DNSOP Working Group
Internet-Draft
Updates: 6195 (if approved)
Intended status: Standards Track
Expires: January 7, 2020

W. Krecicki
E. Hunt
D. Mahoney
ISC

July 6, 2019

Domain Name System (DNS) Resource Record types for transferring covert information from primary to secondaries
draft-krecicki-dns-covert-00

Abstract

The Domain Name System (DNS) Resource Record TYPEs IANA registry reserves the range 128-255 for Q-TYPEs and Meta-TYPEs [RFC6895] - Resource Records that can only be queried for or contain transient data associated with a particular DNS message.

This document reserves a range of RR TYPE numbers for Covert-TYPEs - types that are an integral part of the zone but cannot be accessed via a normal QUERY operation.

Uses for such records could include zone comments that are transferrable with the zone, expiry times for dynamically updated records, or Zone Signing Keys for inline signing. This document, however, does not define any specific Covert RR types.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Domain Name System (DNS) has no mechanism for sending control information in-band when transferring zone data from primary to secondary servers. This document specifies a range of Resource Record TYPEs that can be used for this purpose. Covert Resource Records can be transferred with the zone during zone transfer, but are not accessible by a normal QUERY operation. It also specifies a method for informing the primary server that the secondary understands Covert semantics, and can be relied upon not to disclose contents of Covert RRs to querying clients.

1.1. Definitions

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. Handling of Covert Resource Records

Covert Resource Records require special handling for both queries and zone transfers. This document does not define any specific Covert Resource Record types. When defined, those types may require additional handling on the server side as well; however, that is outside the scope of this document.

2.1. The COVERT-OK option

A client querying or a secondary transferring a zone from a primary server must explicitly signal its understanding of COVERT RR types. The mechanism for this is an EDNS option, with OPTION-CODE [TBD]. OPTION-LENGTH MUST be zero and OPTION-DATA MUST be empty.

2.2. Protection of Zone Transfers

If a secondary server requesting a zone transfer does not understand the Covert semantics, then it will serve the Covert records to its clients. Therefore a protection mechanism must be put in place so that secondary servers that do not understand Covert semantics do not receive Covert records.

If a server requesting a zone transfer understands Covert semantics, it MUST send a COVERT-OK option in the transfer request. If a primary server providing a zone transfer receives such a request, it then knows it can transfer the covert data and the secondary server will cooperate in protecting it.

If the primary server receives a zone transfer request without the COVERT-OK option it MUST NOT transfer the zone with Covert RRs. The default behaviour MUST be to refuse the transfer altogether, but an implementation MAY have a configuration option to allow transfer of the zone with Covert RRs stripped when transferring to a non-compliant secondary.

2.3. Authoritative server behaviour

Covert Resource Records might contain sensitive data; therefore, they MUST NOT be served to regular clients. An authoritative server queried for a Covert RR MUST return an answer as if the RRset the client client requested does not exist: NODATA if there are non-Covert Resource Records with the the same owner name or the node is an empty non-terminal, or NXDOMAIN otherwise.

The server MAY provide a mechanism allowing clients to query for Resource Records in the Covert range, but it MUST be protected by a mechanism disallowing access from general public (e.g. an ACL or TSIG authentication) and access MUST NOT be enabled by default. The server MUST verify that the query has the COVERT-OK option, and MUST NOT return COVERT records otherwise.

2.4. Recursive server behaviour

Recursive servers MUST NOT send the COVERT-OK option when iterating. If a COVERT record is received in response to an iterative query, it MUST NOT be cached, and it MUST NOT be returned to the client. If a recursive server receives a request for a COVERT record, it MAY iterate to verify whether the answer should be an NXDOMAIN or NODATA, or it MAY simply return a NODATA response immediately.

2.5. Interaction with DNSSEC

Covert Resource Records are not available for regular querying and are used only internally. Their presence in a zone should not, in any way, change the behaviour of that zone for ordinary clients. Therefore, when signing the zone, Covert Resource Records MUST be treated as if they do not exist: - Covert Records MUST NOT be signed. - Nodes that contain only Covert RRs and are not empty non-terminals MUST be ommited from NSEC [RFC4034] and NSEC3 [RFC5155] RR chains. - Any Covert RR types MUST NOT be included in the Type Bit Map field of an NSEC or NSEC3 RR.

2.6. Interaction with ZONEMD

TBD

2.7. UPDATE behaviour

Covert Resource Records MAY be submitted via UPDATE [RFC2136]. Servers SHOULD ignore prerequisites that specify Covert RR types, in order to conceal from untrusted clients the presence or absence of Covert RRs.

3. Update to RRTYPE Allocation Template

The RRTYPE Allocation Template from [RFC6895] is updated to contain a checkbox for Covert-RR:

```
      B.2 Kind of RR:  [ ] Data RR  [ ] Meta-RR  [ ] Covert-RR
```

4. Security considerations

Since Zone Transfers are unencrypted, the contents of Covert RRs might still be snooped by an on-path attacker. Protection against this kind of attack is outside the scope of this document, but it could be achieved by using, for example, a secure tunnel, a private network, or XFR over TLS transport.

5. IANA Considerations

IANA is requested to reserve range 61440-61695 (0xF000-0xF0FF) in the Resource Record TYPEs registry for Covert types. The procedure for registering RR types from [RFC6895] should be used.

IANA is requested to assign an EDNS option code to the COVERT-OK option.

6. Acknowledgments

TBD

7. 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>.

[RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, DOI 10.17487/RFC2136, April 1997, <https://www.rfc-editor.org/info/rfc2136>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC6895] Eastlake 3rd, D., "Domain Name System (DNS) IANA Considerations", BCP 42, RFC 6895, DOI 10.17487/RFC6895, April 2013, <https://www.rfc-editor.org/info/rfc6895>.

[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>.

Authors’ Addresses

Witold Krecicki
ISC
950 Charter St
Redwood City, CA 94063
US

Email: wpk@isc.org

Evan Hunt
ISC
950 Charter St
Redwood City, CA 94063
US

Email: each@isc.org

Dan Mahoney
ISC
950 Charter St
Redwood City, CA 94063
US

Email: dmahoney@isc.org