ATHENE
National Research Center
for Applied Cybersecurity

Attacking with Something That Does Not Exist: ‘Proof of Non-Existence’ Can Exhaust DNS Resolver CPU

Authors

Olivia Gruza, Elias Heftrig, Oliver Jacobsen, Haya Schulmann, Niklas Vogel, and Michael Waidner

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Fraunhofer SIT

TECHNISCHE UNIVERSITÄT DARMSTADT

Contents

Outline

Analysis of the NSEC3-Encloser attack (CVE-2023-50868), which leads to CPU load and DoS on DNS resolvers.

Key Contributions:

- A tool for automated evaluation of the attack
- Investigate the attack beyond proof-of-concept in the CVE.
- First evaluation of an attack that exploits NSEC3 records for creating a load on DNS resolvers.

Background: DNS

Domain **N**ame **S**ystem RFC1034:
Hierarchical, distributed database to map human-readable domain names (e.g., www.example.com) to arbitrary resource records, foremost IP-addresses and server addresses.

Core infrastructure of the internet on which other services rely on.

```
                            |
                            |
          +-----------------+------------------------+
          |                 |                        |
         COM               DE                      ARPA
          |                 |                        |
          |                 |                        |
     +----+---+      +------+--------+     +------+------+-----+
     |        |      |               |     |      |            |
  EXAMPLE  USENIX  ATHENE-CENTER  UNI-FRANKFURT  IN-ADDR  SRI-NIC  ACC
```

Background: DNS

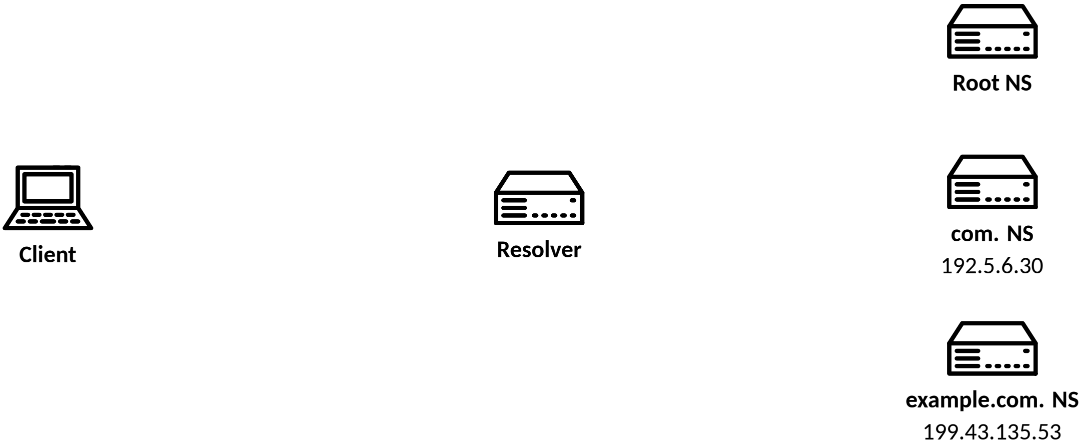


Figure: DNS Recursive Request Example.

Background: DNS

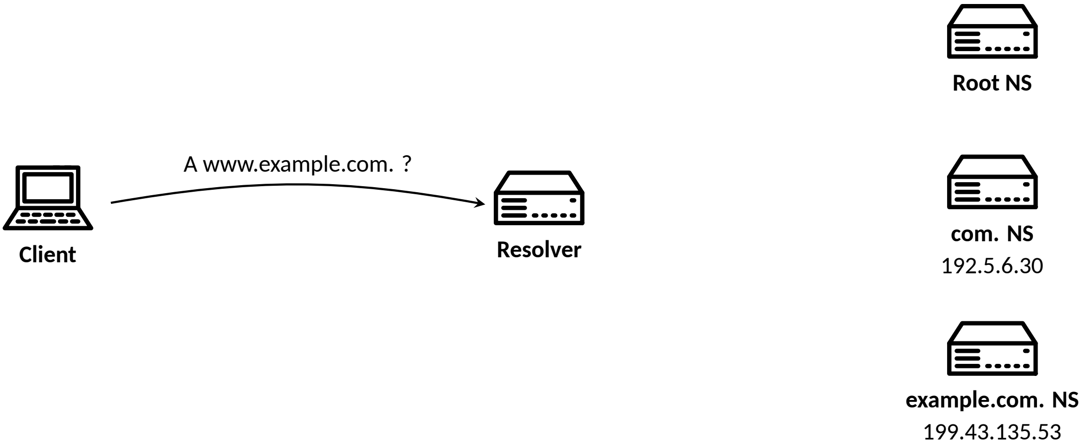


Figure: DNS Recursive Request Example.

Background: DNS

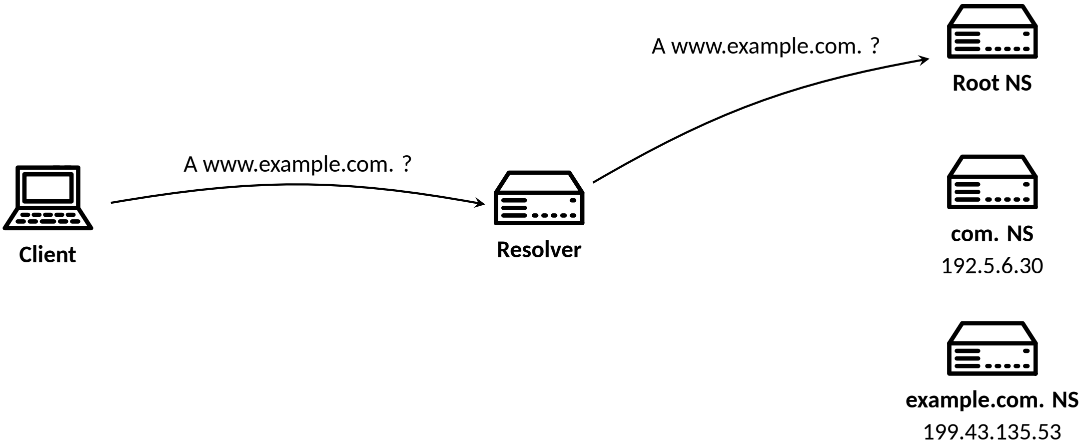


Figure: DNS Recursive Request Example.

Background: DNS

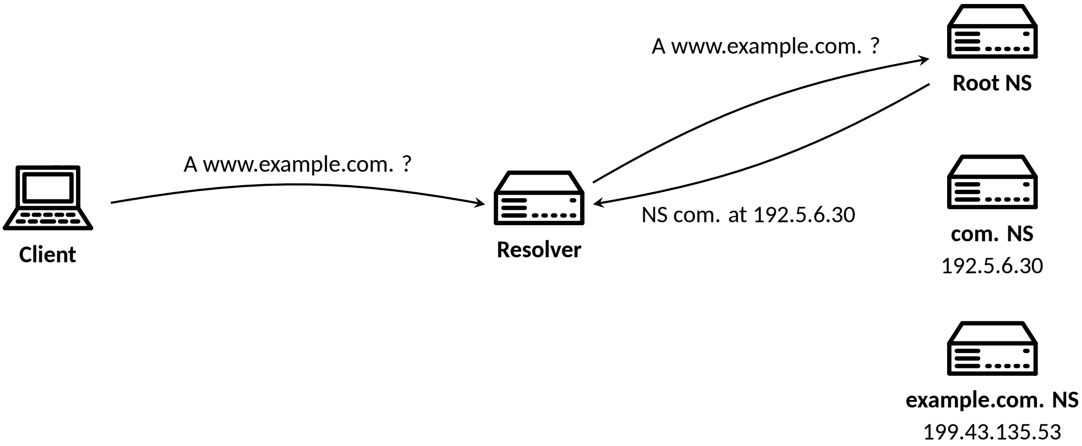


Figure: DNS Recursive Request Example.

Background: DNS

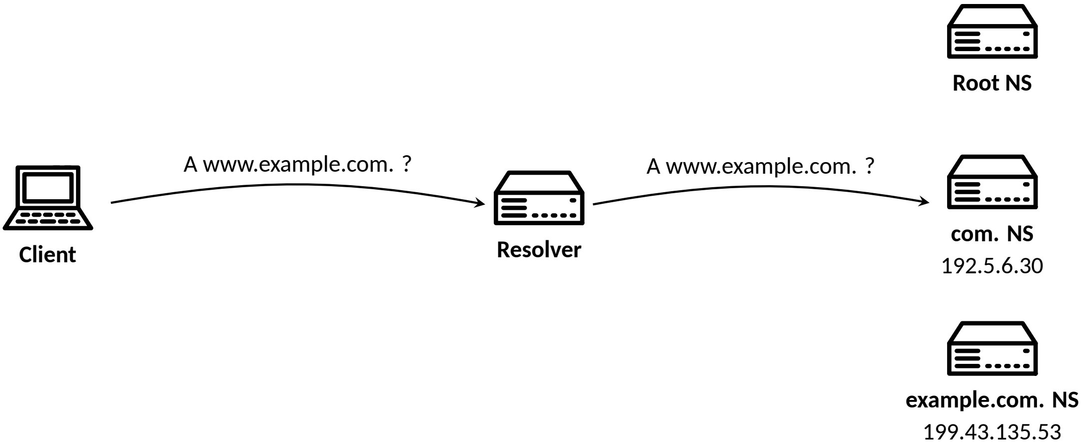


Figure: DNS Recursive Request Example.

Background: DNS

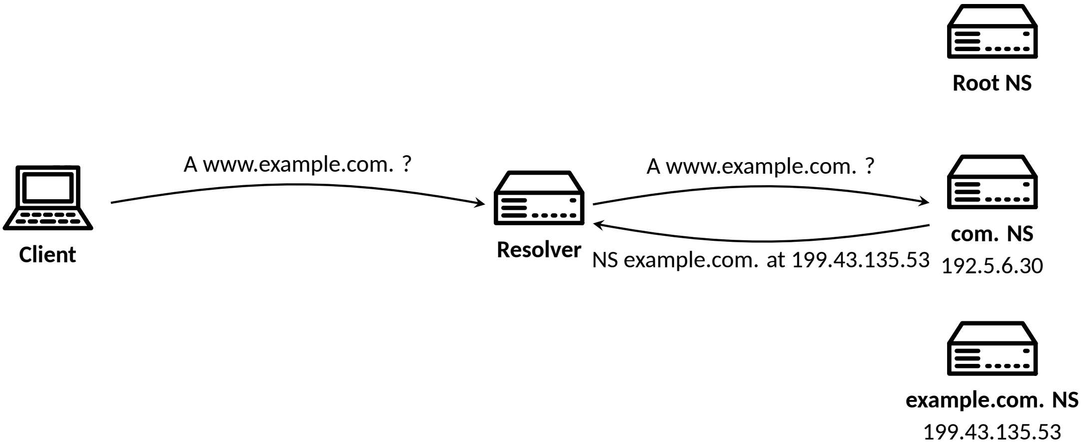


Figure: DNS Recursive Request Example.

Background: DNS

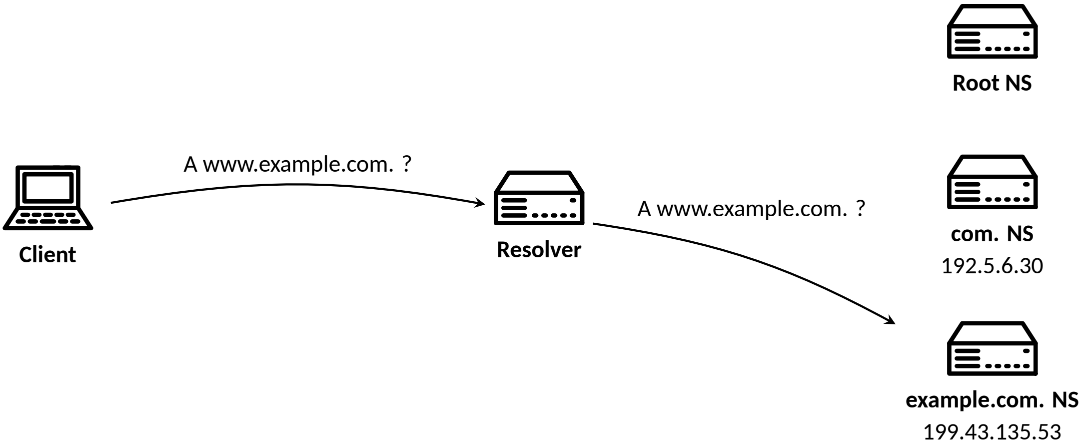


Figure: DNS Recursive Request Example.

Background: DNS

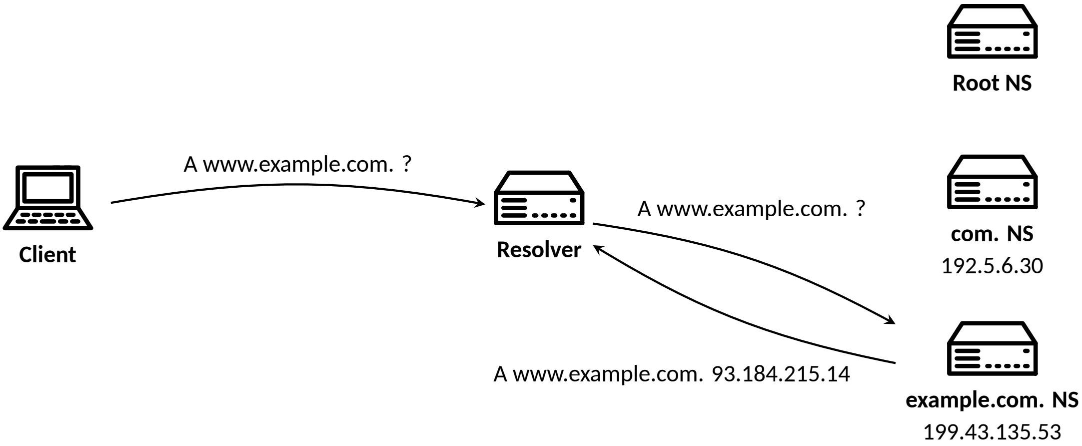


Figure: DNS Recursive Request Example.

Background: DNS

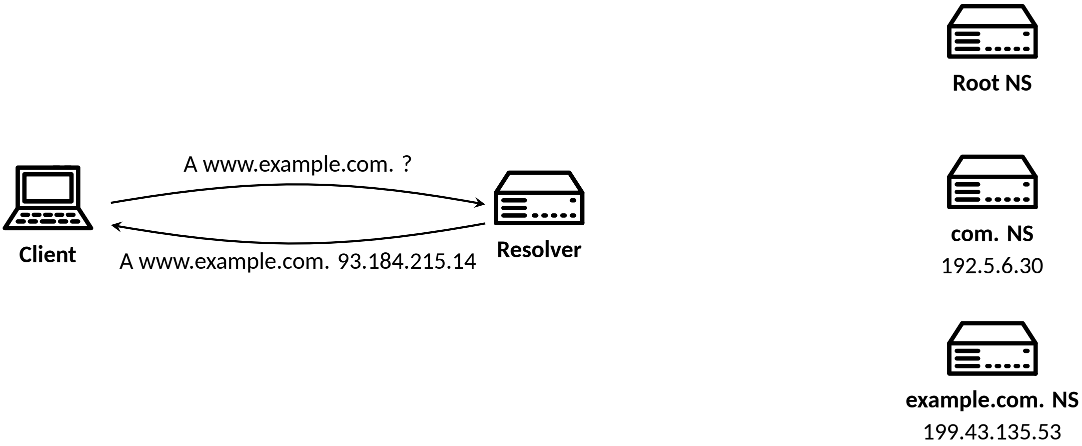


Figure: DNS Recursive Request Example.

Background: Proving Non-Existence in DNS

NSEC

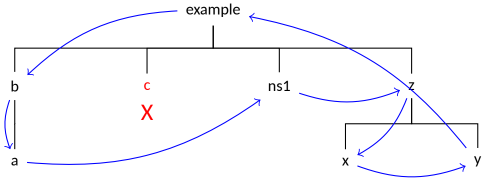
NSEC record links domain names in zone to its canonical successor.

Proves non-existence of domain names that fall inbetween.

e.g., `a.b.example. NSEC ns1.example.`

Problem:

Reveals zone tree via zone walking.



NSEC3

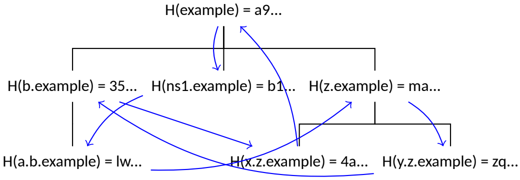
NSEC3 record links the hash of a domain name to the alphanumeric next hash in the zone.

Poves non-existence of any preimages to hashes in this range.

e.g., `lw...g4.example. NSEC3 ma...6e`

Advantage: Obfuscates zone tree.

Disadvantage: Requires more elaborate validation.



Background: NSEC3

Closest Encloser Proof

Proving non-existence resolver-side based on NSEC3 RRs: **Closest Encloser Proof**

E.g., proving `v.w.x.y.z.example.` $\notin$ `example.` zone requires finding a pair of encloser/next closer:

`v.w.x.y.z.example.`

- `z.example.` — existing encloser
- `y.z.example.` — non-existing next closer

Proof algorithm sequentially strips away labels until closest encloser is found:

1. Hash the name
2. Return NXDOMAIN if closest encloser identified
3. Remove fist label, goto 1.

Background: NSEC3

Parameters

NSEC3 allows zone operators to choose NSEC3 parameters in the NSEC3PARAM RR to harden against dictionary attacks.

Iterations

A number of how many times the hash needs to be re-hashed.

Salt

An up to 255-byte value that must be appended to the hashed value for each hash iteration.

Key Size	Iterations
1024	150
2048	1500
4096	2500

Table: Iterations Parameter Limits Are Based on Key Size

Background: NSEC3

Parameters

NSEC3 allows zone operators to choose NSEC3 parameters in the NSEC3PARAM RR to harden against dictionary attacks.

Iterations

A number of how many times the hash needs to be re-hashed.

Salt

An up to 255-byte value that must be appended to the hashed value for each hash iteration.

Expected closest encloser proof complexity:
$\mathcal{O}(\text{nr of labels} \cdot \text{iterations} \cdot \text{salt length})$

Key Size	Iterations
1024	150
2048	1500
4096	2500

Table: Iterations Parameter Limits Are Based on Key Size

NSEC3-Encloser Attack

CVE-2023-50868

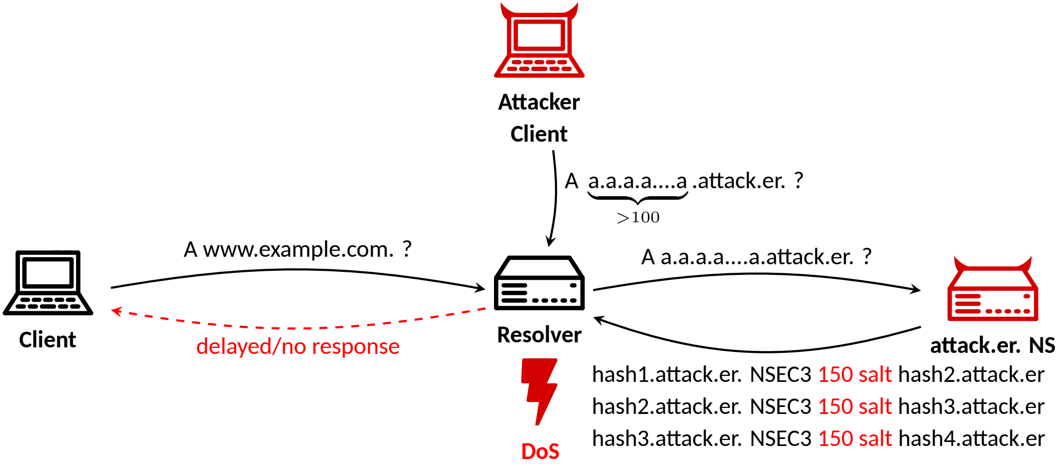


Figure: DNS NSEC3-Encloser Attack.

The issue is not new…

RFC9276: Guidance for NSEC3 Parameter Settings (Aug 2022)

Acknowledges for iterations:

- Attackers “likely [are] able to find most of the ”guessable” names despite any level of additional hashing iterations.”
- “Most names published in the DNS are rarely secret or unpredictable.”

Acknowledges for salt:

- “[N]o single pre-computed table works to speed up dictionary attacks against multiple target zones.”
- “This makes very frequent re-salting impractical and renders the additional salt field functionally useless.”

Recommends for validating resolvers:

- Resolvers are “encouraged to lower their default limit for returning SERVFAIL when processing NSEC3 parameters containing large iteration count values.”
- No concrete advice for handling salt.

Attack Evaluation

Zonfile Generator

- Generates keys and static zonefiles for reproducing the attack
- Allows generation of many different iterations and salt values for testing

https://github.com/Goethe-Universitat-Cybersecurity/NSEC3-Encloser-Attack

Setup

- Containerized resolvers running with one CPU and DNSSEC enabled
- NSD nameserver serving the attacker zones
- Self-developed attacker client

```
;; ZONE 'ATTACK.ER'

ATTACK.ER. 0 IN SOA NS1.ATTACK.ER. NS1.ATTACK.ER. 0 0 0 10 0

ATTACK.ER. 0 IN NS NS1.ATTACK.ER.

ATTACK.ER. 0 IN DS 35650 7 1 e8316...

ATTACK.ER. 0 IN DNSKEY 257 3 7 AwEA...
ATTACK.ER. 0 IN DNSKEY 256 3 7 AwEA...

ATTACK.ER. 0 IN NSEC3PARAM 1 0 150 -

HKHV...38AU.ATTACK.ER. 0 IN NSEC3 1 1 150 - HKHV...38B0

HKHV...38B0.ATTACK.ER. 0 IN NSEC3 1 1 150 - QCQC...7U45

NS1.ATTACK.ER 0 IN A 6.6.6.6

QCQC...7U45.ATTACK.ER. 0 IN NSEC3 1 1 150 - SN5U...89IT A RRSIG

SN5U...89IT.ATTACK.ER. 0 IN NSEC3 1 1 150 - SN5U...89IU NS SOA
    DS RRSIG DNSKEY NSEC3PARAM

SN5U...89IU.ATTACK.ER. 0 IN NSEC3 1 1 150 - HKHV...38AU

[...] ;; RRSIG records
```

Figure: Generated attack zonefile example.

Attack Evaluation

Resolver Implementations

Resolver	Version	Iteration Limit
Bind9	9.16.1	RFC5155
Bind9	9.18.12	150
Unbound	1.17.1	150
PowerDNS	4.8.2	150
Knot	5.6.0	150

Table: Resolver versions and iterations limits in the test setup.

Attack Evaluation
Parameter Iterations

Analysis of NSEC3 iterations on the CPU load.

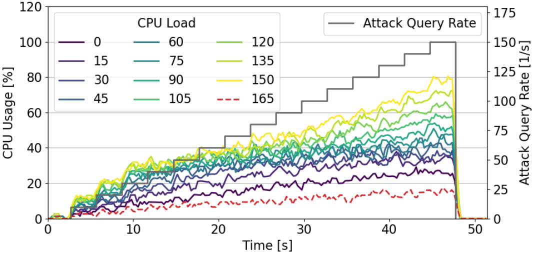


Figure: Unbound

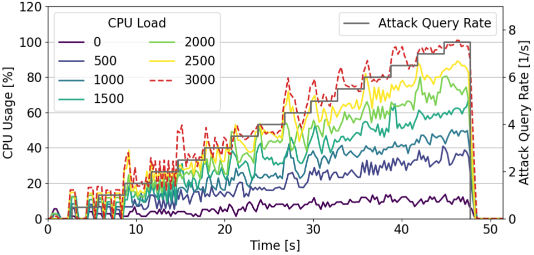


Figure: Bind9.16.1

Attack Evaluation

Parameter Iterations

Analysis of NSEC3 iterations on the CPU load using maximum (150/2500) iterations.

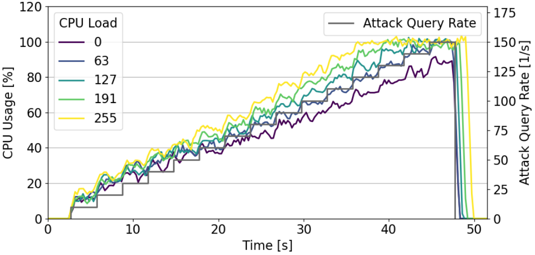


Figure: Unbound

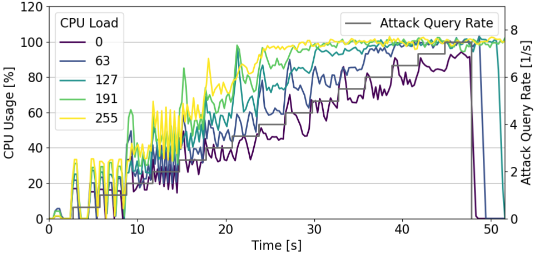


Figure: Bind9.16.1

Attack Evaluation

Comparative Analysis

Comparison of CPU workload between resolvers.

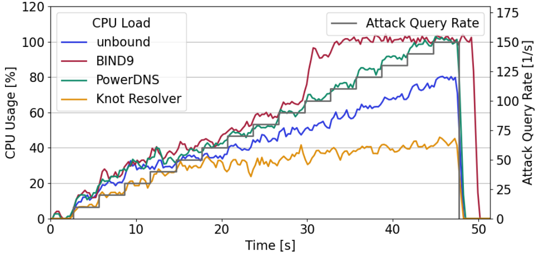


Figure: 150 iterations, 0 byte salt

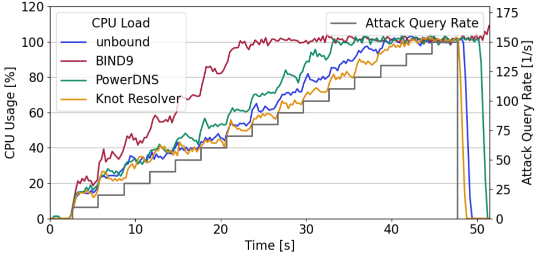


Figure: 150 iterations, 255 byte salt

Attack Evaluation
Benign Analysis

Evaluation of peak benign traffic drop rates under stress conditions.

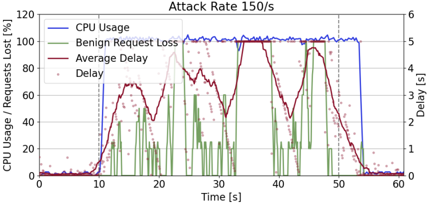


Figure: Unbound attacked with rate 150/s

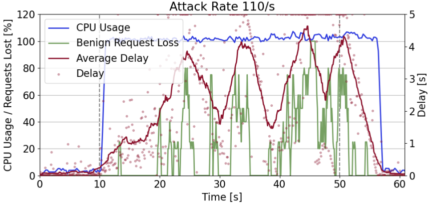


Figure: Bind9.18.12 attacked with rate 110/s

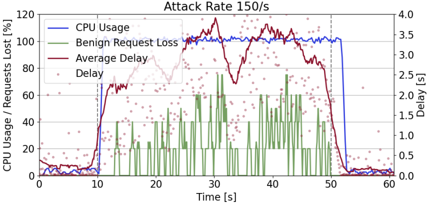


Figure: Knot attacked with rate 150/s

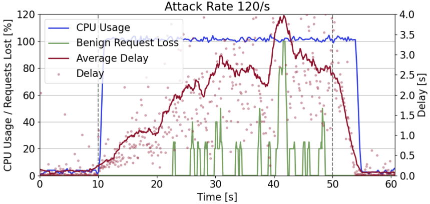


Figure: PowerDNS attacked with rate 120/s

Attack Evaluation

Measured Drop Rates

Resolver	Attack Rate	Total Loss Rate	Adjusted Loss Rate*
Bind9.18.12	150/s	5.10%	7.01%
Bind9.18.12	110/s	16.42%	22.99%
Unbound	150/s	**24.75**%	**34.66**%
PowerDNS	150/s	1.97%	2.76%
PowerDNS	120/s	5.62%	7.87%
Knot	150/s	12.87%	18.01%

(*Total loss rate relative to the attack duration)

Table: Measured peak client request loss rate with an attack over 40s, 150 iterations, and 255 byte salt.

Measurements of Signed Domains

Goal: Find out how NSEC3 is used in the internet and how the RFC9276 guidelines are applied.
Methodology: Query DNSSEC information of nameservers of the Tranco Top-1M domains (in the week following 2024-03-10).

Key insights:

- 66 339 (6.63%) of the Tranco Top-1M domains are signed.
- Of these, 27 761 (41.85%) use NSEC3 while 37 354 (56.31%) use NSEC.
- 21 522 (77.53%) of the domains using NSEC3 send records with iterations > 0 (median 5, maximum 500 iterations), 21 248 (76.54%) of the domains utilizing NSEC3 employ a salt (median 8, maximum 64 bytes).

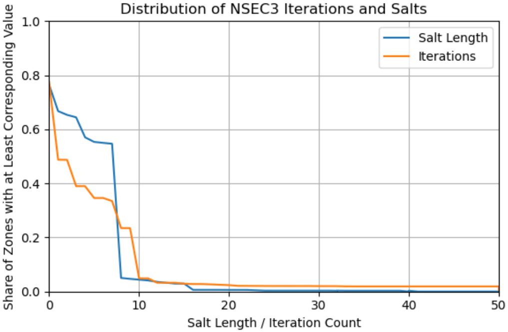


Figure: Share of zones which meet or exceed the configured Salt Length / Iteration Count in signed DNS zones.

Conclusion

- We performed the first evaluation of the attack and measured the impact on resolvers
- We developed a test setup to evaluate the impact of DNS DoS attacks on clients
- NSEC3-Encloser can exhaust resolver CPU with attack rate in the low hundreds
- There is impact on benign drop rates, causing up to 34.66% loss
- Overall, the impact is limited, since it requires high attack volumes for relatively limited impact. The attack is inferior to other attacks, such as KeyTrap.