Black Lies Empty Non-Terminal Sentinel

draft-huque-dnsop-blacklies-ent-01

IETF 111 DNS Operations Working Group
Thursday, July 29th 2021
Shumon Huque

Propose another name for this later (not now please)

“Black Lies” - Compact DNSSEC denial of existence

- Described in an expired Internet draft from Cloudflare ~ March 2016:
  - https://datatracker.ietf.org/doc/html/draft-valsorda-dnsop-black-lies
- Never proposed for RFC publication, in any category (as far as I know).
- But becoming “widely” deployed amongst online signers:
  - 3 major commercial managed DNS providers: Cloudflare, NS1, and Amazon Route53
- Eliminates the concept of NXDOMAIN entirely!!
- This has some operational implications.

NXDOMAIN considered unnecessary?

- Clever hack or egregious hack?
- For names that don’t exist, a Black Lies implementation pretends that they do actually exist, but don’t have any data associated with the queried type.
- i.e. they return NODATA answers (NOERROR response code, an empty ANSWER section)
- Stated rationale:
    - **More compact answers**. A signed NODATA response requires just 1 NSEC record (and corresponding signature).
    - **Higher performance**: only 1 online cryptographic signing operation is needed.
    - By contrast, an NXDOMAIN response requires up to 2 NSEC or up to 3 NSEC3 records, and their corresponding signatures.

Operational Implications?

- For typical end user applications, probably nothing; a NODATA response is treated mostly identically to NXDOMAIN.
- But a variety of diagnostic, troubleshooting, traffic characterization, & provisioning tools may need adaptations to correctly deal with this protocol.
- Especially tools that rely on the correctness of the DNS Response Code.
  - Arguably, the RCODE should not be relied on, because it is unauthenticated.
  - But then we must infer non-existence of a name from signed data in the response (namely, NSEC records)
  - Can this inference be reliably drawn with Black Lies?

NXDOMAIN Response

```
$ dig +dnssec nxd.blah.sfdcsd.net. AAAA

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3913
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; QUESTION SECTION:
;nxd.blah.sfdcsd.net.     IN    AAAA

;; AUTHORITY SECTION:
sfdcsd.net.     1799    IN    SOA    dns1.p08.nsone.net. hostmaster.nsone.net.
1619363158 43200 7200 1209600 3600
sfdcsd.net.     1799    IN    RRSIG    SOA 13 2 3600 20210728145830 20210726145830 5986
sfdcsd.net. 8yFF++j9XBPARG+4jcZ/w0IvkVgPeS0eU5n3jS7d6RSFPQcO2k+9oU5V
3H3aev8Qcj0+7m5ht1Z4oaXkZLFclA==
nxd.blah.sfdcsd.net.    3599    IN    NSEC    \000.nxd.blah.sfdcsd.net. RRSIG NSEC
nxd.blah.sfdcsd.net.    3599    IN    RRSIG    NSEC 13 4 3600 20210728145830
20210726145830 5986 sfdcsd.net. TK5ccSxJ8Dt5oHmLi/6cykmglsjT2dMwZAnlbCfdsdN8DxXpu4wULBy9
k/ws0sECMh7AQcs54VJAR1W/XZCFwA==
```

Empty Non-Terminal Response - current

```
$ dig +dnssec ent1.sfdcsd.net. AAAA

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3727
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; QUESTION SECTION:
;ent1.sfdcsd.net.         IN    AAAA

;; AUTHORITY SECTION:
sfdcsd.net.     1799    IN    SOA    dns1.p08.nsone.net. hostmaster.nsone.net.
1619363158 43200 7200 1209600 3600
sfdcsd.net.     1799    IN    RRSIG    SOA 13 2 3600 20210728150036 20210726150036 44688
sfdcsd.net. xSv1lHZIPbKJ5f8pJf0Es0vSg+mr0SFk37Nh1OabvD96UdncINFGxYWG
vDNDcK7jXqRw8cwOK5jjCI8PWsx50w==
ent1.sfdcsd.net.    3599    IN    NSEC    \000.ent1.sfdcsd.net. RRSIG NSEC
ent1.sfdcsd.net.    3599    IN    RRSIG    NSEC 13 3 3600 20210728150036 20210726150036
44688 sfdcsd.net. UElkkdTBMg00mu6v0HFMkEc89IjNNbMg6C4zsBv2RaFsHJFI455oHhaA
3L0rxhuiKW0//pXWHjOx9iwVaIeTcA==
```

Distinguish ENT from NXDOMAIN

- Empty Non-Terminals (ENT) are names that have no resource record type associated with them, but have descendant names that do.
- In the described Black Lies spec, they are indistinguishable from non-existent names, because they have the same type bitmap (“NSEC RRSIG”) in the NSEC record.
- To distinguish them, we propose that implementations add a new synthetic RR type to the NSEC type bitmap for ENT responses only
    - This is deployed in the field today by NS1, using private use RR type# 65281 (Acknowledge Jan Vcelak).
    - We could request an official RR type# allocation.
    - Speaking to another vendor about implementing this too.

Empty Non-Terminal Response - enhanced

```
$ dig8 +nostats +dnssec ent1.sfdcsd.net. AAAA

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3727
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; QUESTION SECTION:
;ent1.sfdcsd.net.         IN    AAAA

;; AUTHORITY SECTION:
sfdcsd.net.     1799    IN    SOA    dns1.p08.nsone.net. hostmaster.nsone.net.
1619363158 43200 7200 1209600 3600
sfdcsd.net.     1799    IN    RRSIG    SOA 13 2 3600 20210728150036 20210726150036 44688
sfdcsd.net. xSv1lHZIPbKJ5f8pJf0Es0vSg+mr0SFk37Nh1OabvD96UdncINFGxYWG
vDNDcK7jXqRw8cwOK5jjCI8PWsx50w==
ent1.sfdcsd.net.    3599    IN    NSEC    \000.ent1.sfdcsd.net. RRSIG NSEC TYPE65281
ent1.sfdcsd.net.    3599    IN    RRSIG    NSEC 13 3 3600 20210728150036 20210726150036
44688 sfdcsd.net. UElkkdTBMg00mu6v0HFMkEc89IjNNbMg6C4zsBv2RaFsHJFI455oHhaA
3L0rxhuiKW0//pXWHjOx9iwVaIeTcA==
```

Code to infer NXDOMAIN

- Sample code to infer Black Lies NXDOMAIN:
    - https://github.com/shuque/blrcode

What next?

- Black Lies is deployed in the field - it should have some sort of stable published reference (even if IETF dnsop does not bless it).
- draft-huque-dnsop-blacklies-ent is also deployed in the field and should have a published reference.
- Attempt to publish both as Informational RFCs? (how? ISE?)
- Add the protocol description from 2016 to draft-huque-dnsop-blacklies-ent, and publish only that as Informational?
- Let this draft expire as well and move on?
- Something else?
- And should we request an official RR type allocation?