DNS 放大攻击检测调研报告

作者：李玉冰

1. DNS 放大攻击原理

放大攻击的原理是利用了请求和响应的不平衡性。例如，发送一个 50 字节大小的请求包，返回 1 个或多个上百字节的应答包，即数十倍、上百倍的放大的攻击流量。结合反射攻击，使应答包的目的 IP 指向被攻击主机 IP，使得被攻击主机无法提供正常服务。

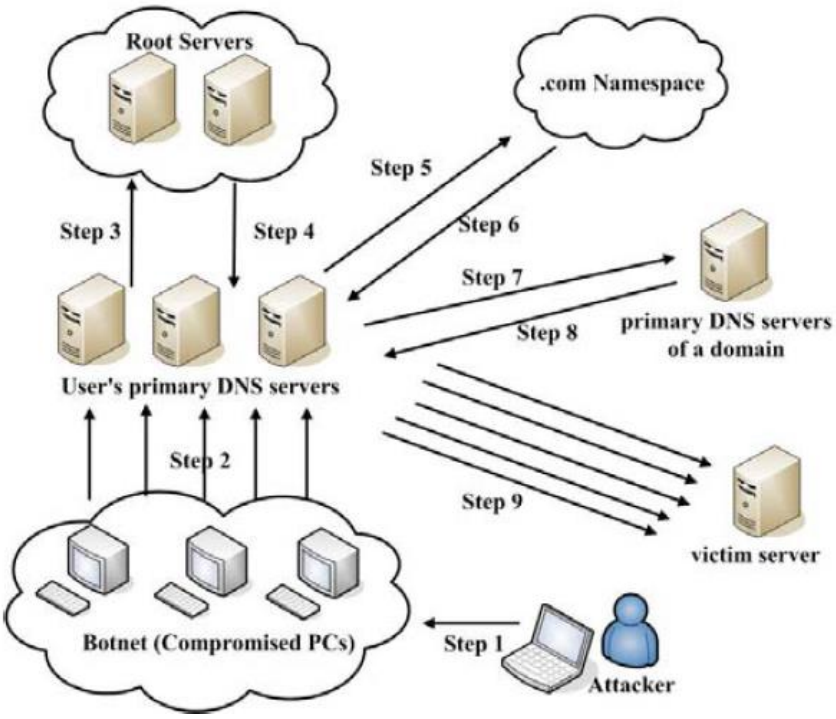

图 1-1 DNS 放大攻击的步骤

DNS 放大攻击(DNS Amplification Attacks)就是利用 DNS 协议的特点和缺陷，让目标主机接收到数量庞大且比请求包大得多的 DNS 应答包。普通的 DNS 请求包的大小一般 70 字节左右，DNS 应答包最大 512 字节(请求包的查询类型为 ANY)，超过 512 字节会被截断。实施 DNS 反射攻击，攻击流量能被放大 7 倍多。而利用 DNS 的扩展机制 EDNS，支持响应 UDP 数据包最大可达 4000 字节，这样攻击流量能被放大 60 倍左右。这个方法需要攻击者控制一个第三方 DNS 服务器，在上面存储一个 4000 字节的记录文本，用于响应查询请求。

著名的 DDoS 攻击防御服务提供平台 Cloudfare 对 DNS 放大攻击的定义和攻击流程说明[1]：此 DDoS 攻击是基于反射的体积分布式拒绝服务（DDoS）攻击，攻击者利用开放 DNS 解析器的功能来以大量流量淹没目标服务器或网络，从而使服务器和其周围的基础设施无法

访问。

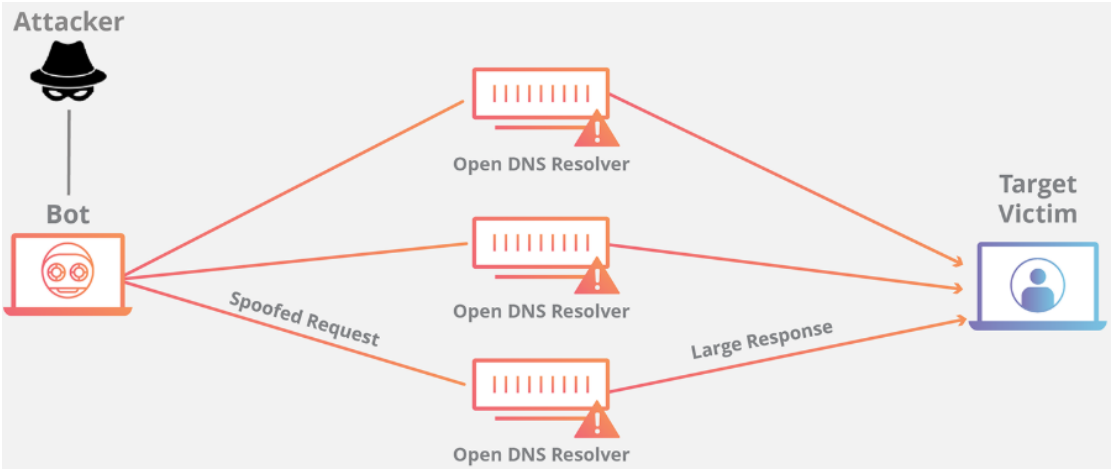

图 1-2 Cloudfare 的 DNS 攻击原理图

如图 1 所示，DNS 放大可分为四个步骤：

- 攻击者使用受感染的端点将具有欺骗性 IP 地址的 UDP 数据包发送到 DNS 递归服务器。数据包上的欺骗地址指向受害者的真实 IP 地址。
- 每个 UDP 数据包都会向 DNS 解析器发出请求，通常会传递一个参数（例如“ANY”），以便接收最大的响应。
- 收到请求后，DNS 解析器会尝试通过响应来提供帮助，它会对欺骗的 IP 地址发送较大的响应。
- 目标服务器的 IP 地址会收到响应，周围的网络基础结构将被大量的流量淹没，从而导致拒绝服务。

著名 DDoS 攻击防御服务提供平台 F5 对 DNS 放大攻击的定义[2]：域名系统（DNS）放大攻击只是许多类型的分布式拒绝服务（DDoS）攻击中的一种。与所有 DDoS 攻击一样，攻击者的目标是通过使响应速度缓慢或完全禁用它来阻止用户访问网络系统，服务，网站，应用程序或其他资源。大多数 DDoS 攻击都是体积式的，因为它们以超出其处理能力的流量轰击受害者的网络。攻击者的目标是将相对较小的 DNS 请求转换为巨大的响应。典型的 DNS 请求（仅几行文本）很小（通常为几十个字节），并且返回的响应仅仅比请求略大。攻击者以实质上放大响应大小的方式来设计 DNS 请求。一种实现方式是不仅请求类似 www.example.com 这样的网站的 IP 地址，而且请求有关整个域的信息（例如，对记录类型“ANY”使用 DNS 请求），因此响应可能包括有关子域，备份服务器，邮件服务器，别名等的详细信息。结果是，一个 10 字节的 DNS 请求可能会生成 10、20 甚至 50 倍大的响应。

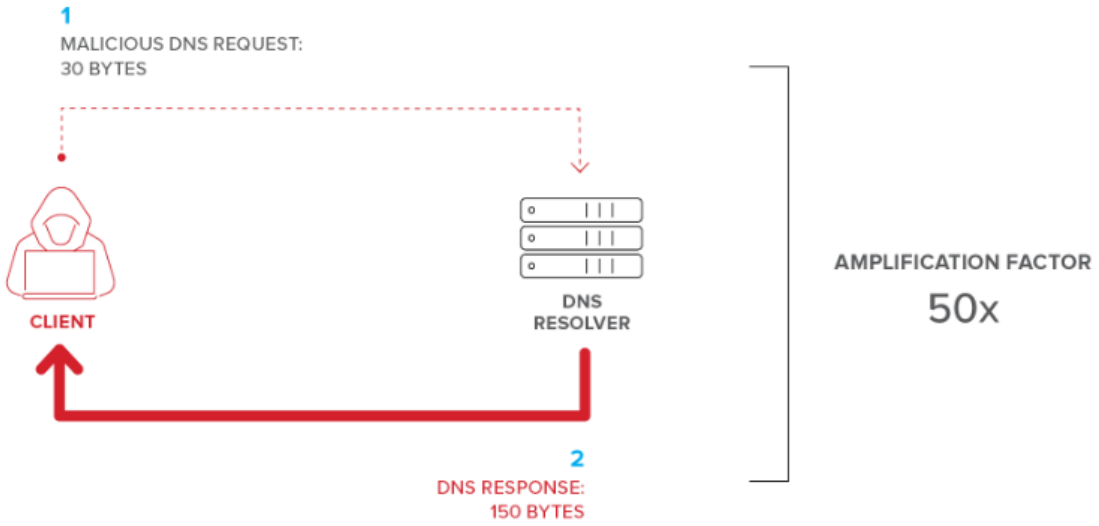

图 1-3 特制的 DNS 请求包导致得到放大 50 倍的响应

2. 研究现状

DNS 放大攻击一直是 DDoS 攻击的主流攻击手段之一。

2.1. 威胁报告

查找对提供 DDoS 防御服务的知名服务提供商如 Akamai、Cloudfare、Imperva、Radware、F5、Arbor、Nexusguard、NeuStar、DOSarrest 的 2019 年 DDoS 威胁报告，查找到与利用 DNS 攻击有关的结果如下。

Imperva 的报告[3]中显示 DNS Response 占 DDoS 攻击流量的 13%，DNS 占 DDoS 攻击流量的 3%。

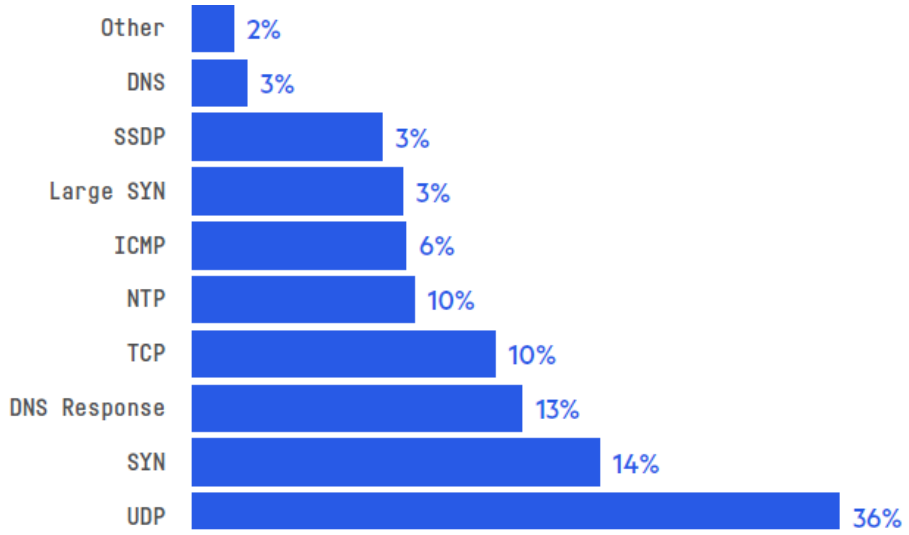

图 2-1 Imperva 威胁报告对攻击向量热门程度的划分

在 Nexusguard 的 2019 年第四季度报告[4]中提出，DNS 放大是整个 2019 年最常见的攻击类型。仅在第四季度，DNS 是最常被利用的媒介，放大攻击同比猛增近 3,000%。

在 Netscout 的 2019 年威胁报告[5]中指出，监测到的 DNS 攻击向量在攻击中的最大服务器数量为 107786。

Attack Vector		Max Servers in Attack	Percent of Population
Ar	ARMS	7,422	17.8%
Bc	BACnet	190	1.13%
Ch	CHARGEN	3,001	9.73%
Cd	CLDAP	8,874	86.87%
Co	COAP_v1	2,296	0.46%
Cp	COAP_v2	2,311	0.42%
Cx	Citrix-ICA	809	12.84%
Dn	DNS	107,786	6.32%

图 2-2：每种协议最大攻击所用服务器占可用服务器的百分比

国家计算机网络应急技术处理协调中心在《2019 年我国互联网网络安全态势综述》中指出[6]：对于来自境外的攻击，其主要攻击方式是 UDP Flood 、TCP SYN Flood 、Memcached Amplification 、NTP Amplification 和 DNS Amplification(DNS 放大)。这五种攻击占比达到 89%。

由此可见 DNS 放大攻击仍是一种流行的攻击手段。

2.2. 安全事件

在 2006 年 2 月，ICANN SSAC 报告了几次 DNS 放大攻击，该攻击使用大型 DNS 服务器淹没了其他受害者。

2013 年 3 月的 Spamhaus 的网络基础设施被认为是互联网历史上最大规模的此类网络攻击。Spamhaus 是负责将与垃圾邮件相关的来源列入黑名单的组织，该组织至少持续了一周的网络洪灾，其高峰期达到了 300 Gbps。多项研究工作的数据集就是基于此事件的数据集。此次事件中，攻击者发出的 DNS 请求数据包为 36 bytes，而 DNS 服务器的响应数据包长为 3000 bytes。攻击者就是利用这种方式，将攻击流量放大了近 100 倍。攻击者伪装来自 Spamhaus 向 DNS 系统发起请求，之后依靠返回的响应包对 Spamhaus 发起攻击，使得合法用户不能访问到 Spamhaus 的网站系统。

在 2016 年 7 月的一次攻击中，使用 DNS 放大的 DDoS 攻击导致了超过 363 Gbps 的洪

灾，Akamai 的一项研究显示，从 2015 年 11 月到 2016 年 2 月，使用 DNS 放大的 DDoS 攻击超过了 400 起[22]。

3. 防御方法

3.1. 常规防御手段

对于非技术人员来说，可购买 DDoS 防御服务来抵御 DNS 放大攻击。，DNS 放大攻击的防御措施有以下几点：

- 正确配置防火墙和网络容量；
- 增大链路带宽；
- 限制 DNS 解析器仅响应来自可信源的查询或者关闭 DNS 服务器的递归查询；
- 使用 DDoS 防御产品，将入口异常访问请求进行过滤清洗，然后将正常的访问请求分发给服务器进行业务处理。

3.2. 前人研究成果

在对于 DNS 放大攻击的研究中，2007 年和 2008 年有所研究，由于没有大型攻击事件，所以没有什么波浪。在 2013 年由于 Spamhaus 遭受到的 DNS 放大攻击，作为当时有史以来最大的 DDoS 攻击，对 DNS 放大攻击的研究再次兴起。随着 SDN 技术和机器学习的发展，对于 DNS 放大攻击的研究持续至今。对 DBLP 收录的全部与 DNS 放大攻击有关的论文进行略读，总结如下。

文献[7]提出一种简单实用的方案，使管理员能够区分真实的和伪造的 DNS 答复。基于 DNS 请求和响应的**一对一映射思想**，使用 IPtraf 工具记录 DNS 请求和响应，对于没有映射关系的数据（孤立对）分类为可疑并丢弃。作者基于 PHP 定制工具，即 DNS Amplification Attacks Detector（DAAD），实时处理捕获的数据，该 DAAD 工具的界面可从以下网址公开访问：http://f6tmos.samos.aegean.gr/~tmos，用户名：user，密码：kalimera！(连接已失效，此文章可能一稿多投，另一稿名为“A fair solution to dns amplification attacks”)。

文献[8]为 DNS 放大攻击开发实时交互式**可视化系统**（RTIVS），帮助管理员可视化和分析流量，并检测 DNS 放大攻击。RTIVS 的设计基于 DNS 放大攻击的特征：使用 53 端口、响应中有大量 UDP 数据包、输入和输出 IP 地址不匹配。它提供手动模式和自动模式，以支持推理和识别 DNS 放大攻击。管理员可以轻松地监视网络活动并实时分析大量 UDP 数据包，通过设置 UDP 数据包的阈值来预防 DNS 放大攻击。使用模拟 DNS 放大攻击进行测试。

文献[9]中提出了一种高效低成本的**硬件方法**，先快速地检测 DNS 放大攻击。确认攻击后，以使用两种血液过滤器解决方案过滤掉所有非法的 DNS 响应。利用 DNS 协议的语义特征：DNS 请求和响应的**一对一映射**，但不需要维护映射关系。检测阶段只用几个计数器来检测 DNS 放大攻击的准确性和响应时间，检测到放大攻击严重到足以超过预定义的阈值之

后，进入过滤阶段，以合理的计算和内存成本将合法的 DNS 响应与攻击流量区分开，使用两布隆过滤器解决方案。通过仿真对方案进行评估。

文献[10]针对 DNS 放大带宽攻击(DNS BAA)，基于 DNS BAA 的连续时间马尔可夫链（CTMC）模型，使用**概率模型检查器 PRISM** 对 DNS BAA 进行正式建模和分析，提出三种对策：数据包过滤，随机数据包丢弃和对合法数据包的主动重试。用模型表示受害服务器的带宽争用情况，且由于 BAA 造成虚假流量时为合法请求提供服务。当达到可用带宽（用于处理合法 DNS 流量）的模型状态时，攻击成功。通过连续随机逻辑（CSL）中表示的概率可达性属性来计算攻击概率。对于 DNS 和 DNSSec，都使用来自当时 DDoS 事件的数据或文献中报道的放大效应的测量值来建立模型参数值。

文献[11]提出了一种新的、隐蔽的由 DNSSEC(**DNS 安全扩展)驱动的放大攻击**形式，它利用了大量 DNS 转发器的优势。DNSSEC 相关的 RR（RRSIG，DNSKEY，DS，NSEC3）的大小很大，攻击者利用那些支持 DNSSEC 相关资源记录的响应包作为攻击流量。

文献[12]对**布隆过滤器**的结构进行了修改，提出了针对放大攻击的防御措施。设置两个布隆过滤器一个用于传入响应，一个用于传出响应，当用户向服务器发出请求时，过滤器会存储您的请求并等待响应，如果响应在给定的时间间隔内，则服务器将允许流量通过。如果响应不在给定时间内，则将触发布隆过滤器并阻止该特定 IP。文章的特点在于可以对布隆过滤器进行编辑，并维护先前用户的日志文件，并设置新用户、老用户、黑名单。

文献[13]提供了一个**博弈论模型和分析**，作者发现一般都是经过精心策划后才能获得目标 IP，所以设计模型，让攻击者很难获取到目标 IP。文章设计了一种防反射机制，当滥用 DoS 攻击时，该机制可以消除 DNS 响应的放大因子，**让攻击者消耗的资源量与受害者相同**。

文献[14]提出了一种利用暗网空间来推断和表征 Internet 级 DNS 放大 DDoS 攻击的新颖方法。攻击者通过在暗网内的 DNS 查询，到达 Internet 上开放的 DNS 解析器，本文通过分析**对暗网空间的 DNS 查询**，将输入暗网流量作为输入，从而推断出 DNS 放大攻击，并输出推断出的 DNS 放大攻击活动。该方法基于两个组件：检测和速率。如果检测组件已经向不同的未使用暗 IP 地址发送了至少 25 个 ANY 类型的 DNS 查询，则将流量标记为 DNS 放大 DDoS 攻击。从/13 地址空间收集的 720 GB 真实暗网数据，对所提出的方法进行了经验评估，该方法成功地推断出重要的 DNS 放大 DDoS 活动，包括当时针对最大的反垃圾邮件组织之一的著名攻击。

文献[15]是同一拨人把文献[10]的内容改进了一下重做了一遍。

文献[16]提出并评估一种简单的缓解攻击的方法，目标组织可以使用该方法来缓解攻击，以最小的努力度过极大量的 DNS 放大攻击。文章建议企业将服务远程托管给权威 DNS 服务器，对所有 DNS 流量进行上游过滤，以减轻 DDoS 攻击。还建议企业将 DNS 查询通过隧道传输到远程 DNS 解析器，例如由云提供商或 ISP 托管的远程 VM。

文献[17]提出之前的解决方案必须预先确定参数，这在许多情况下并不容易。而文献[17]的研究中，利用**检测模式和三种功能的组合**来区分正常攻击和攻击，可以解决在高频低放大攻击的情况下检测的局限性的问题。检测方法利用从受监视网络的历史数据中学到的检测模式和三个功能来区分 DNS 服务器上的正常时间段和异常时间段，三种功能为：DNS 请求的频率，一个时间段内放大的数据流量的速率（响应流量/请求流量）和一个时间段内增加的数据包数量。使用 Shumon Huque 在他的博客中发布的数据集模拟攻击流量，使用 kdd cup 99

数据集模拟正常流量。

文献[18]提出了一个由三个阶段组成的防御机制。防御机制可以轻松检测到攻击，快速保护受害者，然后查明所有僵尸并最终将它们与 SDN 网络隔离。文章参考熵算法，结合一对一映射关系，充分**利用 OpenFlow 1.3 协议和 SDN 架构的可见性**。它部署了两级流表和一个计量表来监视 DNS 请求数据包的速度。一旦数据包的速度超过了 SDN 交换机中电表条目中给定的阈值，控制器就会从 SDN 交换机接收警报消息。通知后，控制器开始收集超速数据包，并使用熵算法识别可疑受害者。然后，它可以迅速确认攻击并同时保护可疑受害者。最后，如果发生攻击，则控制器可以追溯攻击路线，查明僵尸并成功隔离它们。使用 Scapy 生成攻击流量。

文献[19]提出一种检测 DNS 放大攻击的机制。文章通过对 DNS 攻击数据集和普通数据集选择 DNS 参数，基于决策树（TREE），多层感知器（MLP），朴素贝叶斯（NB）和支持向量机（SVM）等**机器学习分类算法**对 DNS 流量数据包进行了比较分析，以将 DNS 流量分类为正常和异常。在这种方法中，使用诸如信息增益，增益比和卡方的属性选择算法来实现最佳特征子集。实验结果表明，决策树的准确率达到 99.3%。与其他机器学习算法相比，该模型具有最高的准确性和性能。

文献[20]提出了一种通过 **sFlow 与以安全为中心的 SDN** 的替代解决方案，以及时检测并合理缓解 DNS 放大攻击。首先从转发设备收集流数据，然后检查数据包头中的预定义流值，以查看流量是否源自 DNS 服务器。sFlow 使聚合流可以通过即时缓存立即导出。如果源端口号不是 53，则将流存储在普通缓存中，否则将其存储在立即缓存中。然后通过查看 DNS 应用程序数据来进一步检查过滤后的 DNS 流量。如果流记录中存在匹配的请求查询 ID，则将流量归类为普通 DNS 响应，否则标记为可疑响应，并将标记的流转发到 SDN 控制器以进行缓解。OpenFlow v1.3 带来了流量整形的支持；允许 SDN 控制器根据指定的减速参数（仪表表）更改每个流条目（流表）中数据包的频率。

文献[21]发现，先前的工作主要将 DNS 请求记录在交换机缓存或远程服务器缓存中。在本文中，通过使用软件定义的网络（SDN）为 DNS 查询提供高度健壮和可扩展的数据存储，提出了一种更灵活的模型，该模型最近被引入以使网络系统中的数据和控制平面分离。通过**使用 SDN 控制器来存储所有 DNS 查询记录**，为了检查 DNS 请求和响应之间的“一对一严格映射”，由良性主机生成的 DNS 请求首先存储在交换机的本地内存中，如果该交换机不再具有可用的存储空间，则进一步的 DNS 请求将存储在外部网络实体（例如 SDN 控制器或另一个远程服务器）的存储器中。

文献[22]认为公开的 DNS 服务器缺乏保护，对所有公开请求都进行响应，分析了与 DNS 放大攻击相关的潜在攻击，这些攻击集中于使用权威服务器作为放大器。

文献[23]提出了一种可以保护网络免受这些大型 DNS 放大攻击的解决方案，使用一组地理上分散的路由器，称为**路由器屏障（BoR）**，Anycast-Barrier 和 Proxy-Barrier。想进行自我保护的网络将通过此屏障路由所有传入和传出的流量，屏障会扫描所有传入流量，丢弃攻击流量，并将其余的发送给预期的接收者。对于某些类型的攻击，如 DNS 放大攻击，在可以达到的假设条件下，屏障可以几乎完全准确地缓解攻击流量。因此，到达受害者的攻击数据包的数量可以忽略不计。

文献[24]研究了在 DNS 放大攻击中将 TLD ANSes 用作未知代理的可能性，对 root.zone

文件进行分析。文章**评估了将 TLD ANSes 用作放大器和反射器的潜力**，测量 ANY 和 DNSKEY 查询类型的 DNS 响应。文章证明，当时的 TLD ANSes 可以有效地用作 DNS 放大 DDoS 攻击中的未知代理。文章提供针对 DNSSEC 相关查询的恶意反映响应量的测量结果，并计算相应的 AF。

文献[25]提出将作者之前提出的 DNS CNAME 链式攻击和脉冲透镜攻击的一种形式[temporal lens]结合在一起，组合成一种新的**基于公开 DNS 解析器的放大攻击**。文章设计了一个优化问题，并使用遗传算法解决。并提出了应对攻击的对策。

文献[26]是最新的一篇关于 DNS 放大攻击的文献。文章提出了一种 DNS 放大攻击防御系统(DAAD)，该系统可以**使用流控制技术来阻止 SDN 环境中**来自未经请求的 DNS 查询的响应消息。当交换机从网络内部的主机接收到 DNS 查询时，它将有关查询的信息发送到控制器。控制器为与来自交换机的查询相对应的即将到来的 DNS 响应消息安装新的流规则，帮助交换机过滤掉伪造的 DNS 响应消息。该系统设置在 SDN 控制器中，用来管理交换机的所有流规则。攻击数据包使用 Scapy 生成。

3.3. 总结和思考

DNS 放大攻击是 DDoS 攻击的常用手段之一，可选购合适的 DDoS 防御服务进行部署。

对于 DNS 放大攻击，研究上的防御思路为，记录请求和响应的一一对应关系，一种是存储映射关系，二是使用计算的方式，用布隆过滤器存储映射关系。另一个是控制 DNS 应答包的速率阈值。在此基础之上，设计了各种模型，预设参数，通过模型来防御 DNS 放大攻击。SDN 技术经过了一定的发展以后，映射关系的存储位置由交换机、服务器缓存转移到了 SDN 控制器上。

根据以上对 DNS 攻击研究路线的总结，可以看到目前的趋势是将新的设备和新的概念技术应用到旧的攻击和防御手段中去。当下热门的研究方向有深度学习和 SDN 的数据面可编程。所以在未来一是可以用深度学习进行 DNS 放大攻击流量的识别；二是使用 P4 交换机，将 DNS 请求和响应的映射关系在支持 P4 的高速硬件上进行处理，加快处理速度，减少影响 DNS 正常服务的时间，避免正常的 DNS 解析服务无法进行。三是将提到的两点结合起来，用深度学习建立攻击流量识别模型，得出合适的数值参数，在控制面实现和设定，最终对流量的处理在支持 P4 的硬件上进行，争取更加准确高效地识别出 DNS 放大攻击流量。

4. 数据集

DNS 放大攻击的公开数据集主要是 Spamhaus 事件的数据集，其他研究大多数是使用工具基于攻击模型用 Scapy 生成攻击数据包。还有如文献[22]与域名区域维护者进行联系得到区域文件进行分析，数据并没有公开。DNS 放大攻击提到的数据集一般包括两方面，一是普通数据集，二是攻击数据集。数据集都比较大，不提供下载后的版本，有需求可自行下载。

（1）CAIDA 提供的数据集

地址：https://www.caida.org/data/overview/completed-datasets.xml

可以通过两种互补的方式请求访问 CAIDA 数据：通过 CAIDA 门户网站和通过网络风险和信任政策与分析信息市场（IMPACT）门户网站。其中 DDoS 相关的数据需要**购买**或者**提出申请**才可以访问。

Name	Status	Availability
enter text here to filter by partial name		e.g. public
Anonymized Industry Evaluation Internet Traces Dataset	Complete	Request access (download)
Anonymized Internet Traces	Complete	Request access (download)
Anonymized Internet Traces on IPv6 Day and IPv6 Launch Day	Complete	Request access (download)
Anonymized Internet Traces Summary Statistics	Complete	Public
AS Links: IPv4 Routed /24 AS Links	Complete	Public
AS Relationships	Complete	Public
IPv4 2013 Census dataset	Complete	Request access
OC48 Peering Point Traces (2002-2003)	Complete	Public

图 4-1 CAIDA 数据集

（2）Spamhaus 的攻击数据集

地址：http://blog.huque.com/2013/04/dns-amplification-attacks.html

虽然多篇论文都用此公开数据集，但只在文献[17]中查询到上面贴出的地址，但是无法打开，此处还是列出，可能是网络问题，也可能时间久远已经失效。

（3）kdd cup 99 的数据集

地址：http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

这是 KDD-99 第五届知识发现和数据挖掘国际会议同时举行的第三届国际知识发现和数据挖掘工具竞赛所使用的数据集。竞争任务是建立一个网络入侵检测器，这是一种能够区分称为入侵或攻击的“不良”连接与“正常”的正常连接的预测模型。该数据库包含一组要审核的标准数据，其中包括在军事网络环境中模拟的多种入侵。已下载。

Data files:

- kddcup.names A list of features.
- kddcup.data.gz The full data set (18M; 743M Uncompressed)
- kddcup.data_10_percent.gz A 10% subset. (2.1M; 75M Uncompressed)
- kddcup.newtestdata_10_percent_unlabeled.gz (1.4M; 45M Uncompressed)
- kddcup.testdata.unlabeled.gz (11.2M; 430M Uncompressed)
- kddcup.testdata.unlabeled_10_percent.gz (1.4M;45M Uncompressed)
- corrected.gz Test data with corrected labels.
- training_attack_types A list of intrusion types.
- typo-correction.txt A brief note on a typo in the data set that has been corrected (6/26/07)

图 4-2 KDD-99 提供的数据集

（4）SimpleWiki 收录的和 DNS 有关的数据集

地址：https://www.simpleweb.org/wiki/index.php/Traces

该网站收录了许多 DNS 数据集。如图 4-3，直接点击“Filename”栏的链接即可下载数

据。已选取和 DNS 放大攻击相关的数据集下载。

Datasets for DNSSEC-signed domains

Top-level domain	Filename	File size	SHA256 hash
.com	com.dnssec.db.gz	841M	c69d8bd680825bac272e97b0575a07e90ccbe4ffb2492e13edca4781fb574b7d
.net	net.dnssec.db.gz	174M	e6c2b600c895a30b90fb1dc126a0ae55b28d0d6e0378164f4bca12b0b259bfa9
.org	org.dnssec.db.gz	113M	aff93cb57405d9131567e9d4b687dbd86067c8c162ab28528be3b09ca3f11a08
.nl	nl.dnssec.db.gz	3.8G	740ea3b30c23992ee00a9d595982f0635eb67b12c13c4338b4e39afd72ecfeaa
.se	se.dnssec.db.gz	601M	af2d4a8b1503d021f9151136f39eb843809684de26d64ab3e4a47594953fd4df
.uk	uk.dnssec.db.gz	25M	dda8f4320d7dd8ce44d52bf4d59c30b2dc043fca01cefec06a8922494acb1e93

Datasets for regular domains

Top-level domain	Filename	File size	SHA256 hash
.com	com.non-dnssec.db.gz	1023M	ce3b98e524f4f3589ed4e9a746bf88314a5c3e0815193e21ef98f286d5f787fb
.net	net.non-dnssec.db.gz	209M	47679adee3eb0b8228e4fae98596db64b605aef5ee35324c228e8531a86d2f45
.org	org.non-dnssec.db.gz	209M	0d57968b4734501fba52bca310bbf2e76684a82fe86b393e1dca1a97f4d55758
.nl	nl.non-dnssec.db.gz	1.9G	b07548f8d7ea2d3baf28971d2ec89f5fcf5235c3cee5b3543a159079e2e208a6
.se	se.non-dnssec.db.gz	605M	e2194c2ecedbd962cc5a51411edee9569061228693afc86881f57cda29d300cd
.uk	uk.non-dnssec.db.gz	39M	8809d590c26fb25c903c3ce037c5cc9ec1d28e7a5e6ef90d13b464cd9f6040f4

图 4-3 SimpleWiki 收录的 DNS 数据集

5. 参考文献

[1] Cloudfare 对 DNS 放大攻击的定义：https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/

[2] F5 对 DNS 放大攻击的定义：https://www.f5.com/labs/articles/education/what-is-a-dns-amplification-attack-

[3]Imperva 的 2019 年 DDoS 报告：https://www.imperva.com/blog/2019-global-ddos-threat-landscape-report/

[4] Nexusguard 的 2019 年第四季度报告：https://blog.nexusguard.com/threat-report/ddos-threat-report-2019-q4

[5]Netscout2019 年威胁报告：https://www.netscout.com/blog/asert/netscout-threat-intelligence-report

[6]国家计算机网络应急技术处理协调中心的 2019 年我国互联网网络安全态势综述：https://www.cert.org.cn/publish/main/46/2020/20200420191144066734530/20200420191144066734530_.html

[7] Kambourakis G, Moschos T, Geneiatakis D, et al. Detecting DNS amplification attacks[C]//International workshop on critical information infrastructures security. Springer, Berlin, Heidelberg, 2007: 185-196.

[8] Yu H, Dai X, Baxley T, et al. A real-time interactive visualization system for DNS amplification attack challenges[C]//Seventh IEEE/ACIS International Conference on Computer and Information Science (icis 2008). IEEE, 2008: 55-60.

[9] Sun C, Liu B, Shi L. Efficient and low-cost hardware defense against DNS amplification attacks[C]//IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference. IEEE,

2008: 1-5.
[10] Deshpande T, Katsaros P, Basagiannis S, et al. Formal analysis of the DNS bandwidth amplification attack and its countermeasures using probabilistic model checking[C]//2011 IEEE 13th International Symposium on High-Assurance Systems Engineering. IEEE, 2011: 360-367.
[11] Anagnostopoulos M, Kambourakis G, Kopanos P, et al. DNS amplification attack revisited[J]. Computers & Security, 2013, 39: 475-485.
[12] Sattar U, Naqash T, Zafar M R, et al. Secure DNS from amplification attack by using modified bloom filters[C]//Eighth International Conference on Digital Information Management (ICDIM 2013). IEEE, 2013: 20-23.
[13] Herzberg A, Shulman H. DNS authentication as a service: preventing amplification attacks[C]//Proceedings of the 30th Annual Computer Security Applications Conference. 2014: 356-365.
[14] Fachkha C, Bou-Harb E, Debbabi M. Fingerprinting internet DNS amplification DDoS activities[C]//2014 6th International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2014: 1-5.
[15] Deshpande T, Katsaros P, Smolka S A, et al. Stochastic game-based analysis of the DNS bandwidth amplification attack using probabilistic model checking[C]//2014 Tenth European Dependable Computing Conference. IEEE, 2014: 226-237.
[16] MacFarland D C, Shue C A, Kalafut A J. Characterizing optimal DNS amplification attacks and effective mitigation[C]//International Conference on Passive and Active Network Measurement. Springer, Cham, 2015: 15-27.
[17]Cai L, Feng Y, Kawamoto J, et al. A behavior-based method for detecting DNS amplification attacks[C]//2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS). IEEE, 2016: 608-613.
[18] Xing X, Luo T, Li J, et al. A defense mechanism against the DNS amplification attack in SDN[C]//2016 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC). IEEE, 2016: 28-33.
[19] Meitei I L, Singh K J, De T. Detection of DDoS DNS amplification attack using classification algorithm[C]//Proceedings of the International Conference on Informatics and Analytics. 2016: 1-6.
[20] Aizuddin A A, Atan M, Norulazmi M, et al. DNS amplification attack detection and mitigation via sFlow with security-centric SDN[C]//Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication. 2017: 1-7.
[21] Kim S, Lee S, Cho G, et al. Preventing DNS amplification attacks using the history of DNS queries with SDN[C]//European Symposium on Research in Computer Security. Springer, Cham, 2017: 135-152.
[22] MacFarland D C, Shue C A, Kalafut A J. The best bang for the byte: Characterizing the potential of DNS amplification attacks[J]. Computer Networks, 2017, 116: 12-21.
[23] Gupta V, Sharma E. Mitigating DNS Amplification Attacks Using a Set of Geographically Distributed SDN Routers[C]//2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, 2018: 392-400.
[24] Anagnostopoulos M, Kambourakis G, Gritzalis S, et al. Never say never: Authoritative tld nameserver-powered dns amplification[C]//NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2018: 1-9.

[25] Bushart J. Optimizing Recurrent Pulsing Attacks using Application-Layer Amplification of Open {DNS} Resolvers[C]//12th {USENIX} Workshop on Offensive Technologies ({WOOT} 18). 2018.
[26] Han M, Canh T N, Noh S C, et al. DAAD: DNS Amplification Attack Defender in SDN[J]. 2019.