软件学报 ISSN 1000-9825, CODEN RUXUEW
2026,37(4):1801−1818 [doi: 10.13328/j.cnki.jos.007429] [CSTR: 32375.14.jos.007429]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于大型 DNS 递归服务的域名访问模式测量与分析*

张 宾[1], 杨书徒[1], 姬东岑[1], 张 宇[1,2], 张伟哲[1,2], 涂唯坚[1], 戴一娜[1]

[1](鹏城实验室, 广东 深圳 518055)

[2](哈尔滨工业大学 网络空间安全学院, 黑龙江 哈尔滨 150001)

通信作者: 张宇 E-mail: yuzhang@hit.edu.cn

摘 要: 域名系统 (domain name system, DNS) 协议的性能和操作特性引起了研究和网络运营界的极大兴趣. 在这项工作中, 通过测量分析来自一个大型 DNS 服务商的递归服务器数据, 从一个大型 DNS 运营商递归服务的角度考察了用户访问模式及解析状况. 面向海量的 DNS 数据, 首先提供一种多机分布式并行测量机制和大数据平台存储监控方案, 实现了对 DNS 海量数据的高效测量分析. 然后, 从用户请求响应率、请求域名的情况、请求用户的情况和域名解析的情况多个维度系统分析了 DNS 数据的特征, 并呈现了多个有价值的测量结果, 对提升 DNS 的运维和洞察 DNS 的特性具有重要价值. 最后, 基于对 DNS 缓存命中率的测量分析, 提出一种适用于 DNS 大型运营商进行在线异常检测的通用框架, 并初步验证了框架方案的正确性和可行性.

关键词: 域名系统; 域名系统安全; 网络测量; 攻击检测

中图法分类号: TP393

中文引用格式: 张宾, 杨书徒, 姬东岑, 张宇, 张伟哲, 涂唯坚, 戴一娜. 基于大型DNS递归服务的域名访问模式测量与分析. 软件学报, 2026, 37(4): 1801–1818. http://www.jos.org.cn/1000-9825/7429.htm

英文引用格式: Zhang B, Yang ST, Ji DC, Zhang Y, Zhang WZ, Tu WJ, Dai YN. Measurement and Analysis of Domain Access Patterns Based on Large-scale DNS Recursive Services. Ruan Jian Xue Bao/Journal of Software, 2026, 37(4): 1801–1818 (in Chinese). http://www.jos.org.cn/1000-9825/7429.htm

Measurement and Analysis of Domain Access Patterns Based on Large-scale DNS Recursive Services

ZHANG Bin[1], YANG Shu-Tu[1], JI Dong-Cen[1], ZHANG Yu[1,2], ZHANG Wei-Zhe[1,2], TU Wei-Jian[1], DAI Yi-Na[1]

[1](Pengcheng Laboratory, Shenzhen 518055, China)

[2](School of Cyberspace Science, Harbin Institute of Technology, Harbin 150001, China)

Abstract: The performance and operational characteristics of the domain name system (DNS) protocol continue to attract significant attention from both the research community and network operators. In this study, data collected from a large-scale DNS recursive service is measured and analyzed to examine user access patterns and resolution behavior from the perspective of a major DNS operator. To handle the massive volume of DNS data, this study proposes a distributed parallel measurement mechanism and a big data-based storage and monitoring solution, enabling efficient processing and analysis. The characteristics of DNS data are systematically examined across several dimensions, including user request response rates, domain name request patterns, user distribution, and resolution outcomes. Several valuable insights are presented, offering meaningful guidance for DNS operation optimization and improved understanding of DNS behavior. Finally, based on the analysis of DNS cache hit rates, this study proposes a general framework for online anomaly detection tailored to large-scale DNS operators. The correctness and feasibility of the proposed framework are preliminarily verified.

Key words: domain name system (DNS); DNS security; network measurement; attack detection

---

* 基金项目: 国家重点研发计划 (2024YFB31NL00105); 鹏城实验室重大攻关项目 (PCL2023A05); 广东省基础与应用基础研究重大项目 (2019B030302002)
收稿时间: 2024-10-28; 修改时间: 2025-01-22; 采用时间: 2025-03-17; jos 在线出版时间: 2025-07-17
CNKI 网络首发时间: 2025-07-18

域名系统通过实现域名与 IP 地址的双向关联, 在互联网的运行中发挥着重要作用. 其架构实现为一个具有几个受信任的根服务器的分层系统, 这些根服务器将管理域名到 IP 地址映射的责任分配给与每个域对应的数亿个权威名称服务器, 负责相应域名的权威解析. 递归服务器直接面对用户, 负责将用户的 DNS 请求对权威服务器进行迭代查询, 并向用户返回最终解析结果. DNS 在互联网运行中起着至关重要的作用, 在文献 [1] 中我们从递归侧安全的角度对 DNS 运行及相关安全及防御问题进行了全面的梳理, 总结和分析.

鉴于 DNS 对互联网的运行和安全至关重要, 在过去 10 年中, 它一直是许多测量研究的主题. 先前的测量研究包括测量 DNS 缓存的行为[2], 从根服务器的角度测量全局 DNS 活动[3,4], 并评估了 DNS 在 CDN 中的有效性[5]. Danzig 等人[6]首次对全球 DNS 活动进行了研究, 揭示了 DNS 实现中许多漏洞的普遍性. Gao 等人[7,8]通过分析从安全信息交换 (security information exchange, SIE)[9]采集的全球几百个递归服务器解析数据, 揭示了超过 50% 到根服务器的 DNS 请求不能返回正确的应答. Kim 等人[10]对域名系统漏洞和攻击进行了调查, 为了解 DNS 面临的安全挑战提供了全面的视角. 文献 [11] 从客户端测量递归服务器的部署情况, 文献 [12] 测量了 DNS 加密协议 (DNS-over-encryption, DoE) 的部署和服务状况, 文献 [13] 对 DNS over HTTPS 流量的测量和表征提供了对新兴 DNS 协议性能的深入分析. 还有些工作[14−17]测量了解析路径被劫持的状况. 文献 [18] 的研究关注了 IPv6-only 环境下的 DNS 解析问题, 揭示了大型 DNS 提供商在推动 IPv6 适应性方面的重要作用, 强调了在全球范围内推广 IPv6 的必要性, 而我们对 IPv6 解析情况的研究也与此呼应.

目前尚无测量工作专门针对一个大型的 DNS 运营商, 从大型 DNS 服务商的角度分析域名的访问模式, 特别是缺乏对国内大型 DNS 服务商域名访问模式的测量. DNS 服务商难以从海量的 DNS 流量数据中掌握用户的访问情况及自身的解析状况, 难以更具针对性地进行服务质量和安全状况的运维提升, 本文针对这一现状, 通过对国内一个著名 DNS 大型运营商 DNS 服务的具体测量, 提出了一种高效的海量 DNS 数据的测量方法, 并基于该方法对海量 DNS 数据进行了详细的测量结果分析, 进一步提出针对测量结果的运维和部署建议, 对提升 DNS 运维效率、优化服务质量以及加强互联网基础设施的安全具有重要意义.

通常, 对于大型的 DNS 服务商, 可以利用 ISP 提供的 DNS 服务, 也可以利用第三方商业 DNS 运营商 (如谷歌、OpenDNS、CloudFlare、阿里 DNS、114DNS、360DNS、DNSPod 等) 提供的 DNS 服务. 在许多情况下, ISP 很少向外提供数据服务, 需要求助于第三方商业 DNS 提供商. 在此项工作中, 通过和中国最大的几家商业服务商中的其中一家 DNS 服务商合作, 从服务商中用户请求 DNS 服务的角度分析域名的访问情况和 DNS 的具体解析状况.

合作方服务商是中国最大的第三方 DNS 提供商之一, 全国递归服务节点超过 100 个, 覆盖了国内主流的运营商, 每日 DNS 解析量超过千亿次, 小时在线域名解析用户数超过 1 000 万, 分布在全国多个省和直辖市, 服务了中国大约 1/10 的用户. 因此, 针对此服务商的 DNS 服务数据进行分析, 对全面了解我国的 DNS 服务情况非常重要, 可以窥一斑而知全豹.

在这项工作中, 面向大型 DNS 服务商的用户请求和 DNS 解析的海量 DNS 数据, 本文首先提供了一种多机分布式并行测量机制和大数据平台存储监控方案, 对 DNS 海量数据进行高效的测量分析; 然后, 从用户请求响应率, 请求域名的情况, 请求用户的情况和域名解析的情况系统分析了 DNS 数据的特征; 最后, 基于对 DNS 数据的测量分析, 本文提出了一种适用于 DNS 大型运营商在线检测异常的通用框架, 本文的主要贡献如下.

1) 通过对不同线程解析 DNS 报文的比对分析, 本文提出了一种多机分布式并行报文分发和分析机制, 高效地完成对运营商级别海量数据的分析处理, 并对分析处理结果进行大数据平台存储和状态监控, 以高效实现对各类分析的查询, 并及时处理测量分析程序的异常情况.

2) 通过 DNS 具体数据的分析, 本文从 DNS 用户请求及响应、用户请求状况、根服务器解析情况多角度分析了国内大型运营商的域名访问模式和解析状况, 对比了国内大型运营商和国外 DNS 服务商在域名访问模式上的具体差异, 并提出了提升 DNS 运维效率、优化服务质量的具体建议.

3) 基于对缓存命中率的测量结果, 本文探索了一种适用于大型 DNS 运营商的基于黑白名单机制的检测框架, 这个框架方案适用于已有的 DNS 异常检测方法, 实现了从递归服务器用户侧端口的检测转移到权威侧端口流量的检测目标, 待检测的流量极大下降, 使得大型服务商实时在线的检测实施成为可能, 并初步验证了检测框架的正

确性和可行性.

本文第 1 节介绍 DNS 测量相关的工作. 第 2 节简要介绍被测量的 DNS 数据. 第 3 节对具体的测量方案进行详细剖析. 第 4 节对 DNS 数据进行全面的测量分析和对 DNS 异常检测框架的探索. 第 5 节进行简要总结.

1 相关工作

许多先前的研究已经测量了 DNS 基础设施的性能, 主要有对根服务器服务状况的测量, 对解析劫持情况的测量, 对递归服务器服务情况的测量及其他方面的测量, 本文分别简要介绍.

对根的测量: 在根服务器上进行的多项测量研究报告称[3,4,19,20], 根服务器上很大一部分流量是无效的. 特别是, Brownlee 等人[3]发现, 对 F-根服务器的 60%–85% 的查询是重复的. Castro 等人[4]分析了从多个根服务器收集的流量, 并报告称 98% 的流量是无效的. Castro 等人[19]在后来的一项研究中证实, 一小部分繁忙的客户端 (0.55%) 在根服务器上产生的无效流量最多.

对解析劫持的测量: 文献 [12−15] 测量了解析路径被劫持和解析错误的状况, 文献 [14] 通过对 IP 的 DNS 请求, 测量推断出互联网上有 291 528 台主机执行不正确或恶意的 DNS 服务, 以及许多其他主机提供了不正确和误导性的答案. 文献 [15] 通过主动向 3 种类型的 DNS 解析器发送 83 个特定域名的 DNS 查询, 并跟踪解析器的响应随时间和空间的变化, 揭示了评估 DNS 过滤机制的影响应考虑 3 个因素: DNS 解析程序、客户端位置和阻止域. 文献 [16] 测量发现防火墙在阻止用户访问 Twitter 和 Facebook 等网站的同时, 可能会因一些伪造的回复而受到附带损害. 文献 [17] 对 DNS 拦截进行了大规模的分析, 利用全球 14 8478 个住宅和蜂窝 IP 地址进行分析, 在检查的 3047 个 AS 中, 有 259 个 (8.5%) 表现出 DNS 拦截行为, 此外, 发现拦截请求的 AS 的 DNS 服务器可能使用过时的易受攻击软件.

对递归服务器的测量: Gao 等人[7,8]通过分析从 SIE[9]采集的全球几百个递归服务器解析数据, 发现尽管 DNS 流量的特征在不同网络中差异很大, 但组织内的解析器往往表现出类似的行为, 进一步测量发现向根服务器发出的 DNS 查询中有 50% 以上没有返回成功的应答, 并且根服务器查找失败的主要原因是具有无效顶级域的格式错误的查询. 文献 [11] 从客户端测量递归服务器的部署情况, 通过推出了两个独立的广告活动, 引发了超过 3M 次 DNS 查找, 识别和研究超过 7600 个递归 DNS 解析器, 为 178 个国家的 25000 多个 AS 提供支持, 发现用户对第三方 DNS 提供商的偏好, 比如, Google、OpenDNS、Level3 和 Cloudfare 提供的递归解析服务就占 DNS 请求总数的 13%.

其他测量: 文献 [13] 对 DoE 进行了第 1 次端到端的大规模分析, 通过从互联网扫描、用户端测量和被动监控日志中收集数据, 发现 DoE 服务质量在可访问性和延迟方面是令人满意的, 对于 DNS 客户端, 与传统 DNS 相比, DoE 查询不太可能被路径内拦截破坏, 然而, 该文献发现 25% 的 DoE 服务提供商使用无效的 SSL 证书, 与传统的 DNS 相比, DoE 虽然有上升趋势, 但实际用户要少得多. 文献 [21] 通过测量俄乌战争前后俄罗斯互联网基础设施服务, 特别是 DNS 服务和证书服务在战争前后的变化情况, 发现在战争后部分机构对俄出现域名和证书服务的限制, 引发互联网主权的担忧. 文献 [22] 提出了一种轻量级的主动数据收集方法, 目的是在网络靶场上进行 DNS 模拟, 所提出的收集方法可以在短时间内收集 DNS 数据, 并以较低的存储成本存储收集的数据. 文献 [23,24] 收集了互联网上主要顶级域下所有域的每日 DNS 测量结果 (包括.com、.net 和.org, 占全球 DNS 名称空间的 50%), 提出了一种大数据分布式收集和存储方案, 解决了扩展日常测量以收集最大 TLD (.com, 拥有 123M 个名称) 的数据, 并确保这种规模的测量不会给全球 DNS 基础设施带来不可接受的负担. 而对于 DoH, 文献 [25] 表明, 尽管 DoH (DNS over HTTPS) 和 DoT (DNS over TLS) 等加密 DNS 协议旨在提升隐私保护, 但在实际应用中, 由于受到握手时延、底层传输协议和加密协议的束缚, 其性能可能不如预期. 此外, 还有一些研究专注于评估 DNS over QUIC (DoQ) 的性能表现. 例如, 文献 [26] 中通过代理网络在全球范围内部署了超过两万个客户端进行测量, 以比较 DoH 和传统 DNS 的性能差异. 文献表明, 尽管 DoH 在某些场景下可以提供性能优势, 但全球范围内仍有相当一部分客户端在使用 DoH 时经历了性能下降. 文献 [27] 则进一步深入, 从基础设施的角度探讨了 DNS 的集中化问

题. 研究指出, DNS 基础设施呈现出比以往认知更为集中的趋势, 超过 90% 的转发解析器最终由少数几个大型 DNS 服务提供商支撑, 这引发了对潜在单点故障和服务可靠性的担忧.

关于 DNS 系统的测量工作还有很多, 文献 [28] 从组件、结构、流量、安全这 4 个方面对 DNS 测量研究工作进行了综述, 有兴趣的读者可以具体参见文献 [28], 本文主要对紧密相关的一些文献的工作做了简要描述. 从目前对 DNS 递归服务器测量的相关工作中可以看到, 现有研究对递归服务器的测量主要集中在递归服务器的流量特征研究和递归服务器的部署情况等方面, 目前仍缺乏从一个大型 DNS 运营商的角度来分析 DNS 运行情况, 本文通过对大型 DNS 服务商的递归服务器的流量测量与分析, 弥补现有工作的不足.

2 DNS 数据

分析一个大的服务商的 DNS 数据不是一件容易的事情, 一方面的原因是, 大的服务商的 DNS 数据量非常大, 我们分析的 DNS 服务商递归服务器平均请求量日均约 37 亿条, 平均解析量日均约 36 亿条. 在 DNS 服务商提供的 DNS 数据中, 每天的 DNS 请求和应答流量都以 1 min 为一个 PCAP 源文件进行存储, 这样每天的 DNS 请求和应答流量的源文件就各有 1 440 个, 每个 DNS 请求源文件大小根据时段的请求量不同大约在 100M–500M 之间, 每个 DNS 应答源文件大小根据不同时段大约在 200M–1 200M 之间, DNS 服务商每天的 DNS 数据量都在 TB 级别, 本文分析的数据时段在 2022 年 2 月 19 日–3 月 30 日之间, 大约跨越了一个多月的数据, 如何建立有效的测量分析方案对如此巨大的数据来进行行之有效的分析是面临的巨大挑战.

另外一个方面, 服务商为了保护具体用户的隐私信息, 不能公开每个 DNS 请求客户端的 IP 地址, 所有的 DNS 请求他们都用特定 3 个转发节点的 IP 地址 (221.130.199.19、112.65.210.190、1.192.136.235) 对 DNS 用户请求地址进行了替换, 这样就无法分析具体用户的请求情况, 为了达到分析目标, 他们在请求流量中通过符合 RFC7871 标准的 EDNS subnet 扩展携带用户的 IP 地址的 /24 子网地址, 具体如图 1 所示.

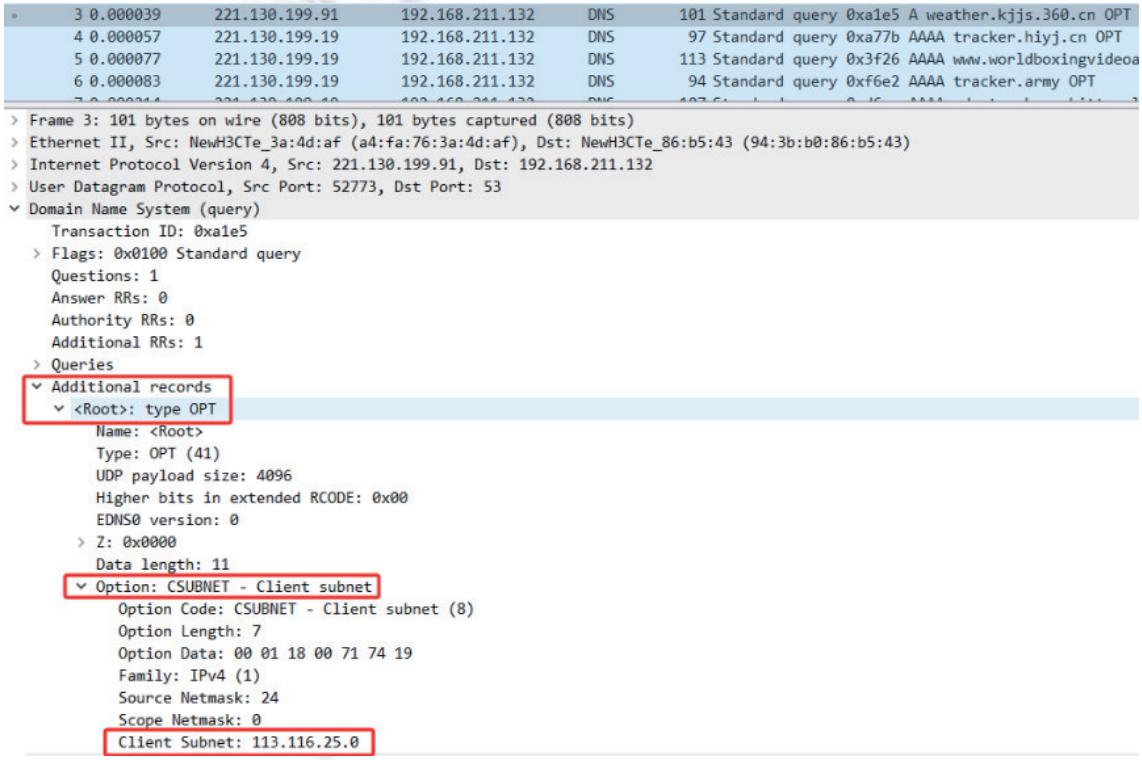

图 1 DNS 请求携带标准 EDNS 扩展 (包含客户端 IP 地址的/24 子网掩码)

3 测量分析方案

对于 DNS 服务商提供的如此庞大的数据量, 如何进行有效的测量分析是本文首先要解决的问题. 测量需要实现周期数据存储不遗漏, 数据不重算, 不少算; 每天汇总数据存储不遗漏, 累加数据不重算, 不少算; 并且在常态下, 分析速度接近留存速度, 平均滞后在 30 min 以内; 同时, 保证分析程序状态和存储数据程序状态可被持续监控.

3.1 多机分布式并行测量机制

数据的分析目标是一系列大量的包括 DNS 报文的 PCAP 压缩文件, 需要对这些文件的内容进行快速有效的读取和分析. 测试发现, 使用 Python 直接读一个 PCAP 压缩包耗时 120 s 以上, 而先解压缩再读包时间超过 50 s, 主要原因是直接读 PCAP 压缩包实际是在内存中解压输出文件流, 支持在内存中读压缩包的组件是 Python 内置的, 性能比较差, 而通过执行 Linux 系统的 tar 命令解压, 采用 C 语言实现, 性能较好, 所以采用先解压再读方式读取 PCAP.

但是, 对于这些文件, 需要考虑在一台机器中用一个线程一次读取一个文件, 还是用多个线程并行读取多个文件, 哪种方式读取效率更高的问题. 表 1 是具体的测试数据, 按照正常推算, 在一台机器上单线程顺序读取两个文件时间为 110 s, 小于表 1 中单台机器两个线程读取两个文件的时间 141 s, 在单台机器单线程顺序读取 5 个文件的时间为 275 s, 远小于在单台机器上启动 5 个线程读取同样 5 个文件的时间, 对于更多的线程通过进一步测试, 并没有单线程处理文件效率更高. 可能的原因在于线程在使用多个内核或处理器的 CPU 密集型任务上获得更好的性能, 但文件读取不是 CPU 密集型任务, 磁盘 IO 是大文件读取的主要性能瓶颈, 使用多线程对文件读取还额外需要进行互斥锁的竞争, 反而降低了效率. 因此, 采用单线程的方式具有更加快速的读取效率.

但是, 由于要处理的文件量比较大, 采用分布式多机的处理方式, 需要把文件及时分发到不同机器上进行并行处理, 具体分发 PCAP 的逻辑如图 2 所示. 主要机制是当解析文件速度不落后留存文件太多时 (≤3 个文件) 时, 只让本机分发节点处理, 减少跨节点传输文件带来的时间消耗. 采用此分发机制的主要因素是 PCAP 文件较大, 特别是应答报文要远大于请求报文, 传输的网络带宽有限, 而过于频繁的文件分发会降低文件的读取效率, 经过测试, 留存 3 个文件以内只在本机分发可以获得较好的文件处理效率. 后续, 对于文件的分发过程可以进行进一步的动态优化, 对于较大的文件留存更少, 而较小的文件留存量增加, 同时增加网络状态参数进行控制.

表 1 不同线程读取时间的对比

线程数	耗时 (s)	读取的文件数
1	55	1
2	141	2
5	1 007	5
10	1 101	10
15	1 453	15

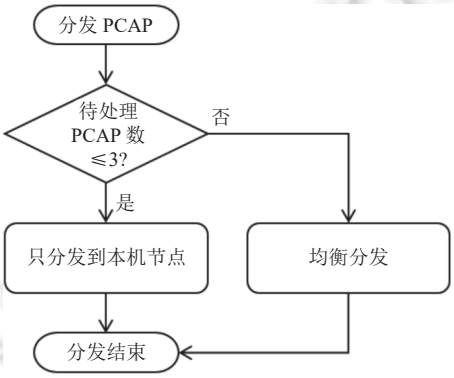

图 2 PCAP 压缩文件分发流程

这样, 一天 DNS 流量对应的 PCAP 压缩文件, 主要解析和分析流程如图 3 所示. 流程分为留存 PCAP 分发, 解析 IP 和分析 IP, 其中分发流程由留存文件所在机器执行, 并轮询被分发的机器获取 IP 列表文件, 被分发的机器包含多台, 每个机器启动解析 IP 的程序, 负责把分发的 PCAP 压缩包解析出 IP 文件; 分析 IP 程序也在 PCAP 留存机器执行, 负责分析 IP 的归属地和运营商等信息, 并做实时累加统计, 完成分析每天留存文件后再通过 Kafka 发送到一个分布式实时存储和搜索引擎 Elasticsearch 服务平台存储. 这样, 后续分析的所有特征和统计信息都进入 Elasticsearch 服务平台.

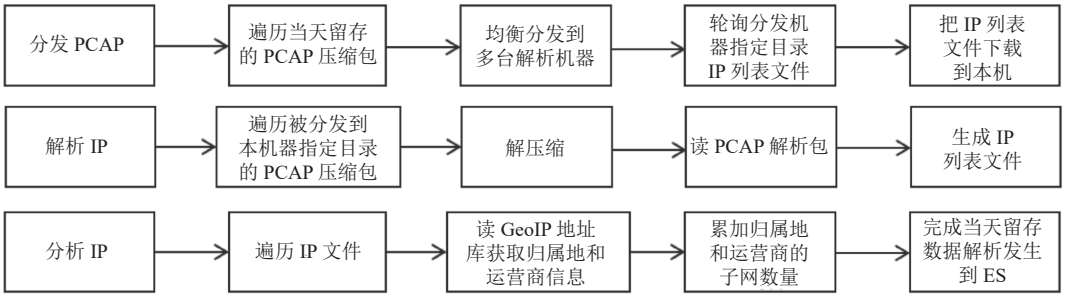

图 3　子网地址解析和分析流程

3.2　大数据平台存储和监控

子网分析输出的数据按时间维度划分为两类, 一类是当天的累加数据, 每小时输出一次, 后一次数据输出后覆盖前一次的存储记录; 一类是小周期内的汇总数据, 每周期输出一次, 每周期的数据输出后追加存储记录, 每周期间隔时长 20 min. 对于周期内的输出数据, 目前的子网分析是基于解析 PCAP 生成的 IP 列表文件. IP 列表文件和每分钟的 PCAP 文件一一对应, 每个文件处理时长不完全一样, 所以把每周期定义为处理每 20 个 PCAP 即每 20 个 IP 列表文件作为周期结束标志, 这样后续进行周期之间数据比较才会有意义. 由于系统解析 PCAP 采用分布式处理, 不是严格按照记录的时间顺序获得 IP 列表文件, 所以每 20 个文件的留存时间不一定顺序排列, 可能个别文件时间顺序会颠倒.

两类数据均通过 Kafka 消息输出, 大数据平台端通过消费 Kafka 消息存储记录. 其中累加数据, 在大数据平台端采用 Elasticsearch 存储, 便于对外提供实时查询. 每周期的汇总数据, 在大数据平台端采用离线文件系统存储, 后续分析时采用离线分析实现. 基于这样的大数据平台, 就非常便于分析和搜索所需要的结果.

大数据平台端实现了任务运行状态监控, 能及时发现任务终止, 同时实现了上传数据的消息堆积监控, 能及时发现上传数据处理阻塞. 程序在每个周期完成后, 向监控平台发送周期标识的数据, 监控平台如果在间隔半个小时内没有收到该数据则预警通知. 接收预警通知后, 到机器上排查进程状态和数据输出状态, 确认程序是否异常. 分析程序异常退出或升级后重启自动恢复, 对于当天重启的情况, 图 4 展示了分析程序接续之前的分析位置, 避免重新开始分析或者重复分析的情况.

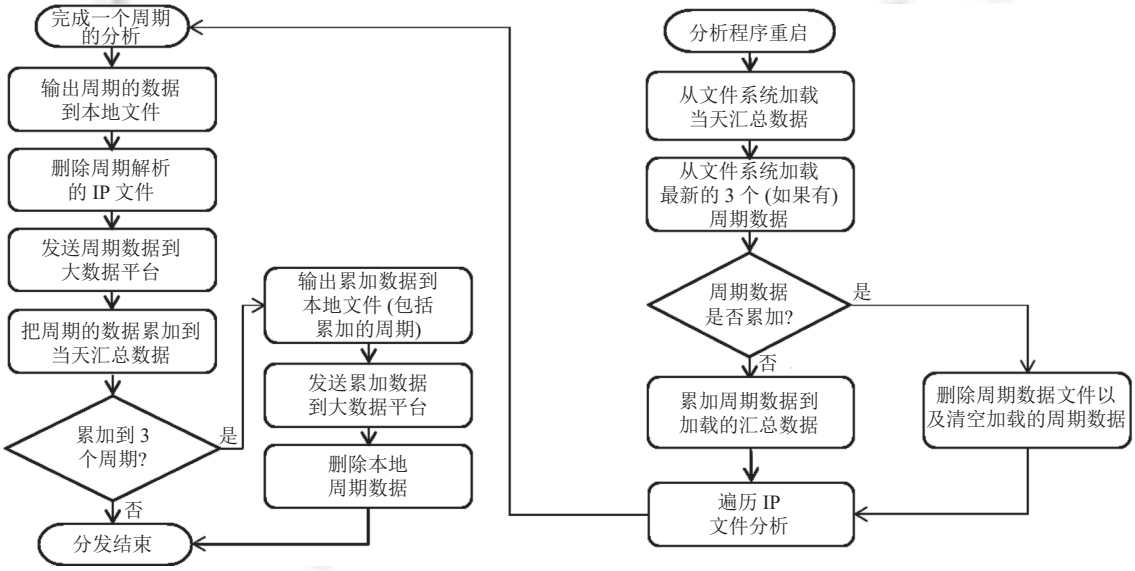

图 4　分析程序实现重启自动恢复流程

4 测量结果

在本节, 本文从不同的角度分析测量收集的 DNS 流量的特征.

4.1 用户解析请求规模与响应率

如图 5 所示, 在 2022 年 3 月 4 日前请求数图像波动明显, 而在之后就趋向平稳. 主要原因是自 2022 年 2 月 18 日–22 日为调试阶段, 只启用了一台转发服务器 (IP 地址为 221.130.199.19), 请求量日均约 12 亿条, 平均每秒约 1.4 万条. 2 月 22 日–3 月 4 日期间由于 DNS 服务器问题导致波动. 自 3 月 4 日起, 为正常平稳阶段, 请求量日均约 37.89 亿条, 平均每秒约 4.38 万条.

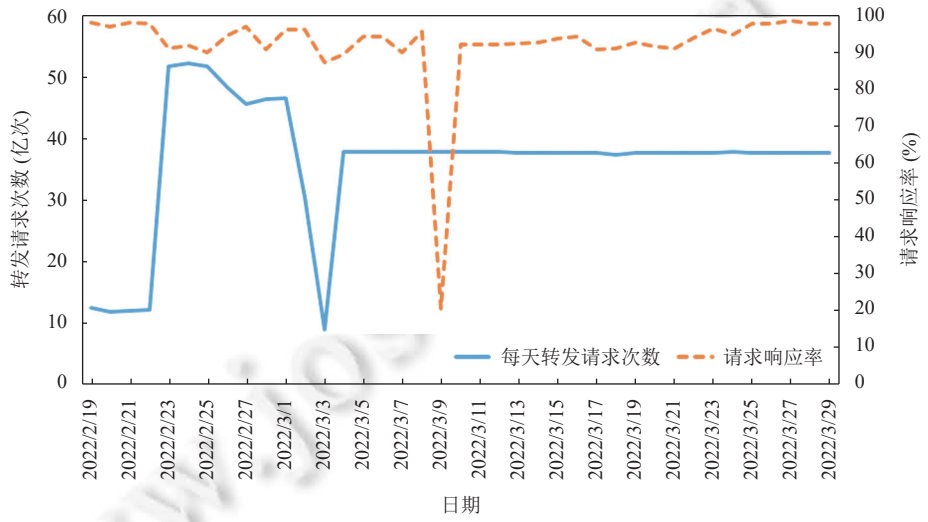

图 5 递归服务器收到的请求数与响应率

响应率是指在一段时间内响应数除以请求数, 响应数为从递归服务器返回给用户的报文数量. 从图 5 中可以看到, 绝大部分的响应率保持在 90% 以上, 但是在 2 月 9 日出现了较大的波动, 产生了较低的响应率. 起初推断是递归服务器遭受了比较大的攻击或是服务器进行升级造成的情况, 后面经过运行状态监控程序的排查发现, 是数据监控程序出现了 bug, 导致间歇的中断和重启, 经过当天的修复, 后续实现了连续稳定的数据监控.

根据 3 月 30 日数据统计, 递归服务器上的总请求数为 37.66 亿, 总响应数为 36.89 亿, 响应率为 97.96%. 从图 5 的数据中可以看到, DNS 服务商尽管面临着海量的用户请求, 绝大部分 (平均 95% 左右) 请求可以得到正常响应, 只有少量没得到响应的请求才需要数据重传. 响应率在一定程度上也反映了 DNS 服务商的服务质量.

4.2 请求的域名情况

图 6 显示了请求数量排名在前面 10 位的域名情况, 排在第 1 的“teredo.ipv6.microsoft.com” 请求量超过 6 亿次, 主要是用户通过微软的 Teredo 服务器隧道连接 IPv6; 排在第 2 的“stactic2.servyou.com.cn” 请求量将近 6 亿次, 主要是用户通过税务 APP 进行税务申报的访问流量. 排在第 3 的“jpupdate.jianpianupdate.com”来自应用程序“荐片”, 它的请求量将近达到 3 亿次. 接着分别是新浪、淘宝、京东、360 等国内大型网站或其相关应用软件引起的访问量比较靠前. 这个明显和国际上 Alexa 提供的排名前 10 的域名服务有很大差别, 只有百度在 Alexa 前 10 里面, 奇怪的是中国的“www.qq.com”排在 Alexa 前 10 中, 而没在此国内大型 DNS 服务商排名前 10 的域名列表中, 这说明了全球域名的访问情况和以中国网民为主的国内服务商的访问情况并不尽相同.

图 7 显示了各个顶级域名的访问占比情况, 用户请求流量总共覆盖了 1 167 个顶级域, 其中 Top10 顶级域名包括: COM、CN、NET、ORG、XYZ、RU、ME、CO、TV、IE. 这个数据也和全球 10 大顶级域名访问总量的排名有所不同, 目前全球 10 大顶级域名总量的排名为: COM、CN、DE、NET、UK、ORG、NL、RU、BR、

XYZ. 这 10 大顶级域中排名第 3 的德国国家顶级域 DE 和英国国家顶级域 UK, 及排名第 7 的荷兰国家顶级域 NL 和排名第 9 的巴西国家顶级域的访问量没有出现在以中国网民为主的前 10 大访问中, 而黑山共和国国家域名 ME, 哥伦比亚共和国国家域名 CO, 图瓦卢国家域名 TV, 及爱尔兰的国家顶级域 IE 则分列第 6–10 位, 这与国内 DNS 服务商中国用户的访问偏好有关, 不能代表全球用户的访问情况.

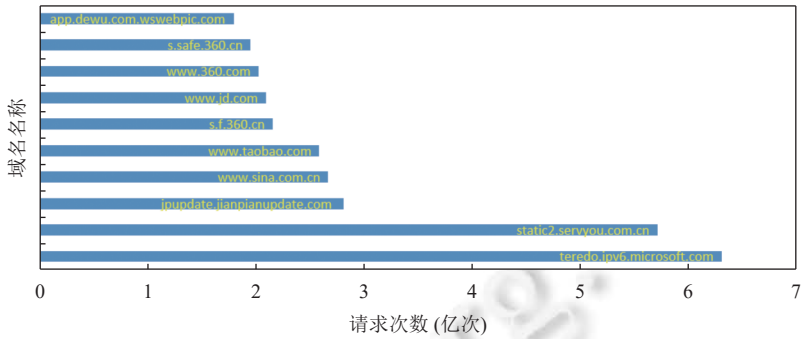

图 6 Top10 用户请求域名规模

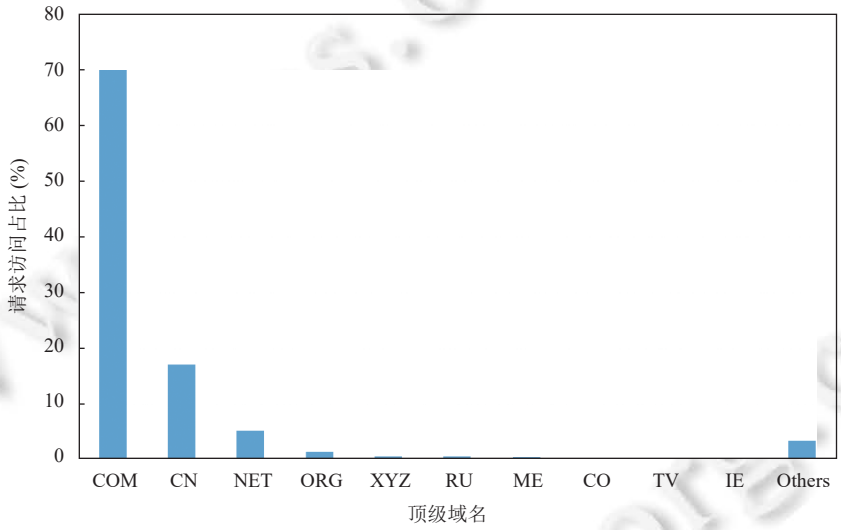

图 7 各个顶级域名请求访问占比

本文进一步测量分析了前面 1 万个二级域名在请求域名总量的占比情况, 如图 8 所示. 排名前 1 000 的二级域名占总请求域名的 93%, 然后依次上升, 基本是越靠前上升趋势越快, 在前 2 000 处出现一个拐点, 后面上升稍微趋缓, 到前 9000 处后基本比较平缓, 上升较慢. 这个结果具有一定的实用价值, 由于平时用户请求的二级域名访问量前 1 000 的占到 93%, 因此, 一些 DNS 服务商可以选用访问量靠前的二级域名作为 DNS 缓存服务器的缓存, 具体的选取量可以根据缓存大小以及上升的拐点位置进行平衡.

图 9 显示了按照不同访问解析类型的域名访问情况. 其中包含 A、MX、AAAA、PTR、DS、CNAME、NS、NAPTR、SOA、RRSIG 共 10 种解析类型, 具体含义如表 2 所示.

从图 9 可以看到, 用户的绝大部分请求是请求域名的 IP 地址, 包括 IPv4 和 IPv6 地址, 占总请求数的 99.5% 以上. A 记录在所有记录中占主导地位, 这和文献 [8,9] 的测量结果一致. AAAA 记录相对于文献 [8,9] 的测量结果明显攀升, 一定程度说明了近些年 IPv6 在我国逐渐呈现较快的部署和应用. 相比于 A/AAAA 记录, 其他记录相对于文献 [8,9] 的测量结果都占比明显较少.

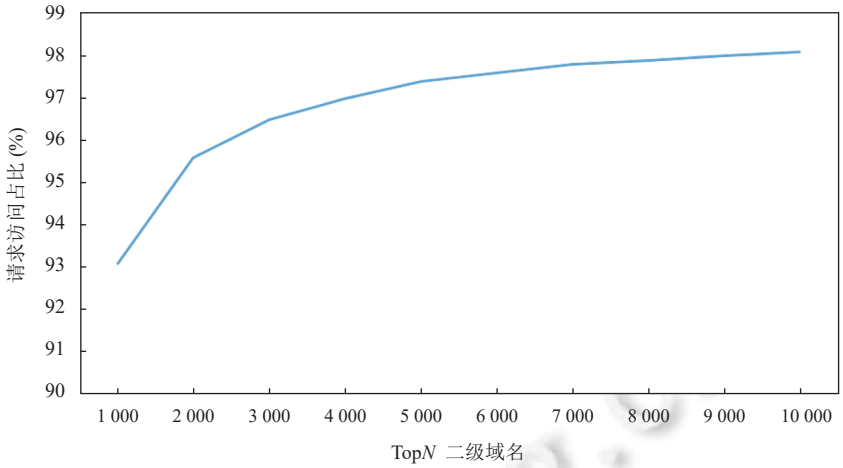

图 8 TopN 二级域名请求访问占比

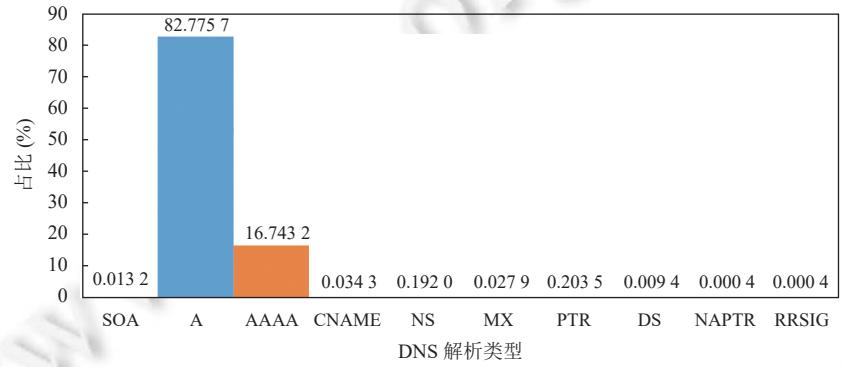

图 9 各个解析类型访问占比

表 2 不同解析类型含义说明

解析类型	含义说明
A	将域名指向一个IPv4地址
CNAME	别名记录, 将域名指向一个域名, 实现与被指向域名相同的访问效果
AAAA	将域名指向一个IPv6地址
MX	建立电子邮箱服务, 将域名指向邮件服务器地址
NAPTR	名称权威指针, 提供了正则表达式方式去映射一个域名, 它是一种用于电话号码解析和转换的DNS记录类型, 通常用于ENUM (电话号码与互联网名称对应) 系统
NS	域名服务器记录, 全称为name server, 用于指定域名由哪个DNS服务器来进行解析
PTR	PTR记录是A记录的逆向记录, 又称为IP反查记录或指针记录, 负责将IP反向解析为域名
DS	DS记录用于验证 DNSSEC区域的子区域的真实性. 父区域上的DS记录包含子区域中KSK的哈希
SOA	起始授权机构记录, SOA记录用于在众多NS记录中哪一台是主服务器
RRSIG	RRSIG记录存储DNSSEC签名. 这些签名用于验证其他DNS记录的真实性和完整性

除了占比最大的 A/AAAA 记录外, 其次是 PTR 反向查询, 由 IP 地址对域名进行反向查询. 再其次是与 PTR 记录占比相差不大的 NS 记录, 用于指定域名由哪个权威服务器来进行解析, 实现域名的权威快速解析. 再者是 CNAME 记录, CNAME 记录的一个重要应用场景是 CDN 服务. 在使用 CDN 服务时, 服务商提供给用户的是一个 CNAME 地址, 而不是一个 IP 地址, 如果服务商需要将 IP 地址更换, 只需要更改自己的服务器设置, 而无需通

知所有使用该 CDN 服务的用户更改域名对应的 IP 地址, 因此可以实现 IP 地址的透明更换.

图 9 中显示其他 DNS 记录占比很小, 比如用于管理域名区域的 SOA 记录, 用于邮件服务的 MX 记录, 用于电话号码到 IP 地址或其他标识符的转换的 NAPTR 记录, 这些特殊用途的 DNS 记录占比很小. 同时, 图 9 中和 DNSSEC 记录相关的用于存放 DNSSEC 公钥散列值的 DS 记录, 及用于存放域名 DNSSEC 签名的 RRSIG 记录占比也很小. 在一定程度上反映了 DNSSEC 在中国用户使用中的比例较少, 和 DNSSEC 相关的记录与文献 [8,9] 中的测量结果相比明显较小, 一定程度上也说明了中国相对国际上部署和应用 DNSSEC 的用户量较小.

4.3 请求的用户情况

图 10 显示了每天用户所在子网数量的变化情况, 用户的 IPv4/24 子网数量在 50–55 万间浮动, 日均约 52 万, 基本没有很突兀的变化. 在连续的两天中, 用户上网也具有一定的连续性, 经统计, 相邻两日用户子网地址重合率约 94.22%. 可以利用这个数据监测子网变动的异常情况, 如果这个数据发生突变, 可能预示着那天的用户访问规模可能出现了异常的情况, 也有可能预示那天出现热点事件. 比如在 3 月 15 日, 尽管突变不明显, 但是子网数量增加还是比较多, 可能与当天发生的热点事件相关.

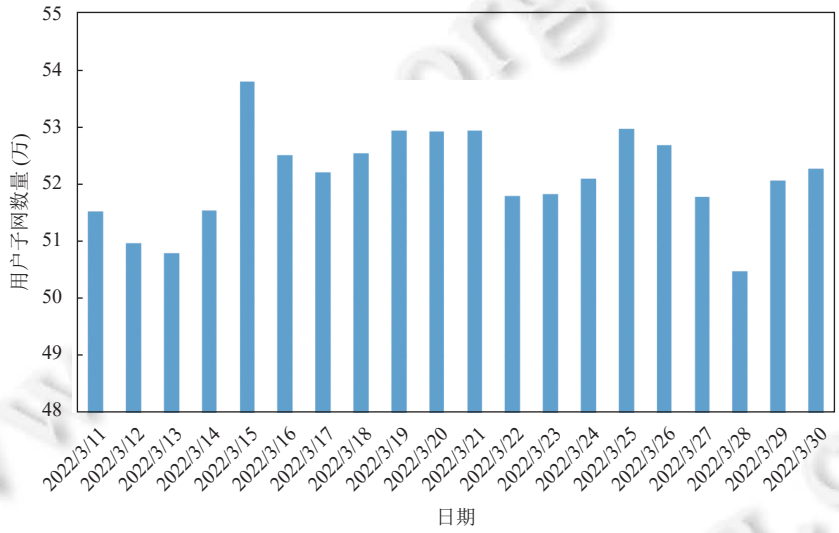

图 10 每天用户所在子网的数量

图 11 显示了用户子网所在国家前 10 名的统计分布. 中国的子网数量排名第 1, 子网规模达 70 万以上, 远超过其他国家, 这也是可以预料的合理结果. 其他国家的子网规模都低于 1 000, 其中美国最多, 一定程度上说明美国华人相比其他国家使用国内 DNS 服务商访问居多. 较难想象一个外国人会通过国内 DNS 服务进行访问. 经统计, 用户子网地址覆盖全球 213 个国家和地区, 用户子网地址归属于全球 220 个运营商, 国外这样的用户应用子网规模也一定程度上说明了中国大型 DNS 服务商的跨国服务能力.

图 12 显示了用户子网在我国省份及地区的分布. 用户子网地址覆盖我国所有省份和地区, 其中山东省、广东省、江苏省、河南省、辽宁省、四川省、河北省、浙江省、北京市、湖南省分列前 10. 这个排名在一定程度上揭示了各个省份和地区的用户使用国内 DNS 服务商上网情况, 但不绝对, 由于 DNS 流量中用户具体 IP 地址是提供的子网掩码, 无法统计各个省内的具体用户情况. 但可以推断, 用户子网各个省份的排名并不能完全代表各个省用户量的排名, 有些省可能一个子网内的用户量很大, 存在较大子网的情况, 而有些地区可能存在子网内的用户量比较少.

图 13 显示了用户子网所在的前 10 个运营商分布. 经统计, 用户子网地址归属于全球 220 个运营商, 数量 Top10 运营商包括: 电信、联通、移动、鹏博士、教育网、阿里云、JIO (印度运营商)、墨西哥电信、西班牙电信、康卡斯特 (美国运营商). 每天平均约 500 个子网地址属于私有 IP 地址范围, 包括来自运营商内部网络的域名

解析请求. 中国 3 大运营商排在前 3, 但中国第 1 大运营商中国移动的子网数量远比其他两家还要少, 是比较意外的情况. 一方面可能说明中国移动的用户使用此 DNS 服务商相对较少, 另一方面也有可能中国移动存在较大的子网, 即子网内的用户数量较多.

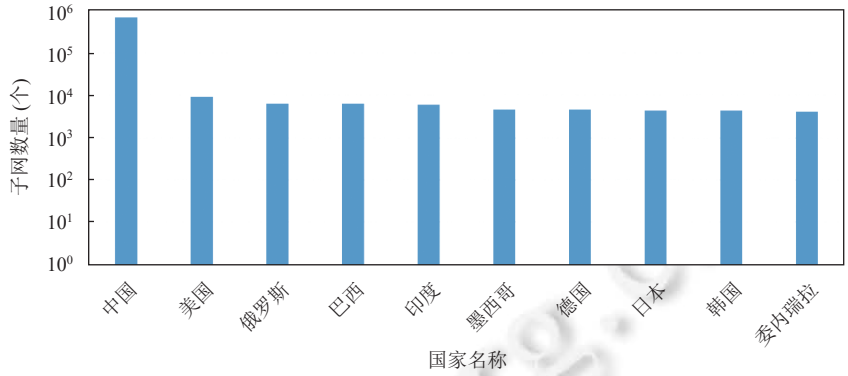

图 11 用户子网所在国家分布前 10 名

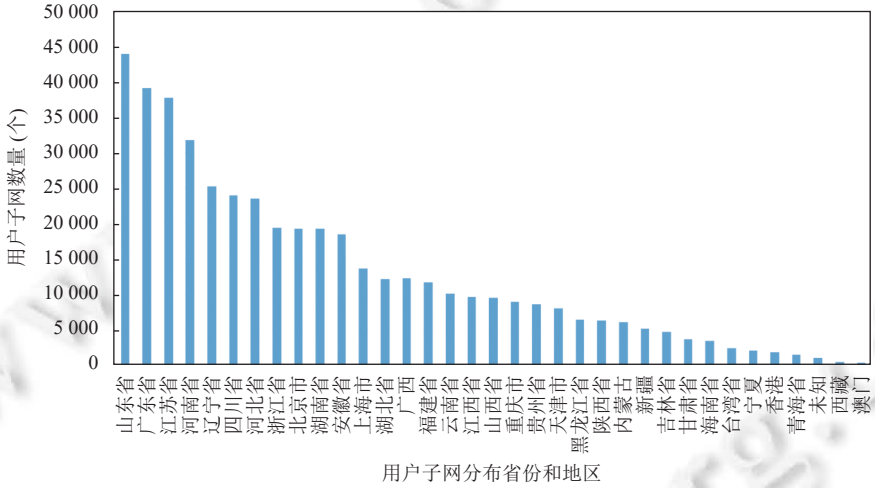

图 12 用户子网在我国省份和地区的分布

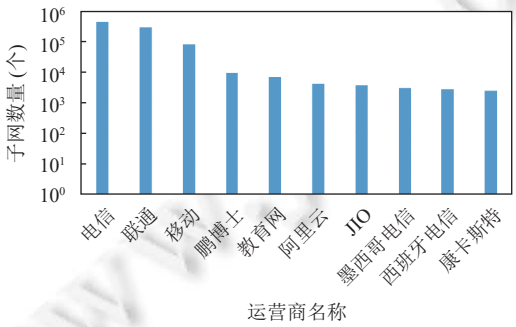

图 13 用户子网所在的前 10 个运营商分布

4.4 域名解析情况

图 14 显示了 DNS 递归服务器的解析成功率. 解析成功率是指在一段时间内解析成功的响应数除以总的响应

数, 其中解析成功的响应状态为 NOERROR、NXDOMAIN, 解析失败的响应状态为 SERVFAIL、REFUSED. NOERROR 意思是成功的响应, 即这个域名可以正常解析成需要的类型; NXDOMAIN 意思是不存在的记录, 也就是这个被解析的域名在权威服务器中并不存在; SERVFAIL 意思是服务器失败, 也就是这个域名的权威服务器拒绝响应或者响应拒绝; REFUSED 意思是拒绝, 也就是这个请求源 IP 不在服务的范围内.

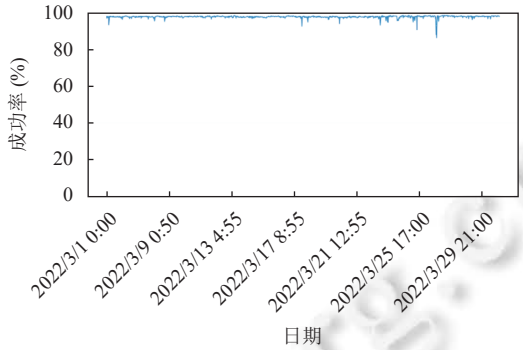

图 14 递归服务器解析成功率

通过分析解析失败的记录, 发现基本上是因为 SERVFAIL 的响应状态引起, SERVFAIL 的响应状态分 3 种情况: 1) 递归服务器至权威服务器中间的网络存在异常, 递归服务器在发出递归请求并完成重试超时后, 给请求源一个 SERVFAIL 的应答; 2) 权威服务器向递归服务器应答 REFUSED, 即当权威服务器不存在主域名及对应的 SOA 记录时, 权威会向递归服务器返回 REFUSED, 即不在我服务的范围内, 递归服务器在收到这个 REFUSED 应答后, 给请求源一个 SERVFAIL 的应答; 3) 当权威服务器存在主域名但是由于区文件被破坏导致权威域上的 NS 记录异常时, 权威服务器会向递归服务器返回 SERVFAIL 即解析失败, 递归服务器收到 SERVFAIL 应答后, 给请求源即客户端一个 SERVFAIL 的应答.

表 3 统计了对于不同 DNS 记录的各种应答结果的占比情况. 其中 NOERROR 代表可以解析到正常的结果, NXDOMAIN 表示用户请求的域名有误, 可能是用户的误操作等原因导致的, 这两种情况都代表域名解析成功的情况, 占用户请求总数的 97.4% 以上. 解析成功率较高的记录依次为: NAPTR、A、AAAA, 达到 95% 以上, 而 A/AAAA 记录从图 9 中可以看到是用户请求的主要记录. 表 3 显示, 除了 RRSIG 记录, 其他记录的解析成功率都在 90% 以上. RRSIG 记录解析成功率低也一定程度上说明了很多 DNSSEC 签名无法进行验证, 侧面反映了 DNSSEC 在实际部署应用中存在的问题.

表 3 不同 DNS 记录应答结果占比 (%)

解析类型	NOERROR	SERVFAIL	NXDOMAIN	REFUSED
SOA	57.565 094 3	8.006 960 5	34.427 945 2	0
A	77.542 446 4	1.889 964 4	20.567 589 3	0
AAAA	81.264 067 6	4.073 141 9	14.662 790 5	0
CNAME	76.510 577 8	15.606 644 9	7.882 777 2	0
NS	83.070 125	16.589 95	0.339 925	0
MX	65.526 94	20.786 455 3	13.686 604 7	0
PTR	30.142 166 7	19.622 610 8	50.235 222 5	0
NAPTR	99.058 650 7	0.791 154 4	0.150 195	0
DS	89.913 667 7	8.210 131 2	1.876 201 2	0
RRSIG	51.811 373 9	48.073 756 4	0.114 869 6	0
全部记录	79.412	2.503 4	18.083 2	0

表 3 中也可以看到, 导致用户解析失败的原因主要由 SERVFAIL 造成, 很少出现服务器拒绝服务的情况. 经对递归服务向根和权威服务器的迭代查询应答结果统计, 绝大部分的 SERVFAIL 的应答出自第 1 种情况, 即来源

于递归服务器到上级权威服务器的正常丢包. 总体来讲, 针对用户域名请求, 递归服务器的解析成功率约为 97.5%, 这个值是比较高的, 充分说明了 DNS 服务器的高可用性和高可靠性.

递归服务器在进行递归解析前先由缓存服务的历史解析记录进行解析, 如果到来的 DNS 请求有对应的缓存记录, 则直接向用户返回缓存中的解析记录, 图 15 为缓存服务器在测试期间的缓存命中率. 如图 15 所示, 针对用户域名请求, 缓存服务器的总缓存命中率约 94.59%, 这个缓存命中率比较高, 说明绝大部分的请求会在递归服务的本地缓存进行解析, 缓存的高命中率大大增强了 DNS 请求的解析效率.

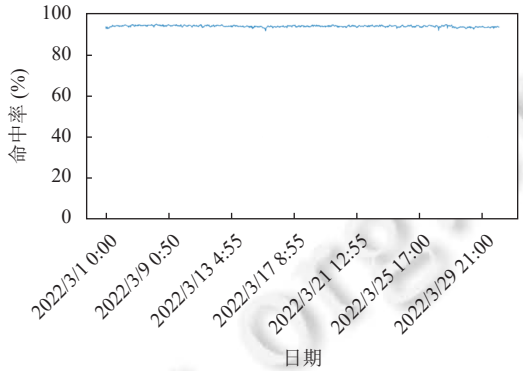

图 15 缓存命中率

递归服务器收到用户的 DNS 查询请求后, 如图 15 所示, 绝大部分在本地缓存完成解析并向用户返回应答结果, 少部分未命中的 DNS 请求则需要从根服务器进行迭代查询. 图 16 显示了递归服务器向根服务器的迭代请求次数, 递归服务器向根服务器发送解析请求日均 691 万条, 平均每秒约 80 条, 平均约 548 条用户请求会触发一条递归服务器到根服务器的请求, 覆盖 1 168 个顶级域.

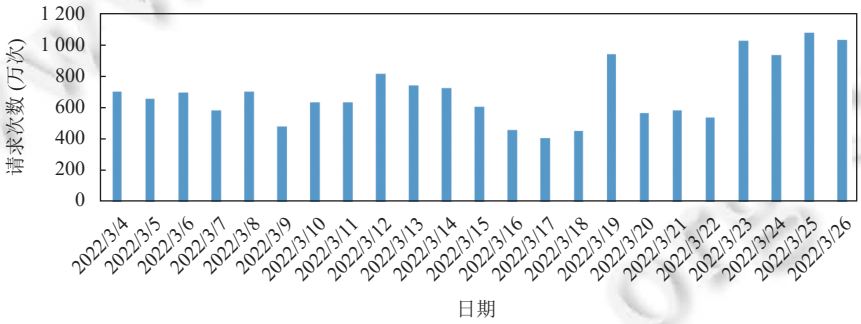

图 16 递归服务器向根服务器的迭代请求次数

递归服务器向上对根服务器进行迭代查询时, 由于根服务器拒绝响应, 线路丢包等问题, 递归服务器也无法得到每个请求的应答. 后文图 17 显示了递归服务器向根服务器每日请求的平均响应率, 总的平均响应率约 81.78%, 这个响应率比预想的要低很多, 可能的原因是递归服务器距离根服务器较远. 基于此, 本文建议运营商采用 RFC8806 提出的本地根策略, 通过直接在递归服务器上设置根区镜像, 将根区文件设置在本地使用, 从而避免从根服务器的迭代查询.

递归服务器向根服务器进行迭代查询时, 请求报文发出到对应的应答报文返回为这个 DNS 请求报文的时延. 每天所有报文的时延的平均值为这天报文的平均时延, 后文图 18 显示了递归服务器向根服务器的请求应答的平均时延. 最小在 40 ms 左右, 最大在 80 ms 左右, 基本相差一倍. 总的平均请求响应时延为 58.81 ms, 这个时间体现了根服务器对递归服务器的服务效率.

4.5 大型 DNS 运营商异常检测探索

学术界目前已经提出很多利用 DNS 流量进行异常检测的方法, 比较著名和典型的有: Notos[29]、Exposure[30]、

FluxBuster[31]、ExecScent[32]、Segugio[33]、DNSMap[34]、BotGAD[35,36]、BotDAD[37]等, 这些方法都涉及深度报文检测. 利用 DNS 报文进行检测必须对 DNS 报文完成解包, 无法像网络流量通过流技术快速统计流特征进行检测, DNS 报文检测方法都是通过对报文进行解析后然后统计特征, 再利用模型或其他技术进行检测. 从表 1 中得知, 对于 DNS 大型运营商, 1 min 的流量解析时间都要将近 1 min, 而且多线程并不能提高解析效率, 因此, 目前已有的 DNS 流量检测技术难以满足大型运营商实时在线的检测需求. 通过 DNSMap[34]和 BotDAD[37] 方法对我们分析的 DNS 流量进行了测试, 其检测效率无法在大型运营商上进行在线部署应用.

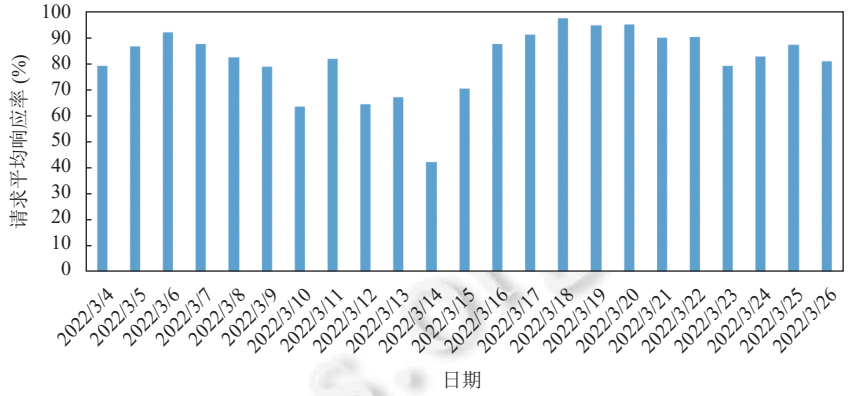

图 17 递归服务器向根服务器的请求平均响应率

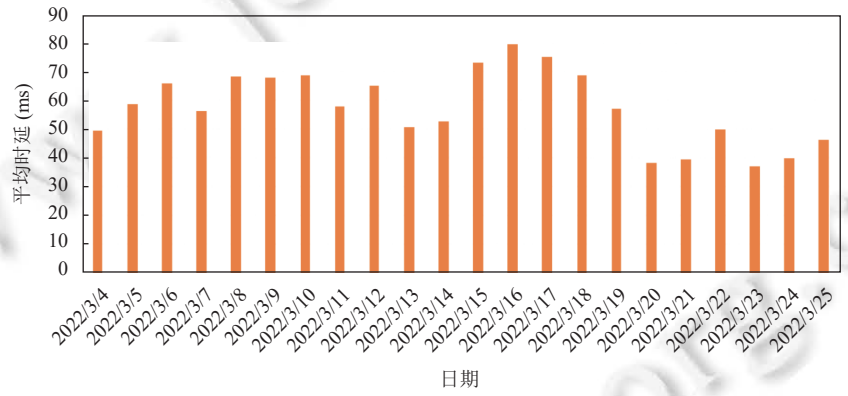

图 18 递归服务器向根服务器的请求应答的平均时延

因此, 需要探索未来在大型 DNS 服务商中的检测方案. 如图 19 所示, 通常对 DNS 流量检测是在递归服务器到用户侧的端口流量上进行检测, 但在大型服务商中这个端口流量太大, 解包时间太长, 无法达到实时在线的检测目标. 根据缓存命中率的测量结果 (图 15), 绝大部分的解析在递归服务器的缓存完成, 递归服务器向权威侧的迭代查询流量只占用户侧流量的很少一部分. 因此, 最有效的提高检测效率的思路是将异常检测从递归服务器用户侧端口转移到权威侧端口.

但如果只用权威侧端口流量进行检测, 只能检测到这部分流量的异常情况, 没有检测缓存中具体记录, 并不能反映整个用户的异常情况. 由于缓存没有区分正常和异常记录的能力, 它只留存记录, 因此缓存中的解析记录本身可能存在异常的情况, 比如缓存污染等, 递归服务器会将缓存中异常的解析结果向客户应答, 导致解析异常. 探索的思路是, 能否找到一种替代缓存的应答技术, 使得绝大部分流量在递归服务本地解析, 同时该技术可以区分正常和异常记录, 只将正常的解析记录向客户应答, 阻断异常的记录, 这样就可以实现在权威侧端口进行检测, 不仅大大提高了检测效率, 而且具有恶意域名阻断能力.

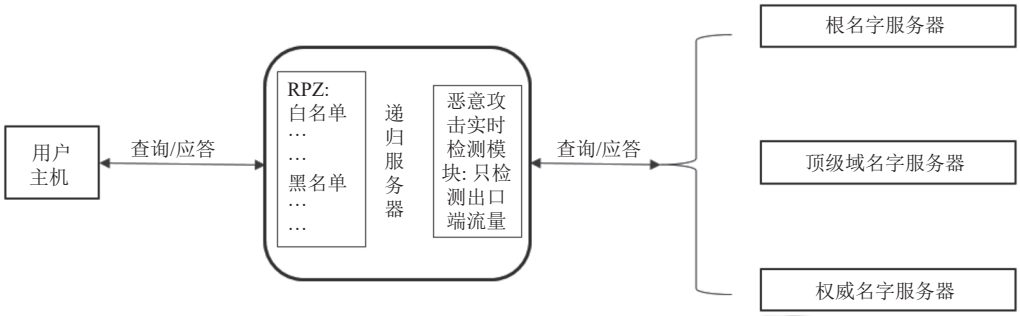

图 19 大型 DNS 服务商检测框架方案

沿此思路, 将前面一段历史 DNS 流量通过已有的异常检测方法如 DNSMap[34]等把记录分成正常和异常两个部分, 那些不确定的去除掉, 带有正常和异常标记的记录写入递归服务器, 解析器通过一种机制优先处理用户请求, 匹配到正常的部分直接应答, 异常的部分应答 NXDOMAIN 或者一个警告网站 (实现阻断功能), 未能匹配的请求将经由权威侧端口进行迭代查询, 这样就可以在权威侧部署传统的异常检测方法进行检测, 异常检测方法将检测到的异常和正常记录进一步更新到递归服务器中. 这样就实现了从递归器用户侧端口转移到权威侧端口的检测, 极大地减少了待检测的流量, 使得大型服务商的实时检测成为可能.

这种机制本文称为域名黑白名单机制, 具体使用响应策略区域 (response policy zone, RPZ) 技术实现. RPZ 由 ISC 首度发明并在 BIND 中实现, 它是一个开放的厂商中立的标准, 用于交互 DNS 防火墙配置信息, 它是配置在一种特殊的 DNS 区文件中的 DNS 防火墙策略, 目前大部分 DNS 服务软件都具有 RPZ 功能. RPZ 为 DNS 服务器提供一种应答拦截机制, 匹配过滤特定的域名或 IP, 改变应答结果. RPZ 通过 RPZ 区文件设置记录拦截规则, 规则包括匹配条件和执行相应的干预动作. 通过 RPZ 机制实现内网解析, 匹配到的域名直接由 RPZ 本地返回.

本文应用 RPZ 实现黑白名单机制, 创建 RPZ 区域以存储域名黑白名单, 白名单部分存储正常解析记录, 黑名单部分存储恶意域名记录, 用户请求首先与递归服务器中的 RPZ 区域存储的记录进行匹配, 匹配到的记录直接向用户返回, 包括通过白名单返回正常解析记录, 和通过黑名单对恶意域名阻断或者转到一个提示网站, 具体使用 BIND 中的 RPZ 区域配置进行说明, 如下所示.

```
zone "rpz" {
type master;
file "/etc/bind/rpz.zone";
allow-query any; ;
allow-transfer localhost; ;
};
rpz.zone 文件配置如下:
;whitelist part
www.hit.edu.cn A 32.23.32.34
A 23.4.45.6
nextcloud.your-domain.com A 192.168.0.103
www.facebook.com A 23.23.232.2
…
;blacklist part
malicious1.org CNAME .
*.malicious1.org CNAME .
malicious2.org CNAME .
```

```
www.malicious.net. CNAME drop.garden.example.com.
drop.garden.example.com. A 192.168.7.89
…
```

未匹配到 RPZ 区文件中的用户请求将进一步向权威服务器进行迭代查询, 在递归服务器权威侧端口部署检测系统对这部分流量进行检测, 并依据检测结果更新 RPZ 区文件记录的黑白名单. 此方案实现了在权威侧端口实施检测的目标, 待检测的流量极大下降. 权威侧端口流量的具体检测方法可以使用文献 [29−37] 任何一种方法进行, 将检测后正常的记录更新进白名单, 恶意记录更新进黑名单. 目前我们开发了一个自动化程序, 可以完成将 DNS 历史解析记录自动写入 RPZ 区文件, 由 RPZ 实现黑白名单机制, 对用户请求实时应答的能力, 并初步验证了该机制的正确性和可行性.

通过使用 DNS 流量测试了 RPZ 区文件的命中率, 如图 20 所示. 对于当前分钟的 DNS 请求, 如果保留其前 1 min 的 DNS 解析记录, 则命中率约为 55%, 如果保留其前 2 min 的 DNS 解析记录, 命中率约为 60%, 命中率随着保留更多的 DNS 记录而不断增加. 如果保留其前 1 h 的 DNS 记录, 则命中率达到 88%. 也就是说, 如果将前 1 h DNS 请求的历史解析结果记录在 RPZ 区文件中, 递归服务器只需要向权威侧服务器发送大约占用户总请求流量的 12%, 而在递归服务器权威侧端口也只要检测总流量的 12%, 将会大大地提高检测效率.

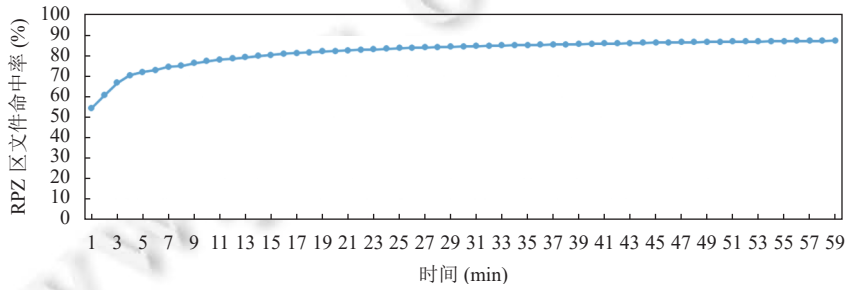

图 20 RPZ 区文件的命中率

5 总 结

本文从一个大型 DNS 运营商的角度测量分析了用户域名的访问模式及解析状况, 针对大型运营商海量的 DNS 数据, 本文提出了一种多机分布式并行测量机制和大数据平台存储和监控方案, 实现了对 DNS 海量数据的高效测量分析, 此项技术可为其他大型数据的测量和分析提供参考. 基于测量机制, 多维度丰富的 DNS 数据测量分析结果展示了中国用户的访问特征以及和国际互联网用户访问的差异情况, 对提升 DNS 的运维和洞察 DNS 的特性具有重要价值. 本文基于测量提出并初步验证了一种适用于 DNS 大型运营商部署异常在线检测的通用框架, 此项技术对大型运营商部署异常检测系统具有重要的参考价值.

References

[1] Zhang B, Zhang Y, Zhang WZ. Study and analysis of recursive side DNS security. Ruan Jian Xue Bao/Journal of Software, 2024, 35(10): 4876–4911 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6987.htm [doi: 10.13328/j.cnki.jos.006987]

[2] Jung J, Sit E, Balakrishnan H, Morris R. DNS performance and the effectiveness of caching. IEEE/ACM Trans. on Networking, 2002, 10(5): 589–603. [doi: 10.1109/TNET.2002.803905]

[3] Brownlee N, Claffy KC, Nemeth E. DNS measurements at a root server. In: Proc. of the 2001 IEEE Global Telecommunications Conf. San Antonio: IEEE, 2001. 1672–1676. [DOI: 10.1109/GLOCOM.2001.965864]

[4] Castro S, Wessels D, Fomenkov M, Claffy K. A day at the root of the Internet. ACM SIGCOMM Computer Communication Review, 2008, 38(5): 41–46. [doi: 10.1145/1452335.1452341]

[5] Pang JA, Hendricks J, Akella A, de Prisco R, Maggs BM, Seshan S. Availability, usage, and deployment characteristics of the domain name system. In: Proc. of the 4th ACM SIGCOMM Conf. on Internet Measurement. Taormina Sicily: ACM, 2004. 1–14. [doi: 10.1145/

1028788.1028790]
[6] Danzig PB, Obraczka K, Kumar A. An analysis of wide-area name server traffic: A study of the Internet domain name system. ACM SIGCOMM Computer Communication Review, 1992, 22(4): 281–292. [doi: 10.1145/144191.144301]
[7] Gao HY, Yegneswaran V, Chen Y, Porras P, Ghosh S, Jiang J, Duan HX. An empirical reexamination of global DNS behavior. In: Proc. of the 2013 ACM SIGCOMM Conf. Hong Kong: ACM, 2013. 267–278. [doi: 10.1145/2486001.2486018]
[8] Gao HY, Yegneswaran V, Jiang J, Chen Y, Porras P, Ghosh S, Duan HX. Reexamining DNS from a global recursive resolver perspective. IEEE/ACM Trans. on Networking, 2016, 24(1): 43–57. [doi: 10.1109/TNET.2014.2358637]
[9] Farsight Security, Inc. Farsight security archive. 2013. https://archive.farsightsecurity.com/
[10] Kim TH, Reeves D. A survey of domain name system vulnerabilities and attacks. Journal of Surveillance, Security and Safety, 2020, 1(1): 34–60. [doi: 10.20517/jsss.2020.14]
[11] Callejo P, Cuevas R, Vallina-Rodriguez N, Rumin ÁC. Measuring the global recursive DNS infrastructure: A view from the edge. IEEE Access, 2019, 7: 168020–168028. [doi: 10.1109/ACCESS.2019.2950325]
[12] Lu CY, Liu BJ, Li Z, Hao S, Duan HX, Zhang MM, Leng CY, Liu Y, Zhang ZF, Wu JP. An end-to-end, large-scale measurement of DNS-over-encryption: How far have we come? In: Proc. of the 2019 Internet Measurement Conf. Amsterdam: ACM, 2019. 22–35. [doi: 10.1145/3355369.3355580]
[13] Jerabek K, Rysavy O, Burgetova I. Measurement and characterization of DNS over HTTPS traffic. arXiv:2204.03975, 2022.
[14] Dagon D, Provos N, Lee CP, Lee W. Corrupted DNS resolution paths: The rise of a malicious resolution authority. In: Proc. of the 2008 Network and Distributed Security Symposium. San Diego: The Internet Society, 2008.
[15] Cheng YN, Liu YL, Li C, Zhang ZX, Li N, Du YJ. In-depth evaluation of the impact of national-level DNS filtering on DNS resolvers over space and time. Electronics, 2022, 11(8): 1276. [doi: 10.3390/electronics11081276]
[16] Anonymous. The collateral damage of Internet censorshIP by DNS injection. ACM SIGCOMM Computer Communication Review, 2012, 42(3): 21–27. [doi: 10.1145/2317307.2317311]
[17] Liu BJ, Lu CY, Duan HX, Liu Y, Li Z, Hao S, Yang M. Who is answering my queries: Understanding and characterizing interception of the DNS resolution path. In: Proc. of the 2019 Applied Networking Research Workshop. Montreal: ACM, 2018. 15–16. [doi: 10.1145/3340301.3341122]
[18] Streibelt F, Sattler P, Lichtblau F, Gañán CH, Feldmann A, Gasser O, Fiebig, T. How ready is DNS for an IPv6-only world? In: Brunstrom A, Flores M, Fiore M, eds. Proc. of the 24th Passive and Active Measurement. Cham: Springer, 2023. 525–549. [doi: 10.1007/978-3-031-28486-1_22]
[19] Castro S, Zhang M, John W, Wessels D, Claffy K. Understanding and preparing for DNS evolution. In: Proc. of the 2nd Traffic Monitoring and Analysis. Zurich: Springer, 2010. 1–16. [doi: 10.1007/978-3-642-12365-8_1]
[20] Wessels D, Fomenkov M. Wow, that's a lot of packets. 2003. http://dns.measurement-factory.com/writings/wessels-pam2003-paper.pdf
[21] Jonker M, Akiwate G, Affinito A, Claffy KC, Botta A, Voelker GM, van Rijswijk-Deij R, Savage S. Where .ru?: Assessing the impact of conflict on Russian domain infrastructure. In: Proc. of the 22nd ACM Internet Measurement Conf. Nice: ACM, 2022. 159–165. [doi: 10.1145/3517745.3561423]
[22] Li S, Du SS, Huang WF, Liang SY, Deng JX, Wang L, Huang HW, Liao XH, Su S. A light-weighted data collection method for DNS simulation on the cyber range. KSII Trans. on Internet and Information Systems, 2020, 14(8): 3501–3518. [doi: 10.3837/tiis.2020.08.020]
[23] van Rijswijk-Deij R, Jonker M, Sperotto A, Pras A. The Internet of names: A DNS big dataset. In: Proc. of the 2015 ACM Conf. on Special Interest Group on Data Communication. London: ACM, 2015. 91–92. [doi: 10.1145/2785956.2789996]
[24] van Rijswijk-Deij R, Jonker M, Sperotto A, Pras A. A high-performance, scalable infrastructure for large-scale active DNS measurements. IEEE Journal on Selected Areas in Communications, 2016, 34(6): 1877–1888. [doi: 10.1109/JSAC.2016.2558918]
[25] Kosek M, Schumann L, Marx R, Doan TV, Bajpai V. DNS privacy with speed?: Evaluating DNS over QUIC and its impact on Web performance. In: Proc. of the 22nd ACM Internet Measurement Conf. Nice: ACM, 2022. 44–50. [doi: 10.1145/3517745.3561445]
[26] Chhabra R, Murley P, Kumar D, Bailey M, Wang G. Measuring DNS-over-HTTPS performance around the world. In: Proc. of the 21st ACM Internet Measurement Conf. ACM, 2021. 351–365. [doi: 10.1145/3487552.3487849]
[27] Xu CX, Zhang YY, Shi F, Shan H, Guo BY, Li YW, Xue PF. Measuring the centrality of DNS infrastructure in the wild. Applied Sciences, 2023, 13(9): 5739. [doi: 10.3390/app13095739]
[28] Liu WF, Zhang Y, Zhang HL, Fang BX. Survey on domain name system measurement research. Ruan Jian Xue Bao/Journal of Software, 2022, 33(1): 211–232 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6218.htm [doi: 10.13328/j.cnki.jos.006218]
[29] Antonakakis M, Perdisci R, Dagon D, Lee W, Feamster N. Building a dynamic reputation system for DNS. In: Proc. of the 19th USENIX Conf. on Security. Washington DC: USENIX Association, 2010. 273–290.
[30] Bilge L, Sen S, Balzarotti D, Kirda E, Kruegel C. Exposure: A passive DNS analysis service to detect and report malicious domains. ACM Trans. on Information and System Security, 2014, 16(4): 14. [doi: 10.1145/2584679]

[31] Perdisci R, Corona I, Giacinto G. Early detection of malicious flux networks via large-scale passive DNS traffic analysis. IEEE Trans. on Dependable and Secure Computing, 2012, 9(5): 714–726. [doi: 10.1109/TDSC.2012.35]
[32] Nelms T, Perdisci R, Ahamad M. ExecScent: Mining for new C&C domains in live networks with adaptive control protocol templates. In: Proc. of the 22nd USENIX Conf. on Security. Washington: USENIX Association, 2013. 589–604.
[33] Rahbarinia B, Perdisci R, Antonakakis M. Efficient and accurate behavior-based tracking of malware-control domains in large ISP networks. ACM Trans. on Privacy and Security, 2016, 19(2): 4. [doi: 10.1145/2960409]
[34] Berger A, D'Alconzo A, Gansterer WN, Pescapé A. Mining agile DNS traffic using graph analysis for cybercrime detection. Computer Networks, 2016, 100: 28–44. [doi: 10.1016/j.comnet.2016.02.009]
[35] Choi H, Lee H, Kim H. BotGAD: Detecting botnets by capturing group activities in network traffic. In: Proc. of the 4th Int'l ICST Conf. on Communication System Software and Middleware. Dublin: ACM, 2009. 2. [doi: 10.1145/1621890.1621893]
[36] Choi H, Lee H. Identifying botnets by capturing group activities in DNS traffic. Computer Networks, 2012, 56(1): 20–33. [doi: 10.1016/j.comnet.2011.07.018]
[37] Singh M, Singh M, Kaur S. Detecting bot-infected machines using DNS fingerprinting. Digital Investigation, 2019, 28: 14–33. [doi: 10.1016/j.diin.2018.12.005]

附中文参考文献

[1] 张宾, 张宇, 张伟哲. 递归侧 DNS 安全研究与分析. 软件学报, 2024, 35(10): 4876–4911. http://www.jos.org.cn/1000-9825/6987.htm [doi: 10.13328/j.cnki.jos.006987]
[28] 刘文峰, 张宇, 张宏莉, 方滨兴. 域名系统测量研究综述. 软件学报, 2022, 33(1): 211–232. http://www.jos.org.cn/1000-9825/6218.htm [doi: 10.13328/j.cnki.jos.006218]

作者简介

张宾, 博士, 高级工程师, 博士生导师, 主要研究领域为网络安全, 网络管理, 数据分析.
杨书徒, 工程师, 主要研究领域为网络流量测量.
姬东岑, 工程师, 主要研究领域为网络空间安全.
张宇, 博士, 教授, CCF 高级会员, 主要研究领域为互联网基础设施安全, 网络拓扑测量, 未来网络体系.
张伟哲, 博士, 教授, 博士生导师, CCF 杰出会员, 主要研究领域为信息安全, 系统结构.
涂唯坚, 工程师, 主要研究领域为网络运维.
戴一娜, 博士生, 主要研究领域为网络空间安全.