵尸网络规模越大，伪造源 IP 地址的 DNS 查询分组越容易被本方法有效识别并过滤，从而避免了攻击目标遭受来自 DNS 服务器的反射流量攻击。

7 结束语

随着分布式 DNS 反射 DDoS 攻击流量的隐蔽性增强和攻击形式的层出不穷，传统的基于网络流量统计分析和网络流量控制等技术方法的误判率大幅度上升，多个检测器的协作问题也是安全性能提升的制约因素。基于真实 IP 地址对应主机发送的数据分组到达 DNS 服务

器所经过的路由跳数很难伪造的原理，本文提出了基于 TTL 值智能研判的分布式 DNS 反射 DDoS 攻击检测技术，能够有效识别近 90% 的源 IP 地址伪造分组，较好地解决了现有基于流量统计分析以及机器学习等技术方法存在误判率高、性能不足的问题；本文还提出了基于多系统融合的伪造源地址溯源阻断技术，极大地释放了此类攻击对运营商基础 IP 网络的带宽资源、DNS 系统计算资源及运维压力。

参考文献

1 国家互联网应急中心. 2013 年互联网网络安全态势综述, 2014
CNCERT. A Survey of Internet Security Situation in 2013, 2014

2 国家互联网应急中心. 2014 年互联网网络安全态势综述, 2015
CNCERT. A Survey of Internet Security Situation in 2014, 2015

3 罗志强, 史国水, 沈军等. 移动互联网安全热点技术研究. 电信科学, 2013(Z1): 254~256, 261
Luo Z Q, Shi G S, Shen J, *et al.* Research on mobile Internet security technology. Telecommunications Science, 2013 (Z1): 254~256, 261

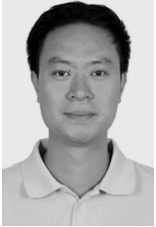
4 唐宏, 罗志强, 沈军. 僵尸网络 DDoS 攻击主动防御技术研究与应用. 电信技术, 2014(11): 76~80
Tang H, Luo Z Q, Shen J. Research and application of the active defense technology of DDoS attack in botnet. Telecommunications Technology, 2014(11): 76~80

5 徐图, 罗瑜, 何大可. 多类支持向量机的 DDoS 攻击检测的方法. 电子科技大学学报, 2008, 37(2): 274~277
Xu T, Luo Y, He D K. Detecting DDoS attack based on multi-class SVM. Journal of University of Electronic Science and Technology of China, 2008, 37(2): 274~277

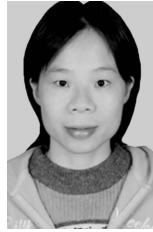


- 6 顾晓清, 王洪元, 倪彤光等. 基于时间序列分析的应用层 DDoS 攻击检测. 计算机应用, 2013,33(8): 2228~2231
- Gu X Q, Wang H Y, Ni T G, *et al.* Detection of application-layer DDoS attack based on time series analysis. Journal of Computer Applications, 2013, 33(8): 2228~2231

[作者简介]



罗志强,男,中国电信股份有限公司广州研究院云计算研究所高级工程师,主要研究方向为 DNS 安全和僵尸网络安全防护技术。



沈军,女,中国电信股份有限公司广州研究院云计算研究所高级工程师,主要研究方向为互联网流量聚类处理及 DNS 安全检测技术。



金华敏,男,中国电信股份有限公司广州研究院云计算研究所所长、高级工程师,主要研究方向为网络安全和流量安全防护技术。