NSEC type bitmaps non-compliance survey

Petr Špaček

2021-11-30

https://www.isc.org

Type Bitmap: Precise – Optimal

- `$ dig +dnssec users.isc.org TLSA`

  `users.isc.org. NSEC _443._tcp.…`

  `A ~~CNAME~~ ~~SOA~~ … RRSIG NSEC …`

All good

- `$ dig +dnssec users.isc.org A`

  `users.isc.org. A 149.20.1.88 …`

- Optimal for aggressive use of cache (RFC 8198)

Type Bitmap: Super-set – Works

- `$ dig +dnssec cloudflare.com` **`TLSA`**

  `cloudflare.com. NSEC\000.cloudflare.com. A NS SOA … SSHFP RRSIG NSEC DNSKEY ~~TLSA~~` **`SMIMEA`** …

  Not present in type bitmap only when queried for – works

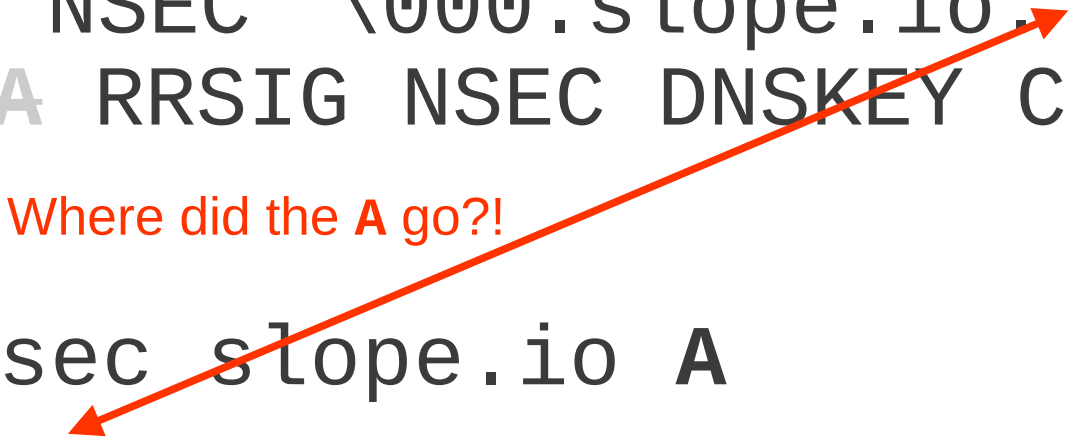
- `$ dig +dnssec cloudflare.com` **`SMIMEA`**

  `cloudflare.com. NSEC\000.cloudflare.com. A NS SOA … SSHFP RRSIG NSEC DNSKEY ~~SMIMEA~~` **`TLSA`** …

  - https://blog.cloudflare.com/black-lies/

Type Bitmap: Subset – Broken

- `$ dig +dnssec slope.io` **`AAAA`**
- `slope.io.  NSEC  \000.slope.io. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY CDS CDNSKEY`



- `$ dig +dnssec slope.io` **`A`**

  `slope.io.  A  3.13.31.214`

  `slope.io.  RRSIG  A ...`

Not present in type bitmap ***even though an RR set with RRSIG exists*** – poisons cache! Allows replay attacks!

What do broken bitmaps cause?

- Break aggressive use of cache (RFC 8198)
  - Knot Resolver, PowerDNS Recursor, Unbound, BIND soon, Google Public DNS
- Create hidden security vulnerability!
  - Enable replay attack to securely deny an (otherwise existing) RR type!

Survey data set

- Tranco list
  - Version VLXN
  - 1 M domains
- Scan for DS records
  - 35 668 domains with DS
  - 3.57 % of 1 M

NSEC* type bitmap discrepancies

- `dnsviz probe <domain with DS>`
  `| dnsviz grok`
  `| fgrep`
  `EXISTING_TYPE_NOT_IN_BITMAP`
- 187 broken domains / 35 668 with DS
  - 0.52 % of signed domains
  - 0.0187 % of Tranco 1M
  - Tranco rank 1005 and "less important"

NSEC(3) type bitmap discrepancies

- 35 domains with broken NSEC
  - ~ 0.1 % of signed domains
- 152 domains broken NSEC3
  - ~ 0.42 % of signed domains

Affected Operators – NSEC

- ArvaCloud ~ 17 %
- DNSimple ~ 75 %
- Alibaba DNS ~ 6 %
- NIC.br ~ 1 domain – fixed in 2 hours!
- Each slightly different type of breakage
- Clearly custom code
- Notified via e-mail yesterday

Affected Operators – NSEC3

- treasury.gov ~ 15 %
- All the rest <= 6 domains
- An appliance(s) problem(s)?
  - https://en.blog.nic.cz/2019/07/10/error-in-dnssec-implementation-on-f5-big-ip-load-balancers/ strikes again?

Closing words

- BIND 9.18
  - Plans to enable RFC 8198 for NSEC **by default**
  - "Soon"
- Fix your domains
  - … before they break even more

Thank you!

- Main website: https://www.isc.org
- Software downloads: https://www.isc.org/download or https://downloads.isc.org
- Presentations: https://www.isc.org/presentations
- Main GitLab: https://gitlab.isc.org

References

- Tranco list: Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. 2019. "Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019). https://doi.org/10.14722/ndss.2019.23386