Identifying and Reacting to Unsolicited DNS Queries

draft-koch-dns-unsolicited-queries-03

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the
provisions of BCP 78 and BCP 79. This document may contain material
from IETF Documents or IETF Contributions published or made publicly
available before November 10, 2008. The person(s) controlling the
copyright in some of this material may not have granted the IETF
Trust the right to allow modifications of such material outside the
IETF Standards Process. Without obtaining an adequate license from
the person(s) controlling the copyright in such materials, this
document may not be modified outside the IETF Standards Process, and
derivative works of it may not be created outside the IETF Standards
Process, except to format it for publication as an RFC or to
translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering
Task Force (IETF), its areas, and its working groups. Note that
other groups may also distribute working documents as Internet-
Drafts.

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."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at

This Internet-Draft will expire on September 10, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Abstract

This document deals with unsolicited Domain Name System (DNS) queries directed towards authoritative name servers. It identifies reasons for the existence of these queries and lists some observed or proposed reactions.

1. Introduction

Authoritative name servers should see Domain Name System (DNS) queries only for domain names within or below zones they are authoritative for. Responses are either positive responses (consisting of RRSets), negative responses (either NXDOMAIN [RFC5395] or NOERROR/NODATA) or referrals. The latter point the querying entity towards another set of name servers for names in delegated zones, i.e., for names "below" those zones served authoritatively.

Operational experience shows that many larger authoritative name servers receive a non-negligible amount of DNS queries that do not match the above description and will be called "unsolicited DNS queries" further on. This term is not intended to have any legal meaning or implication. Instead it should express that the usual DNS delegation and resolution process either does not lead to those queries or the references are unknown to and unintended by the server operator.

This document explores different causes and properties of unsolicited DNS queries and provides a list of reactions to those queries as seen on the Internet. (Discussion of trade-offs needs to be intensified.)

This document primarily deals with unsolicited queries directed towards authoritative name servers. Abusive DNS queries towards recursive name servers for amplification or reflection attacks are described in [RFC5358]. Where the term "authoritative server" is not useful per se without stating which zone(s) it refers to, it is meant to express that the server does not offer DNS recursion to any client.

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].
(Comments should be directed at the author.)

2. Types of Unsolicited Queries

A DNS query is identified by the triple of QNAME, QTYPE and QCLASS. Either of these or any combination might or might not be expected at an authoritative name server.

QTYPE is a flexible part in this triple, since if a server is authoritative for a certain zone in a particular class, a query for any QTYPE (except DS [RFC4034]) is rightfully directed towards this server. Sometimes QTYPES do not match well known types, but a name server must still be able to authoritatively respond for zones it serves, as per [RFC3597].

QCLASS is expected to be IN, the only class widely used on the Internet. Although [RFC1123], section 6.1.2.2, restricts the use of QCLASS=*, queries with this parameter are sometimes seen. They can usually be answered, since "*" (or ANY) matches IN, but the AA bit can never be set as per section 3.7.1 of [RFC1034]. QCLASS=CHAOs is also used in identification queries [RFC4892].

QNAME should fall into or below any of the zones served authoritatively. If the QNAME is not matched by any of these zones, it may be an ancestor of a served zone (e.g. a query for "ORG" to a name server serving "example.ORG"), in which case QNAME is at least known to exist, or it may be completely unrelated to any of the zones present.

Message types other than QUERY (Opcode 0) may also appear but are only discussed in Appendix A.

3. Causes of Unsolicited Queries

There are various causes for unsolicited DNS queries and it might be impossible to find and list all of them. Therefore the following list is most likely incomplete.

3.1. Lame Delegations

Lame delegations [RFC1912][RFC4697] are a common operational problem. They direct DNS queries at name servers that are meant to be authoritative for a zone, but cannot serve it authoritatively for a variety of reasons beyond the scope of this discussion. A lame delegation might be due to an NS RR in the delegating zone as well as an NS RR in the delegated zone itself.
3.2. Taking a Server for a Resolver

Enterprises and ISPs with end customers usually provide for DNS configuration information during session initiation, by DHCP or other protocols. Amongst those parameters are "name servers" to use by the users’ or customers’ end systems. The term "name servers" is ambiguous in this case, since what is really offered is the address (or are the addresses) of full (recursive) resolvers that are able and willing to accept and act upon the end systems’ DNS queries. Sometimes end users feel the need to circumvent the default configuration provided as explained above and manually configure the resolver addresses into their stub resolvers. Popular candidates are the "name servers responsible for the Example ISP", i.e., Example’s authoritative name servers. In similar scenarios, random ISPs’ or enterprises’ authoritative name servers are selected just for being well known or traded as being "good name servers". Following best practice, these authoritative name servers do not offer recursion, but will still see many unsolicited queries [RFC4697].

These queries usually have the RD bit set.

3.3. Probing

Some load balancing systems or content delivery networks try to dynamically respond to DNS queries with A RRSets preferring the address(es) "closest" to the requestor. Proximity tests sometimes involve DNS queries destined either to the requesting recursive name server or to one of the authoritative servers for the requestor’s zone (determined by reverse mapping). QNAMEs in these queries vary between random strings and the root (".").

3.4. Configuration or Implementation Problems

Typographic errors like mistyped addresses in resolver configurations or zone files (e.g., giving a wrong address for a name server in authoritative or glue data) can misdirect DNS traffic.

Missing checksums may let corrupt DNS queries pass undetected, which may lead to unexpected QCLASS, QTYPE or QNAME values, amongst others.

Implementation faults or configuration errors may lead to a QCLASS of ANY.

3.5. Debugging

Some queries will be due to debugging or research, i.e., they are either manually initiated or generated by a debugging or surveying script. This includes queries that are meant to check the
availability of a certain zone as well as host identification queries [RFC4892] and those used for DNS fingerprinting [FPDNS].

3.6. Attack Traffic

DNS traffic aimed at authoritative or recursive servers or anywhere else for the sole purpose of resource exhaustion or Denial of Service (DoS) is out of the scope of this document.

4. Response Variants

When constructing a response to an unsolicited query, care must be taken not to disturb the correct use of the responding server. Especially any kind of response should not degrade the service for those zones the server is actively able and willing to serve. This includes having the server marked as non-responsive or ‘down’ by remote resolvers. On the other hand it is not useful to invest too much effort into these responses, e.g. by trying to satisfy requests for recursion or by automatically making the server authoritative for zones that are delegated lame.

No Response might be sent at all. This will lead to a timeout at the resolver and may make the responsible administrator aware of the configuration issue. Silence is also used to throttle high volume query streams. However, this reaction may indicate to the querying entity that the server is not available at all and thus may degrade service for the zones served authoritatively. Not sending a response at all also opens the window for a spoofing attacker, where this is relevant.

Sink Delegations consist of a large set of NS records which each point to several unreachable IP addresses. Neither the names nor the addresses should interfere with any in production system. This type of defense can be used to time out query streams for a single QNAME or a whole domain.

DNS Error Responses often carry a DNS RCODE for "Server Failure" (2) or "Refused" (5). In the case of QCLASS other than IN, sometimes "Not Implemented" (4) is seen as well. These responses are short since they do not carry any RRSets [RFC2181] and may be rate limited. However, only a stateful resolver will be able to skip the server based on this information and some resolvers even repeat the DNS query instantaneously.
Best Effort Responses are based on best knowledge the responding server has and, consistent with algorithm 4.3.2 in [RFC1034], usually appear as "upward referrals". These responses point at a higher level in the DNS tree (most often this is the NS RRSet for the root zone) and serve no practical purpose in that they do not constitute progress in the resolution process. This very pattern can, however, be recognized by the querying resolver. "Upward referrals" to the root can often be easily triggered and therefore due to their size bear some risk of abuse in amplification attacks. Upward referrals are NOT RECOMMENDED.

Defensive Negative Responses authoritatively indicate either a name error (RCODE 3) for QNAME or the absence of any RRSet matching QTYPE to the querier. The SOA RR in the response usually signals a short negative TTL [RFC2308]. The intent of these responses is to induce errors on the side of the requestors to make them aware of a configuration problem. This may or may not work, since a query may be part of a chain of queries along a DNS search path, where negative responses will just be ignored. Negative responses might be able to throttle high volume query streams better than other DNS error responses.

Defensive Positive Responses send back an A RR at least for QTYPE=A. They are meant to throttle high volume query streams and usually either point to a website that notifies of a configuration error or to the loopback address. These responses are intrusive to a certain extent (as are the queries triggering them) and might have operational and legal implications. The AA bit may or may not be set. In an attempt to override an NS RRSet in a resolver’s cache, these responses may have NS RRSets in their authority section pointing to unreachable name servers (to increase resolution time) or the loopback interface (to keep traffic local to the requestor).

All of the responses above may be sent with a delay to discourage the further use of the server, assuming the server selection follows section 7.2 of [RFC1034]. This may again have a negative side effect on the service to the remaining zones on the same server.

A server might send different responses depending on whether or not the RD bit was set in the query. However, even at an authoritative server not all queries with RD=1 will be unsolicited. Most full (iterative) resolvers will clear the RD bit when sending queries, but today’s DNS traffic shows that some don’t.
5. Security Considerations

This document deals with unsolicited DNS queries that may lead to resource consumption on the server side. Using wrong, unwilling or untrusted resolvers for DNS name resolution exposes the user to the risk of DNS spoofing. Defensive responses as described above may lead to technical problems at the resolver side and may also have legal implications. Defensive responses cannot be secured by Secure DNS [RFC4033] and will lead to validation failures.

"Upward referrals" can be abused in reflection or amplification attacks.

The appendix mentions two scenarios that can lead to an endless back and forth of DNS packets between two name servers.

(This section needs more work.)

6. IANA Considerations

This document does not propose any new IANA registry nor does it ask for any allocation from an existing IANA registry.

7. Acknowledgements

The author would like to thank Jaap Akkerhuis and Danny Thomas for their review and helpful input. Jon Lewis suggested the sink delegations on the NANOG list.

8. References

8.1. Normative References


8.2. Informative References


[RFC4697] Larson, M. and P. Barber, "Observed DNS Resolution
DNS messages are distinguished by Opcode and QR bit. DNS queries have an Opcode of 0 and the QR bit cleared.

Responses should not be sent for messages with the QR bit set [I-D.arends-dnsext-qr-clarification].

FORMERR or NOTIMP responses should be sent for unknown or obsoleted Opcodes [RFC3425].

Certain UDP based services can be exploited to provide a steady back and forth of unrecognized message and error response. If the advise given above is followed, only services keeping the "QR bit" (MSB in the third octet of the payload [RFC1035]) unset can be abused. This includes, e.g., daytime [RFC0867] and chargen [RFC0864], but not the echo protocol [RFC0862]. Some implementations rate limit error responses to mitigate this attack.

Messages types NOTIFY and UPDATE are in wider use and will be addressed separately:

A.1. NOTIFY

[RFC1996] only deals with the case of NOTIFY messages received from unknown masters. Sometimes, a receiving name server might not be authoritative for the zone. That means the NS RR (or an explicit configuration directive) that led to the NOTIFY message is misplaced. In these cases sending a REFUSED response may help identifying the problem at the source.

A.2. Dynamic Updates

Root and Toplevel Domain (TLD) name servers as well as those authoritative for zones high in the IN-ADDR.ARPA tree see a lot of
UPDATE requests [RFC4697].

Sections 4.5 and 4.6 of [RFC2136] describe how a conforming client is supposed to react to DNS response codes: SERVFAIL, NOTIMP, silence or ICMP error messages are interpreted as a per server failure, where REFUSED should prevent further UPDATE attempts.

Appendix B. Document Revision History

This section is to be removed should the draft be published.

B.1. Changes from -02 to -03

Updated references.

Expanded on upward referrals.

B.2. Changes from -01 to -02

Expanded Security Considerations.

Minor edits.

B.3. Changes from -00 to -01

Expanded on Defensive Responses.

Added Probing and Attack Traffic.

Appendix A (non-query messages) added.

B.4. Initial Document

First draft

Author’s Address

Peter Koch
DENIC eG
Kaiserstrasse 75-77
Frankfurt 60329
DE

Phone: +49 69 27235 0
Email: pk@DENIC.DE