DNSOP
Internet-Draft
Updates: 1035 (if approved)
Intended status: Standards Track
Expires: September 7, 2015

O. Gudmundsson
M. Majkowski
CloudFlare Inc.

March 6, 2015

Standard way for Authoratitive DNS servers to refuse ANY query
draft-ogud-dnsop-any-notimp-00

Abstract

DNS ANY query is widely abused for reflection attacks. This feature was designed to aid in debugging. As there is no good reason for applications to ever issue an ANY query this document codifies how an authoritative server can reject such queries.

Status of This Memo

This Internet-Draft will expire on September 7, 2015.

Copyright Notice

Table of Contents

1. Introduction

DNS is an evolving protocol, at glacial phase, this document specifies how an Authorative server can reject an ANY query. ANY queries are widely abused by attackers doing reflection attacks as they return the largest answers. Over the years a number of attempts have been made to throttle ANY queries, ranging from returning TC bit to all UDP ANY queries, blocking them totally, and QoS'ing the number of ANY queires accepted per second. All of those are band-aids.

Some modern Authoritative servers, such as those used by CDN's, do not have DNS zones. For those servers answering ANY query truthfully is hard work. Thus ignoring ANY queries simplifies the implementation.

2. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Protocol change

An Authorative DNS[RFC1035] server can reject ANY query by returning RCODE = 4 (NOTIMP).

A Recurisive Resolver SHOULD ignore RD bit set on ANY query. Additionaly as Recursive Resolver SHOULD remember that ANY queries are not available from upstream Auth server, this SHOULD be cached for at least 5 minutes.

4. IANA considerations

No IANA action is requested

5. Security considerations

ANY query is mainly used for attacks on the internet due to its amplification factor. Codifying this behavior makes life harder for attackers, at minimal cost for DNS operators.

6. Internationalizaiton Considerations

NONE

7. Implementation Experience

TBD

8. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Appendix A. Document history

[RFC Editor: Please remove this section before publication]

00 Initial version

Authors' Addresses

Olafur Gudmundsson
CloudFlare Inc.
San Francisco, CA 94107
USA

Email: olafur@cloudflare.com

Marek Majkowski
CloudFlare Inc.
London
UK

Email: marek@cloudflare.com