dnsop
Internet-Draft
Intended status: Best Current Practice
Expires: 20 January 2026

X.L. Li
Y.Q. Qiu
Nankai University

July 2025

Best Current Practices for DNS Resolver Resilience Against Coordinated Amplification Attacks
draft-li-dnsop-resolver-resilience-00

Abstract

This document describes an attack vector, exemplified by the "DNSBomb" attack, that leverages the emergent behavior of several widely- implemented DNS resolver mechanisms. By combining query timeouts, query aggregation, and response timing, an attacker can turn a set of resolvers into powerful amplifiers for a Pulsing Denial-of-Service (PDoS) attack. This attack is difficult to detect due to its low average traffic rate but can be highly effective at overwhelming a target’s resources.

This document provides operational guidance and a set of best practices for DNS resolver implementers and operators to mitigate this threat. The goal is to harden the DNS ecosystem by reducing the potential for resolvers to be used in such a coordinated fashion, thereby improving the operational resilience of the DNS.

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 2 January 2026.

Copyright Notice

Table of Contents

1. Introduction

The Domain Name System (DNS) [RFC1034] [RFC1035] has long been used as a vector for reflection and amplification attacks [RFC5358]. A sophisticated variant, the Pulsing Denial-of-Service (PDoS) attack [Shrew], uses intermittent, high-volume traffic bursts. This pattern makes PDoS attacks challenging to detect with conventional traffic analysis, yet they remain highly effective.

The "DNSBomb" attack [DNSBomb] demonstrates a practical method for generating such bursts by exploiting the combined, emergent behavior of standard resolver features. The attack model does not rely on a single protocol vulnerability but on the operational ambiguity in how resolvers should handle a specific sequence of events: a large number of queries from a single source for a domain whose authoritative server is slow to respond.

This document specifies best practices for resolver implementations and configurations to mitigate this and similar attack vectors. These practices are designed to limit the ability of an attacker to accumulate and concentrate responses without negatively impacting legitimate use cases.

1.1. 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.

2. Terminology

Pulsing DoS (PDoS) Attack:
: A Denial-of-Service attack characterized by intermittent, short bursts of high-volume traffic separated by periods of little or no attack traffic.

Query Accumulation:
: An attack phase where a resolver receives and holds numerous queries, typically from a spoofed source IP, while awaiting a delayed response from a malicious authoritative nameserver.

Response Concentration:
: The near-simultaneous transmission of a large number of DNS responses from a resolver to a single target. This is the culmination of the attack, forming the traffic pulse.

Response Pacing:
: A mitigation technique whereby a resolver deliberately de-synchronizes the transmission of a large batch of responses to a single client to prevent a traffic spike.

3. Attack Model

The attack model assumes the adversary can send IP-spoofed DNS queries and controls an authoritative nameserver for a domain. The attack proceeds in three phases:

1. *Accumulation:* The attacker sends a low-rate stream of queries for unique subdomains of their controlled domain to one or more recursive resolvers. The source IP address is spoofed to that of the victim. The attacker's authoritative server receives the upstream queries from the resolver but deliberately withholds its response. The resolver's query timeout window (potentially extended by IP defragmentation timeouts [RFC0791]) becomes the accumulation period.

2. *Amplification:* The attacker leverages query aggregation within the resolver to minimize the upstream query load on their authoritative server. When the attacker finally responds, it sends a large response, using EDNS(0) [RFC6891] to maximize the payload size. This single large response will be used as the basis for responding to all accumulated queries.

3. *Concentration:* Upon receiving the single, delayed response, the resolver unblocks all pending client-side queries. Due to optimizations for low latency, many resolvers will transmit all of these responses to the victim's IP address nearly simultaneously, creating a powerful, concentrated traffic pulse.

4. Problem Statement

This attack vector arises from an operational ambiguity in current DNS specifications. While features like query timeouts, aggregation, and fast response are individually beneficial for performance and resilience, their interaction under specific, maliciously crafted conditions is not well-defined. Resolvers lack clear guidance on how to differentiate between a legitimate, large-scale query event (e.g., from a large NAT) and a coordinated attack. This document aims to provide that guidance to reduce the potential for exploitation.

5. Mitigation Strategies and Operational Guidance

To mitigate this attack vector, this document recommends a set of interrelated strategies for resolver software and its operation.

5.1. Response Pacing

The most direct mitigation for the response concentration phase is Response Pacing. When a resolver is about to send a large number of responses to a single client IP address in a short time window (e.g., as a result of a single upstream answer), it SHOULD introduce a small, randomized delay (jitter) between each response transmission.

This technique de-synchronizes the response burst, spreading it out over time and reducing its peak bandwidth. The total delay should be carefully calibrated to avoid a significant performance impact on legitimate clients.

Operational Trade-offs: This mechanism may introduce minor latency for legitimate clients behind large-scale NATs. The pacing algorithm should be configurable and potentially adaptive based on the number of responses in the queue.

5.2. Guidance on Timeout Values

Long upstream query timeouts provide a larger window for query accumulation. It is RECOMMENDED that resolver operators configure shorter timeouts for queries to authoritative servers. A value between 1.5 and 3 seconds is generally sufficient to accommodate most network conditions without providing an excessive window for attackers.

Resolver software MAY also implement adaptive timeouts. For example, if an authoritative server is consistently slow, the resolver could dynamically shorten the timeout for subsequent queries to it.

5.3. Limiting Query Accumulation

Resolvers SHOULD implement a mechanism to limit the number of pending queries that can be accumulated per source IP address (or prefix). A configurable limit on the number of outstanding queries from a single source directly caps the scale of the accumulation phase.

Once this limit is reached, the resolver SHOULD either drop new queries from that source or respond immediately with an appropriate error code (e.g., REFUSED) until some of the pending queries are resolved. This is preferable to holding an unbounded number of queries.

Operational Trade-offs: A limit that is too low could affect service for users behind large-scale NATs. This limit should be configurable by the operator.

5.4. EDNS(0) Buffer Size

To limit the amplification factor, it is a standing best practice for resolver operators to configure a conservative EDNS(0) UDP buffer size. A value of 1232 bytes is RECOMMENDED, as this avoids IP fragmentation on most network paths. Operators SHOULD NOT configure larger values without a specific and compelling operational requirement.

6. Security Considerations

The practices described in this document are designed to mitigate a specific attack vector and are not a complete solution for all DNS-based DoS attacks. The effectiveness of these mitigations relies on their combined deployment.

Source address validation remains the most fundamental defense against attacks requiring IP spoofing. Network operators are strongly urged to implement ingress filtering as described in BCP 38 [RFC2827] and BCP 84 [RFC3704].

The mitigations proposed herein involve operational trade-offs between security and performance. For example, Response Pacing adds latency, and strict query accumulation limits may impact legitimate users. Operators must be able to configure these parameters to suit their specific environment. The default settings in resolver software should prioritize resilience.

While these measures make individual resolvers more resilient, a sufficiently motivated attacker could still achieve a significant impact by coordinating a very large number of unpatched or misconfigured resolvers. Therefore, broad adoption of these best practices across the community is essential for improving the overall security posture of the DNS.

7. IANA Considerations

This document has no IANA actions.

Contributors

The authors of the "DNSBomb" paper, Dashuai Wu, Haixin Duan, and Qi Li, provided the foundational research for the attack vector described in this document.

References

Normative References

[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/info/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/info/rfc8174>.

Informative References

[DNSBomb] Li, X., Wu, D., Duan, H., and Q. Li, "DNSBOMB: A New Practical-and-Powerful Pulsing DoS Attack Exploiting DNS Queries-and-Responses", May 2024, <https://www.researchgate.net/publication/376355184>.

[Shrew] Kuzmanovic, A. and E. Knightly, "Low-rate TCP-targeted denial of service attacks", ACM SIGCOMM Computer Communication Review vol. 33, no. 4, pp. 75-86, 2003.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

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

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

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <https://www.rfc-editor.org/info/rfc2827>.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, DOI 10.17487/RFC3704, March 2004, <https://www.rfc-editor.org/info/rfc3704>.

[RFC5358] Damas, J. and F. Neves, "Preventing Use of Recursive Nameservers in Reflector Attacks", BCP 140, RFC 5358, DOI 10.17487/RFC5358, October 2008, <https://www.rfc-editor.org/info/rfc5358>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/info/rfc6891>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

Authors' Addresses

Xiang Li
Nankai University
38 Tongyan Road
Tianjin
Tianjin, 300355
China
Email: lixiang@nankai.edu.cn

Yuqi Qiu
Nankai University
38 Tongyan Road
Tianjin
Tianjin, 300355
China
Email: norahqiu@163.com