Identifying and Reacting to Unsolicited DNS Queries

draft-koch-dns-unsolicited-queries-00

1. Introduction

Authoritative name servers should see Domain Name System (DNS) queries directed towards authoritative name servers. It identifies reasons for the existence of these queries and lists some existing and proposed reactions.
queries only for domain names within or below zones they are authoritative for. Responses are either positive responses (consisting of RRSets), negative responses (either name error 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" below. This term is not intended to have any legal meaning or implication. Instead it should express that the usual DNS delegation and resolution process does not lead to those queries given the information the server operator is aware of.

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. It may, at a later stage, include recommendations in favor of or against certain kinds of responses.

This document only deals with unsolicited queries directed towards authoritative name servers. Abusive DNS queries for amplification or reflection attacks are described in [I-D.ietf-dnsop-reflectors-are-evil]. While the term "authoritative server" is not useful per se without naming for which zone(s) the server is authoritative, it is meant to express that the server does not offer DNS recursion for any client. Terminology may improve in future versions of this draft.

Comments should be directed at the author.

(This is an early version and thus will not pass the ID nits test.)

2. Types of Unsolicited Queries

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

QTYPE might be unexpected, but if a server is authoritative for a certain zone in a particular class, a query for any QTYPE 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]. Then there are obviously strange queries, e.g. for names of nameservers, where only A or AAAA queries make sense, but these are out of the scope of this document.
QCLASS is expected to be IN, the only class widely used on the Internet. All other classes are wrong in DNS queries, except for QCLASS=* (or ANY), which matches any class, including IN. While these queries can be answered, the AA bit can never be set as per section 3.7.1 of [RFC1034].

QNAME should fall into or below any of the zones served authoritatively. If the QNAME is not matched by any of the zones, it may be for 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.

Other messages types, like NOTIFY [RFC1996] and UPDATE [RFC2136], may also appear but are out of the scope of this document.

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] are a common operational problem. They direct DNS queries to 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. A special case is address space reuse where an NS RR points to a name that does not belong to the authoritative server but resolves to one of its IP addresses.

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 kind of an unfortunate choice since what is really offered is the address (or are the addresses) of full resolvers that are able and willing to accept and act upon the end systems’ DNS queries. Sometimes end users (or helpful third parties) feel the need to circumvent the default configuration provided as explained above and manually configure the resolver addresses into their stub resolvers. Primary candidates are often 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". Being really good, these authoritative name servers do not offer recursion and will see many unsolicited queries [I-D.ietf-dnsop-bad-dns-res].

These queries usually have the RD bit set.

3.3. Configuration or Implementation Problems

Sometimes it is as simple as that: mistyped addresses in resolver configurations or zone files misdirect traffic.

Missing check sums 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 QLASS of ANY.

3.4. 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 [I-D.ietf-dnsop-serverid] and those used for DNS fingerprinting [FPDNS].

3.5. Attack Traffic

... 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’. 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 and thus may degrade service for the zones served authoritatively.

DNS Error Responses usually carry a DNS RCODE for server failure (2) or refused (5). In the case of QLASS 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 may include "upward referrals", often referrals for the root domain. These referrals serve no practical purpose in that they do not constitute progress in the resolution process. "Upward referrals" point at a higher level in the DNS tree and can be rather huge.

Defensive Negative Responses authoritatively indicate either a name error (RCODE=3) or the absense of the QTYPE (NOERROR/NODATA) 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 legal implications.

A server might choose different responses for queries with the RD bit set. 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.

{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. References

7.1. Normative References


7.2. Informative References

[FPDNS] Schlyter, J. and R. Arends, "fpdns - Fingerprinting DNS Servers".


Appendix A. Document Revision History

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

A.1. Initial Document

First draft
Author’s Address

Peter Koch
DENIC eG
Wiesenhuettenplatz 26
Frankfurt  60329
DE

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

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.