DNS Operation Group
Internet-Draft
Intended status: Best Current Practice
Expires: 9 July 2026

P. Zuo
CNNIC
J. Ableyy
Cloudflare
Z. Yan
CNNIC

January 2026

Avoid Large Records with a Wildcard Owner Name
draft-avoid-large-wildcard-records-00

Abstract

As DNS hosting becomes increasingly centralized, with multiple zones hosted on shared authoritative name servers, the risk of DNS amplification attacks has grown. By crafting large DNS records with wildcard owner names, attackers can exploit these shared servers to launch high-volume DDoS amplification attacks.

This document provides operational guidance for DNS hosting providers to mitigate DDoS risks arising from amplification of responses derived from wildcard owner names.

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 5 July 2026.

Copyright Notice

Table of Contents

1. Introduction

The DNS system exhibits a small-query, large-response characteristic, which can lead to high amplification towards targeted victims. Both recursive and authoritative DNS servers can be abused as amplifiers. Previous work [RFC5358] recommends restricting recursive lookup services to intended clients to prevent unintended amplification. Additionally, [RFC8482] recommends returning minimal-sized responses for queries with QTYPE=ANY.

However, the risk of DNS amplification remains critical. The centralization of DNS hosting and the increasing number of open recursive resolvers worldwide have heightened the potential for DDoS amplification attacks. On one hand , exploitation of a single hosted zone may affect all zones on the same name server.On the other hand, the large and globally distributed population of open resolvers provides attackers with an extensive amplification surface.

This document provides guidance for DNS hosting providers to mitigate DDoS risks arising from maliciously crafted DNS records.

2. Problem Description

A DNS amplification attack typically requires the following conditions:

1. Very large responses to DNS queries.
2. Queries that consistently bypass recursive DNS caches.
3. Low operational cost or effort for the attacker.

These conditions can be easily satisfied by configuring oversized DNS records such as large TXT records with wildcard owner names on shared DNS hosting platforms. An attacker can then issue small queries with randomized labels, discard the replies, and trigger excessive traffic between recursive resolvers and authoritative servers. Because wildcard expansion forces each random name to bypass resolver caches, the queries are repeatedly forwarded upstream to authoritative DNS servers. The attack is highly efficient because an originating stub resolver using UDP without EDNS(0) will trigger a truncated response from the open resolver, which prevents large authoritative answers from reaching the originating host. As a result, bandwidth consumption is confined to the path between open resolvers and authoritative servers. The lack of EDNS(0) also provides only a weak signal, making it difficult to develop effective mitigations based solely on this behavior.

The following illustrates a scenario where an attacker could exhaust the outbound capacity of a victim authoritative server:

1. Identify the authoritative name server for the victim domain.

2. Register a domain controlled by the attacker on the same name server.

3. Create oversized records with a wildcard owner name, such as TXT records.

4. Identify open recursive resolvers by scanning the IP space.

5. Use automated tools to send DNS queries for random subdomains (e.g., {random}.attack TXT) to open recursive resolvers.

6. The outbound capacity from the authoritative server hosting the victim domain will be exhausted.

Attackers can also leverage compromised hosts, for example systems within a botnet that rely on their configured recursive resolvers, to initiate the attack. In this case, DNS queries can be triggered indirectly by other application protocols. Examples include a web advertisement that embeds a URL containing the target domain and a randomized sublabel, or a minor compromise of a popular web page that inserts an equivalent invisible reference. These mechanisms allow large volumes of queries to be generated without requiring direct control of the DNS client software.

3. Recommendations

This section provides best practices for maintaining DNS data at reasonable sizes and reducing the risk that a shared authoritative server may be abused. Recommendations primarily target DNS hosting providers.

Operators should enforce size limits for large records, particularly those with wildcard owner names, and apply restrictive controls when records have very short TTLs. Thresholds should be determined based on the operational environment and risk tolerance.

Recommended practices:

1. *Apply size limits to records with wildcard owner names.*

   Enforce maximum size thresholds for DNS records defined under wildcard owner names to prevent amplification through oversized responses.

2. *Apply size limits to records with very small TTLs.*

   Short TTL values increase cache-miss frequency, which amplifies the number of forwarded queries.

3. *Monitor for abnormal traffic patterns.*

   Implement logging and real-time alerting to detect unusually high query volumes or other indicators of potential attack activity.

4. *Rate-limit queries that generate large responses.*

   Apply per-source, per-prefix, or query-type-aware rate limiting to reduce amplification effects and prevent overload on authoritative servers.

5. *Restrict and periodically review wildcard usage.*

   Require justification and periodic review for wildcard records with large RDATA to avoid unintended amplification exposure.

6. *Test mitigation controls.*

   Regularly test monitoring, rate-limiting, and record-size enforcement mechanisms under realistic conditions, adjusting thresholds to maintain protection without disrupting legitimate traffic.

These measures reduce the attack surface for DNS amplification attacks while enabling operators to balance availability and security for their users.

4. Implementation Experience

Tests have shown that some DNS hosting providers allow users to configure oversized records with wildcard owner names. Responses exceeding the standard UDP packet size trigger TCP fallback, allowing responses up to approximately 64 KB, yielding amplification factors exceeding 1000x.

Observations from providers include:

1. GoDaddy imposes no limit for jumbo TXT records.
2. Cloudflare imposes a limit of 8192 bytes for jumbo TXT records.
3. Microsoft DNS service imposes a limit of 4096 bytes.
4. Alibaba Cloud and DNSPod set limits following disclosure of these risks.

5. Normative References

[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>.

[RFC8482] Abley, J., Gudmundsson, O., Majkowski, M., and E. Hunt, "Providing Minimal-Sized Responses to DNS Queries That Have QTYPE=ANY", RFC 8482, DOI 10.17487/RFC8482, January 2019, <https://www.rfc-editor.org/info/rfc8482>.

Appendix A: Bandwidth Impact Model

This non-normative appendix provides an illustrative model of the aggregated bandwidth impact of large DNS responses in amplification scenarios.

In large-scale amplification scenarios, total bandwidth impact grows proportionally with the number of attack sources and the average response size. To assist operators in evaluating practical effects of response size limits, a simplified model is provided.

Let:

* _N_ = number of attack sources (or open resolvers exploited)
* _q_ = per-source query rate (queries per second)
* _Q_ = query packet size (bytes)

* _S_ = authoritative response size (bytes)
* _R_ = fraction of queries resulting in cache misses, generating upstream traffic

The total query rate is _N*q_.

Approximate bandwidth at different points in the resolution path:

* Attacker upstream bandwidth: _N*q*Q_ bytes/s
* Authoritative server outbound bandwidth: _N*q*R*S_ bytes/s
* Resolver total bandwidth (receive + send): _(N*q*Q + N*q*Q*R + N*q*R*S)_ bytes/s

These relationships are linear in _S_, illustrating that reducing response size proportionally reduces bandwidth requirements for all participants. This model ignores retransmissions, protocol overhead, and TCP fallback.

For illustration, consider two nominal attack-source distributions:

Parameter	Case A	Case B
Number of sources (N)	1,000	50,000
Query rate per source (q)	1 qps	1 qps
Query size (Q)	60 bytes	60 bytes
Cache miss ratio (R)	1.0	0.8

Table 1: Attack Source Distributions

Approximate aggregate bandwidths at different response size caps:

Response Size (bytes)	Attacker Upstream (Case A / Case B)	Authoritative Outbound (Case A / Case B)	Resolver Total (Case A / Case B)
65,535	0.480 Mbps / 24.0 Mbps	524.3 Mbps / 21.0 Gbps	525.2 Mbps / 21.1 Gbps
8,192	0.480 Mbps / 24.0 Mbps	65.5 Mbps / 2.62 Gbps	66.5 Mbps / 2.66 Gbps
4,096	0.480 Mbps / 24.0 Mbps	32.8 Mbps / 1.3 Gbps	33.7 Mbps / 1.35 Gbps
1,024	0.480 Mbps / 24.0 Mbps	8.2 Mbps / 0.32 Gbps	9.1 Mbps / 0.37 Gbps
512	0.480 Mbps / 24.0 Mbps	4.1 Mbps / 0.16 Gbps	5.1 Mbps / 0.21 Gbps

Table 2: Aggregated Bandwidth at Different Response Size Threshold

Authors' Addresses

Peng Zuo
CNNIC
No.4, Yard 9, Qiche Museum West Road, Fengtai District
Beijing
100190
China
Email: zuopeng@cnnic.cn

Joe Abley
Cloudflare
Amsterdam
Netherlands
Email: jabley@cloudflare.com

Zhiwei Yan
CNNIC
No.4, Yard 9, Qiche Museum West Road, Fengtai District
Beijing
100190
China
Email: yanzhiwei@cnnic.cn