Domain Name System Operations (dnsop)
Internet-Draft
Intended status: Standards Track
Expires: 26 June 2026

Q. Li
Z. Wang
W. Wu
Z. Li
Chinese Academy of Sciences
J. Yan
China Internet Network Information Center
Z. Li
Chinese Academy of Sciences
Z. Yan
China Internet Network Information Center

23 December 2025

QNAME Minimization Trade-offs : Privacy Leakage and Amplification potential
draft-li-qname-minimization-trade-offs-00

Abstract

This document examines the current protocol policies and operational state of QNAME Minimization (QMIN), defined in RFC 9156 [RFC9156]. While QMIN is a DNS privacy mechanism, its existing implementation strategies introduce subtle trade-offs between privacy and security. Specifically, current policies may still present potential information leakage or introduce query amplification potential. This informational document aims to alert protocol designers, implementers, and users to these emerging challenges and suggests that a careful re-evaluation and improvement of the QMIN mechanism are necessary to fully mitigate these combined privacy and security risks.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 26 June 2026.

Table of Contents

1. Introduction

The Domain Name System (DNS) is foundational to the modern internet. However, its inherent design, which involves recursive resolution and delegation chains, presents challenges related to both privacy and operational efficiency. In the traditional DNS resolution process, recursive resolvers typically send the Original QNAME (the query name identical to the initial client request) across the entire delegation chain [RFC1034][RFC1035]. This practice results in the unnecessary exposure of sensitive subdomain information to intermediate, higher-level nameservers that do not require the full name to perform their delegation task [RFC6973][RFC7626][RFC9076].

To address this critical privacy concern, the QNAME Minimization (QMIN) mechanism was introduced and standardized in RFC 9156 [RFC9156]. QMIN is a technique where a recursive resolver minimizes the DNS query name sent to an authoritative nameserver. Instead of

sending the full name, the resolver only sends the minimum set of labels necessary to receive a referral to the next nameserver in the delegation chain[RFC7816].

For example, to resolve www.example.com., a QMIN-enabled resolver first asks the root server only for com., then asks the .com server only for example.com., and so on.

However, while QMIN successfully mitigates privacy leakage, its implementation has inadvertently introduced new security and performance complexities, primarily related to query amplification. The inherent structure of DNS, where resolution is hierarchical and delegated, means that resolvers must traverse the entire delegation chain, generating a minimum number of requests equal to the chain's length [firstlook][secondlook]. As detailed in the following sections, this baseline query volume is further inflated by factors such as the need to resolve NS records (glue records) and domain redirections (CNAME/DNAME RRs). The adoption of QMIN, due to its label-by-label request nature and the potential to apply minimization to passively introduced Referral QNAMEs (domain names encountered during resolution), can significantly exacerbate this traffic inflation. This characteristic makes QMIN a potential amplifier in various types of DNS resolver amplification attacks.

2. Terminology

The key terms used in this document are defined as follows:

Delegation point: The specific label that leads to a delegation to another nameserver.

Original QNAME: The QNAME identical to the initial client query.

Referral QNAME: Other QNAMEs introduced during the resolution process.

Privacy leakage: Any QNAME labels sent to the current server but not necessary for its task—and are instead destined for servers further down the chain.

3. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

4. QMIN Amplification Characteristics

The DNS resolution scope is hierarchical and delegated. Consequently, each authoritative nameserver can only resolve queries for the specific Zone of Authority it directly manages, along with any subdomains within that zone that have not been further delegated [RFC1034][RFC1035].

To resolve any given domain name, regardless of the method used, recursive resolvers must traverse the entire delegation chain, querying each nameserver in the chain until the nameserver holding the final Resource Records (RRs) is reached, at which point the final resolution is performed. Therefore, the minimum number of requests generated on the authority side by a single user query is equal to the length of the nameserver delegation chain. As a result, the number of requests observed on the authority side generally exceeds the number of user-initiated queries.

Beyond potential network or server anomalies, or domain errors, the primary reasons for this inflation include:

* Delegation Chain Length: A single user query generates a minimum of requests equal to the length of the delegation chain, resulting in higher authority-side traffic for longer chains.

* NS Record Resolution: Resolvers may not be able to obtain the IP addresses of the delegated child nameservers directly from the parent nameserver’s referral response (e.g., due to the lack of glue records in the Additional section), necessitating separate queries to resolve those NS hostnames.

* Domain Redirection: Resolvers may encounter redirection records, such as CNAME or DNAME RRs, during resolution, which redirects the query to a new domain name, thereby increasing the total number of required queries.

The adoption of QNAME Minimization (QMIN), as defined in RFC 9156 [RFC9156], can further amplify the traffic on the authority side because:

* Label-by-Label Request: Under QMIN, resolvers may repeatedly query the same authoritative server label-by-label. If the number of labels in the QNAME exceeds the length of the nameserver delegation chain, the sequential label-by-label querying inherent to QMIN will result in a higher query count compared to non-QMIN resolution.

* Undefined Scope for Referral QNAMEs: RFC 9156 [RFC9156] does not explicitly specify the domain scope for QMIN execution. By default, resolvers may apply QMIN to both the Original QNAME from the user request and any Referral QNAMEs passively introduced in responses, further increasing query traffic.

* Exploitation via Referral Responses: An attacker can exploit QMIN by intentionally returning referral responses that omit glue records in every QMIN request, thus increasing the number of Referral QNAMEs the resolver must process. This can be further escalated by increasing the depth of referral resolution, significantly expanding the authority-side request volume.

Consequently, due to its inherent query amplification characteristics, QMIN can be leveraged as an amplifier in various types of DNS resolver amplification attacks.

5. QMIN Implementation Strategies

While RFC 9156 [RFC9156] imposes necessary constraints on the functionality and deployment of QNAME Minimization (QMIN), significant variations in protocol implementation approaches persist among recursive resolvers. These implementation differences result in notable variances in the amplification risk profile presented by different QMIN strategies.

In summary, three main implementation strategies are currently observed.

5.1. Complete QMIN

Resolvers deploying Complete QMIN apply the minimization technique to both the Original QNAME from the client request and all Referral QNAMEs generated throughout the resolution process. Consequently, Complete QMIN presents the greatest amplification potential and is subject to the largest traffic pressure when facing amplification attacks.

5.2. Root & TLD Only

Under this QMIN implementation strategy, resolvers still apply minimization to the Original QNAME and all Referral QNAMEs, but QMIN querying is strictly used only for labels that are resolved by Root or Top-Level Domain (TLD) nameservers. For subsequent domain prefixes, the No QMIN (full QNAME) policy is used.

The Root & TLD Only strategy mitigates amplification risk by:

* Limiting the scope of QMIN execution to the top levels, thereby avoiding repeated, label-by-label requests to the same authoritative server.

* Restricting the total number of QMIN queries, which limits the volume of malicious Referral QNAMEs that an attacker can construct during an amplification attack.

Therefore, the Root & TLD Only strategy achieves an effectiveness in mitigating amplification attacks that is comparable to the No-QMIN policy.

5.3. Original QNAME Only

In this implementation, resolvers only perform QNAME minimization on the original domain name requested by the user, while adopting the No-QMIN policy for querying all Referral QNAMEs generated during the recursive resolution. However, the "Original QNAME Only" strategy is not effective in reducing the issue of repeatedly querying the same name server with the original QNAME. While it effectively lowers the amplification factor, it still carries a certain risk of amplification.

6. Security Considerations

This document considers the security challenges introduced by the deployment of the QNAME Minimization (QMIN) mechanism.

QMIN’s design goal is to enhance privacy by reducing the exposure of sensitive subdomain information to upstream nameservers. However, as discussed in Section 3, certain QMIN implementation strategies (specifically Complete QMIN) can significantly increase query traffic on authoritative nameservers due to their label-by-label querying nature and the handling of Referral QNAMEs.

This amplification of query traffic makes QMIN a potential amplifier in DNS resolver amplification attacks. A malicious attacker can exploit this characteristic by manipulating referral responses (e.g., omitting glue records) to force resolvers to send a large volume of queries to a target authoritative server, thus posing a Denial of Service (DoS) or Distributed Denial of Service (DDoS) threat.

The guidelines in this document aim to direct protocol designers and implementers to balance the privacy benefits of QMIN against the amplification risks it may exacerbate, recommending strategies that restrict the scope of QMIN, such as the Root & TLD Only approach, to mitigate security risks.

7. IANA Considerations

This document has no IANA actions.

8. References

8.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/rfc/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/rfc/rfc1035>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9156] Bortzmeyer, S., Dolmans, R., and P. Hoffman, "DNS Query Name Minimisation to Improve Privacy", RFC 9156, DOI 10.17487/RFC9156, November 2021, <https://www.rfc-editor.org/rfc/rfc9156>.

8.2. Informative References

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/rfc/rfc6973>.

[RFC7626] Bortzmeyer, S., "DNS Privacy Considerations", RFC 7626, DOI 10.17487/RFC7626, August 2015, <https://www.rfc-editor.org/rfc/rfc7626>.

[RFC7816] Bortzmeyer, S., "DNS Query Name Minimisation to Improve Privacy", RFC 7816, DOI 10.17487/RFC7816, March 2016, <https://www.rfc-editor.org/rfc/rfc7816>.

[RFC9076] Wicinski, T., Ed., "DNS Privacy Considerations", RFC 9076, DOI 10.17487/RFC9076, July 2021, <https://www.rfc-editor.org/rfc/rfc9076>.

[firstlook] de Vries, "A first look at QNAME minimization in the domain name system", International Conference on Passive and Active Network Measurement Springer, 2019.

[secondlook] Magnusson, Mller, and Brunstrom, "A second look at DNS QNAME minimization", International Conference on Passive and Active Network Measurement 496-521, 2023.

Authors' Addresses

Qinxin Li
Chinese Academy of Sciences
Beijing
China
Email: liqinxin23s@ict.ac.cn

Zhaohua Wang
Chinese Academy of Sciences
Beijing
China
Email: wangzh@cnic.cn

Wenhao Wu
Chinese Academy of Sciences
Beijing
China
Email: wuwenhao22s@ict.ac.cn

Zihan Li
Chinese Academy of Sciences
Beijing
China
Email: lizihan24z@ict.ac.cn

Jin Yan
China Internet Network Information Center
Beijing
China

Email: yanjin@cnnic.cn

Zhenyu Li
Chinese Academy of Sciences
Beijing
China
Email: zyli@ict.ac.cn

Zhiwei Yan
China Internet Network Information Center
Beijing
China
Email: yanzhiwei@cnnic.cn