Dissecting NSEC and NSEC3 Deployment in the Wild

DNS OARC 47 Workshop
November 9th 2026, Vancouver, Canada

Yizhe Zhang*, Hyeonmin Lee*, **Shumon Huque**, Yixin Sun

Overview

- Background
  - Authenticated Denial of Existence
  - NSEC
  - NSEC3
  - White Lies
  - Compact Denial of Existence (CDE)

- Our study:
  - How NSEC and NSEC3 are deployed in the wild?
  - Which variants are deployed?
  - How wildcard synthesis interact with NSEC/3 mechanism?

Authenticated Denial of Existence

- Proves a domain name or record type does not exist.
- Why it matters:
  - Forged negative answers can make existing names or record types appear absent.

- Resource Records:
  - NSEC (RFC 4033, 4034, 4035)
  - NSEC3 (RFC 5155)

- Minimally Covering Variants:
  - NSEC White Lies (RFC 4470)
  - NSEC3 White Lies (RFC 7129, Appendix B)
  - Compact Denial of Existence (RFC 9824)

NSEC Resource Records

Example zone:

```
a.example.org.    A       192.0.2.1
                  TXT     “this is record a”
d.example.org.    A       192.0.2.1
                  TXT     “this is record d”
```

RRSIG omitted for brevity.

Owner | Next owner | Type Bitmap

```
a.example.org.    NSEC    d.example.org.    A TXT RRSIG NSEC
```

NSEC NODATA Response

Prove a **query type** does not exist at a domain name.

Query:

```
$ dig    +dnssec       a.example.org.    AAAA
```

Answer:

```
;; ->>HEADER<<- opcode: QUERY,  status: NOERROR, id: 22185
(omitted)

;; AUTHORITY SECTION:
a.example.org. 3600   IN   NSEC     d.example.org.    A TXT RRSIG NSEC
a.example.org. 3600   IN   RRSIG    NSEC     <rdata omitted>
```

NOERROR + type bitmap indicate that the name exists, but the queried type does not.

NSEC NXDOMAIN Response

Prove a **query name** does not exist.

Query:

```
$ dig    +dnssec      b.example.org.    A
```

Answer:

```
;; ->>HEADER<<- opcode: QUERY,  status: NXDOMAIN, id: 22185
(omitted)

;; AUTHORITY SECTION:
a.example.org. 3600   IN   NSEC     d.example.org.    A TXT RRSIG NSEC
a.example.org. 3600   IN   RRSIG    NSEC     <rdata omitted>
example.org.   3600   IN   NSEC      a.example.org. NS SOA RRSIG NSEC DNSKEY
example.org.   3600   IN    RRSIG    NSEC    <rdata omitted>
```

NSEC3 Resource Records

Compute hash of each name in the zone.
Sort the hashes into a chain.
Put consecutive hashes in NSEC3 records.

Example zone:

```
a.example.org.    A       192.0.2.1
                  TXT     "this is record a"
d.example.org.    A       192.0.2.1
                  TXT     "this is record d"
```

RRSIG omitted for brevity.

```
hash(a.example.org.) -> 6HSUDPCUGOVCSU6RIB34SA6RM87TQM57
hash(d.example.org.) -> C8F0L4P2AJE6VRHQOAFS2TSKK0431LOB
```

Hash of Owner

alg, flags, iterations, salt

```
6HSUDPCUGOVCSU6RIB34SA6RM87TQM57 .example.org. NSEC3   1 0 0 -
C8F0L4P2AJE6VRHQOAFS2TSKK0431LOB   A TXT RRSIG
```

Next hash

Type Bitmap

Benefits:

- Mitigates straightforward zone enumeration by hashing domain names
- Supports Opt-Out for more scalable deployment in large delegation-centric zones

NSEC/3 Variant

- “Minimally covering” of NSEC/3
  - Synthesizes minimal NSEC/3 ranges on the fly, rather than using the actual before and after names in the zone
  - Effectively prevent zone enumeration attack
- Variant:
  - White Lies
    - Dynamically constructing a minimally covering of the non-existent name
  - Compact Denial of Existence
    - Always claim that the name exists, but doesn’t have any data associated with the queried record type (always have a NOERROR status code)
    - Lost the NXDOMAIN signal (pseudo type NXNAME has now been standardized in RFC 9824 to conclusively indicate non-existence of the name)

NSEC/3 White Lies

- Dynamically constructing a minimally covering of the non-existent name using an epsilon function.
- No standardized epsilon function -> **provider specific deployment.**

Query non-existence name: foo.example.org.

NSEC owner and next owner name can be:

```
fon\255.example.org.  3600    IN  NSEC    foo\000.example.org.
fon~.example.org.     3600    IN  NSEC    foo!.example.org.
```

NSEC3 owner and next owner name can be:

```
Hash(foo.example.org)->6HSUDPCUGOVCSU6RIB34SA6RM87TQM57
```

Hash - 1

```
6HSUDPCUGOVCSU6RIB34SA6RM87TQM56.example.org.  3600 IN  NSEC3
6HSUDPCUGOVCSU6RIB34SA6RM87TQM58
```

Hash + 1

Compact Denial of Existence (CDE)

- Always claim that **the name exists**, but doesn't have any data associated with queried record type.
- Benefit: minimizing both message size and computation cost

Query:

```
$ dig    +dnssec      b.example.org.    A
```

Answer:

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22185
(omitted)
```

Will always be NOERROR

```
;; AUTHORITY SECTION:
b.example.org. 3600   IN   NSEC     \000.b.example.org.   RRSIG NSEC NXNAME
```

Minimal covering of the next domain name.

Domain name that does not exist.

Since CDE lost the NXDOMAIN signal, the pseudo type NXNAME was standardized in RFC 9824 to indicate the name does not exist.

How Authenticated Denial of Existence are deployed in the wild?

- Datasets:
  - OpenINTEL Datasets (apex domains from the gTLDs, FQDNs from pop lists)
    - Three gTLDS: .com, .net, and .org
    - Four popularity lists: Umbrella, Tranco, Radar, and Majestic
  - www subdomain scanning:
    - Our own scanning using Google public resolver 8.8.8.8
- Scanning methodology:
  - AFSDB (deprecated) query type for (likely) non-existent domain name
    - Apex: 123-non-existence-domain-name.example.test.
    - www: 123-non-existence-domain-name.www.example.test.
- Data collection time:
  - One day snapshot: April 6, 2026, plus follow-on active scans

DNSSEC and NSEC/3 Adoption Rate

	Source domains (from OpenINTEL)							WWW subdomains (from our active prober)				
	SOA	w/ DNSKEY		NSEC		NSEC3		w/ DNSKEY	NSEC		NSEC3	
	#. Apex	#. Apex	%	#. Apex	%	#. Apex	%	#	#	%	#	%
.com	149,021,866	8,364,107	5.61%	1,577,074	18.86%	6,720,037	80.34%	8,364,107	1,463,427	17.50%	6,561,180	78.44%
.net	11,156,231	707,851	6.34%	160,534	22.68%	543,279	76.75%	707,851	155,078	21.91%	532,883	75.28%
.org	10,972,417	707,896	6.45%	146,299	20.67%	556,602	78.63%	707,896	140,760	19.88%	548,415	77.47%
	#. FQDN	#. FQDN	%	#. FQDN	%	#. FQDN	%	#	#	%	#	%
Umbrella	384,922	26,034	6.76%	16,251	62.42%	9,523	36.58%	20,731	13,004	62.73%	6,952	33.53%
Tranco	968,036	79,790	8.24%	49,080	61.51%	30,109	37.74%	71,512	42,812	59.87%	27,054	37.83%
Radar	1,137,219	102,067	8.98%	65,042	63.72%	36,246	35.51%	93,880	58,725	62.55%	33,327	35.50%
Majestic	946,890	75,863	8.01%	40,987	54.03%	34,296	45.21%	69,995	37,372	53.39%	31,237	44.63%

- In the gTLD zones, NSEC3 is dominant (> 75%).
- In the popularity-ranking zones, NSEC is dominant (~ 60%).
- Comparing to 2019 Study*: more than an order-of-magnitude increase
  - NSEC increased from 112K to 1.5M domains
  - NSEC3 increased from 725K to 6.7M domains

* Jonathan Demke and Casey Deccio. 2019. On DNSSEC Negative Responses,Lies, and Zone Size Detection.

NSEC/3 Resource Records Structure

	Source domains (from OpenINTEL)							WWW subdomains (from our active prober)						
	NSEC			NSEC3				NSEC			NSEC3			
#. RRs	1	2	3	1	2	3	4	1	2	3	1	2	3	4
.com	**97.85%**	2.14%	0.01%	12.05%	**44.61%**	43.34%	0.00%	**89.64%**	10.35%	0.01%	11.94%	**44.00%**	44.06%	0.00%
.net	**96.66%**	3.34%	0.01%	12.93%	**46.01%**	41.05%	0.00%	**89.56%**	10.44%	0.00%	12.78%	**45.48%**	41.74%	0.00%
.org	**97.06%**	2.94%	0.00%	11.72%	**44.72%**	43.56%	0.00%	**90.67%**	9.33%	0.00%	11.57%	**44.26%**	44.16%	0.00%
Umbrella	**92.83%**	7.17%	0.00%	4.91%	15.84%	**79.25%**	0.00%	**94.33%**	5.67%	0.00%	4.09%	14.86%	**81.06%**	0.00%
Tranco	**96.62%**	3.38%	0.00%	4.06%	17.31%	**78.63%**	0.01%	**95.90%**	4.10%	0.00%	3.40%	16.99%	**79.60%**	0.00%
Radar	**97.52%**	2.48%	0.00%	5.04%	18.63%	**76.32%**	0.01%	**96.48%**	3.52%	0.00%	4.21%	17.98%	**77.81%**	0.00%
Majestic	**96.74%**	3.25%	0.01%	5.25%	19.77%	**74.97%**	0.01%	**96.71%**	3.29%	0.01%	4.57%	19.38%	**76.05%**	0.00%

Count of NSEC/3 resource records (RRs) per response. Note that we only count NSEC/3 RRs, excluding accompanying records such as RRSIG or other auxiliary resource records.

- Authenticated denial of existence typically contain at most two NSEC or three NSEC3 records. We observe extra responses due to CNAME as shown in red square.

Top Name Server Providers

OpenINTEL				www			
NSEC		NSEC3		NSEC		NSEC3	
NS	%	NS	%	NS	%	NS	%
.com							
cloudflare	38.03%	googledomains	39.98%	cloudflare	36.13%	googledomains	41.65%
infomaniak	7.44%	wixdns	19.40%	infomaniak	7.94%	wixdns	19.61%
registrar-servers	5.82%	ovh	9.60%	registrar-servers	6.17%	spaceship	10.12%
domaincontrol	4.90%	one	3.97%	domaincontrol	5.17%	ovh	9.74%
register	4.73%	openprovider	2.88%	register	4.72%	one	3.97%
.net							
cloudflare	50.01%	googledomains	45.05%	cloudflare	50.98%	googledomains	46.64%
infomaniak	5.48%	wixdns	14.80%	infomaniak	5.61%	wixdns	14.84%
registrar-servers	4.81%	ovh	9.89%	registrar-servers	4.89%	ovh	9.96%
register	3.88%	one	3.83%	register	3.69%	spaceship	6.40%
domaincontrol	2.86%	openprovider	2.76%	domaincontrol	2.88%	one	3.82%
.org							
cloudflare	47.07%	googledomains	46.74%	cloudflare	48.10%	googledomains	48.16%
infomaniak	7.48%	wixdns	15.48%	infomaniak	7.71%	wixdns	15.51%
registrar-servers	5.24%	ovh	7.73%	registrar-servers	5.32%	spaceship	10.21%
domaincontrol	4.24%	one	3.08%	domaincontrol	4.32%	ovh	7.77%
register	2.78%	openprovider	2.24%	register	2.57%	one	3.07%

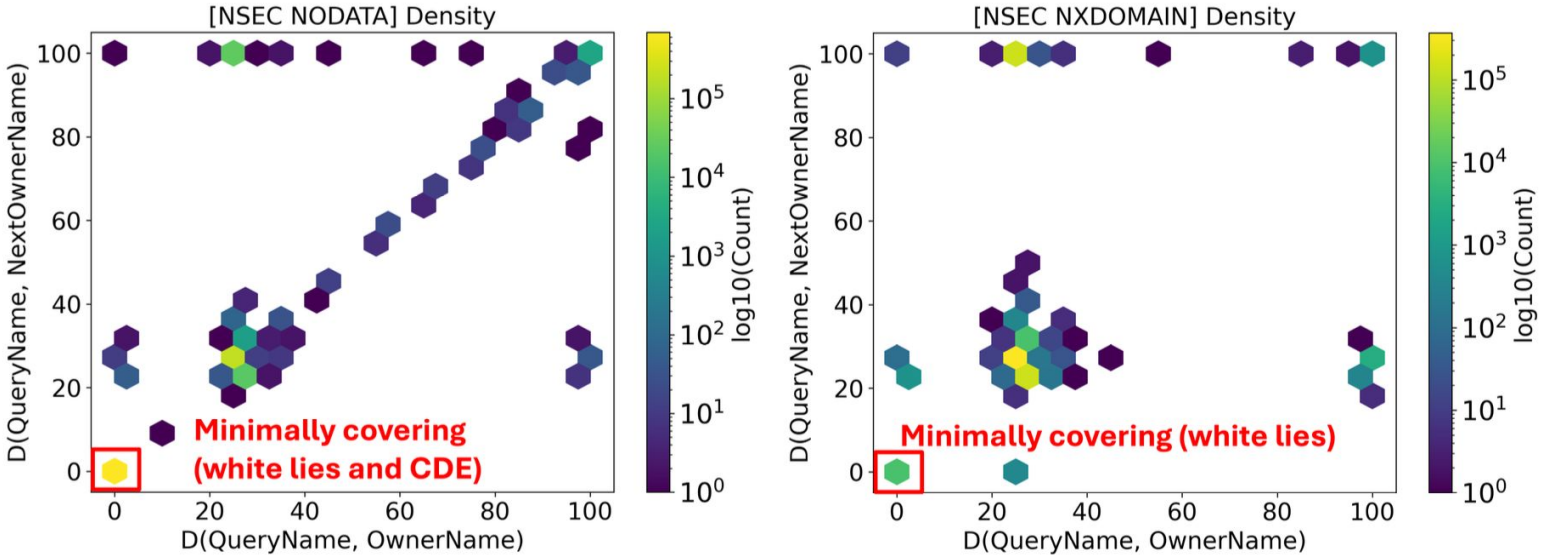
Most DNS providers predominantly deploy either NSEC or NSEC3.

NSEC: Cloudflare dominates (38–50% in TLD zones, 57–68% in top lists). NSEC3: Google Cloud DNS (40–47%), Wix, OVH. Same leaders at apex and www.

NSEC/3 Variant

- Challenge:
  - No standard epsilon function
  - Provider-specific deployment
- Our approach to distinguish CDE and White Lies:
  - **Filtering minimally covering responses:** Both White Lies and CDE employ minimally covering mechanisms to mitigate zone enumeration. As a result, the lexicographical distance between the query name and its predecessor and successor is significantly smaller than in vanilla implementations.
  - **Identifying White Lies and CDE deployments:** Providers deploying CDE are expected to exhibit a dominant proportion of NODATA responses, whereas White Lies deployments retain a mix of NODATA and NXDOMAIN. And CDE returns a single record per response.

Step 1: Identify minimally covering in NSEC/3



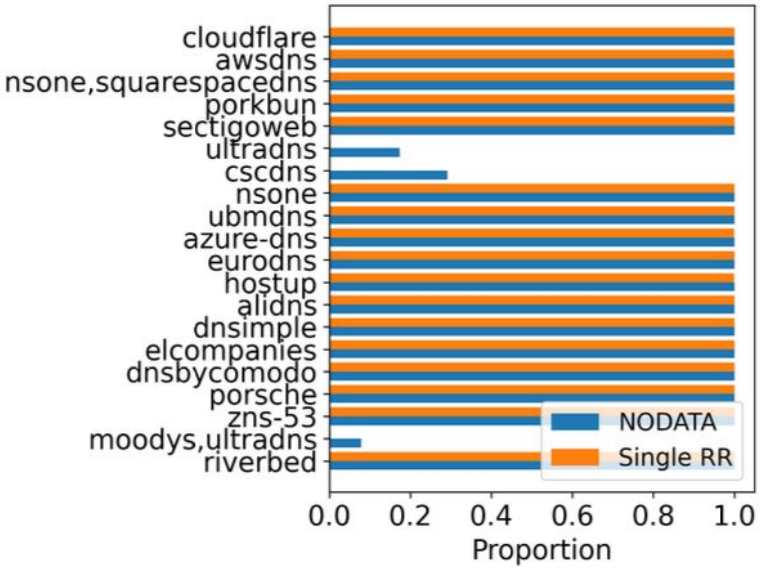
Use regex to filter escape sequences and retain only legitimate (LDH) second-level domain chars. Compute the distances following DNS canonical order. For NSEC3, compute the straight hash distance.

NSEC (.com): 73% of NODATA and 1.5% of NXDOMAIN records have D ≤ 1. NSEC3: numeric distance between hashes; 34% of NODATA and 6% of NXDOMAIN records have D ≤ 2.

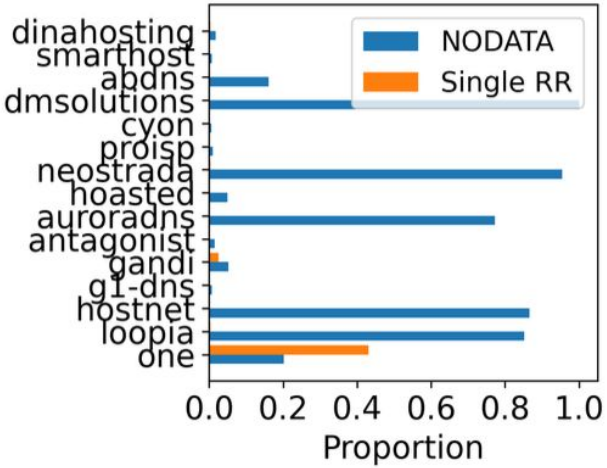
Step 2: Identify CDE and White Lies

(COM zone minimally covering responses only). CDE: High single RR ratio and High NODATA ratio.

NSEC top 20 NS providers



NSEC3 top 15 NS providers



Observation: CDE is prevalent in NSEC deployments but largely absent in NSEC3.

Observed minimally covering patterns in NSEC

Query: nonexistent.nsec-noext.com

Pattern	Observed Providers	Owner Name	Next Owner Name	Functionality	Variation
1	Cloudflare, AWS, NS1, Azure, EuroDNS, etc.	nonexistent.nsec-noext.com	\000.nonexistent.nsec-noext.com	Deny QNAME	*CDE*
2	UltraDNS, CSCDNS*, DomainNetwork*, etc.	{(~)^{*}}.{nonexistent-1}~.nsec-noext.com {(~)^{*}}.!~.nsec-noext.com *.nsec-noext.com	nonexistent!.nsec-noext.com -.nsec-noext.com -.nsec-noext.com	Deny QNAME Deny Wildcard Acknowledge Wildcard	*White Lies*
3	w3h.io	{nonexistent-1}\255.nsec-noext.com \)\255.nsec-noext.com	nonexistent\000.nsec-noext.com *\000.nsec-noext.com	Deny QNAME Deny Wildcard	*White Lies*

* Indicates providers that potentially use UltraDNS backend service.

Note: A detailed reverse engineering of the UltraDNS NSEC White Lies epsilon function: https://github.com/shuque/minimal_nsec/blob/main/UltraDNS.md

White Lies and CDE Adoption Rate

	Source domains (from OpenINTEL)				WWW subdomains (from our active prober)			
	NSEC		NSEC3		NSEC		NSEC3	
	White Lies	*CDE*	*White Lies*	*CDE*	*White Lies*	*CDE*	*White Lies*	*CDE*
.com	0.74%	43.96%	6.98%	0.00%	0.78%	41.92%	16.88%	0.00%
.net	0.96%	56.53%	6.86%	0.00%	0.98%	57.47%	13.21%	0.00%
.org	0.80%	52.75%	5.81%	0.00%	0.83%	53.75%	15.91%	0.00%
Umbrella	1.71%	76.40%	8.11%	0.01%	1.84%	80.14%	10.11%	0.00%
Tranco	1.31%	74.84%	9.31%	0.00%	1.37%	77.16%	13.90%	0.00%
Radar	0.99%	79.17%	10.37%	0.00%	0.96%	80.32%	14.31%	0.00%
Majestic	1.55%	73.04%	11.19%	0.00%	1.52%	73.23%	15.82%	0.00%

Table: % of NSEC-enabled and of NSEC3-enabled domains, respectively

Since 2019 (.com): NSEC CDE 36.5K → 693K; NSEC3 White Lies 18.9K → 469K

Current deployment of NXNAME

We examine NXNAME adoption in CDE deployments and identify the authoritative DNS providers that have already deployed it.

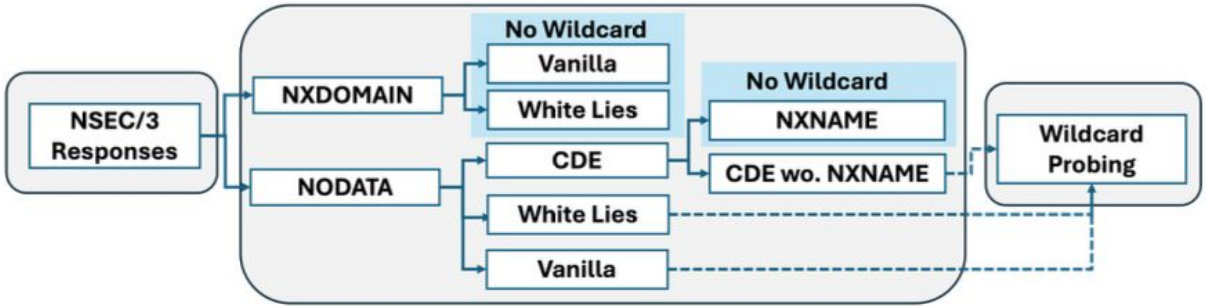
Deployed: Cloudflare, NS1, Porkbun*, SectigoWeb, HostUp*, elcompanies.com*, DNSimple, ubmdns.com*, FoundationDNS*

Not Deployed: AWS Route53, AzureDNS, EuroDNS, AliDNS, DNSbyComodo, zns-53

(* indicates providers that potentially use Cloudflare in the backend)

How Wildcard Synthesis interact with NSEC/3

- Wildcards can change denial semantics, turning an expected NXDOMAIN into NODATA or a synthesized positive response.
- Wildcard applicability depends on zone structure, especially the closest-encloser rule, making behavior vary across hierarchy levels.
- We study apex vs. www responses to understand how wildcard synthesis interacts with NSEC/NSEC3 denial-of-existence proofs.



Wildcard Identification

- **Filter explicit non-wildcard cases:** Exclude NXDOMAIN responses and CDE responses carrying NXNAME, since both indicate the queried name does not exist.
- **Check NODATA proofs:** Use NSEC/NSEC3 intervals to determine whether the wildcard name (or its hash) is explicitly proven nonexistent.
- **Identify wildcard candidates:** Remaining NODATA responses are treated as zones where wildcard synthesis may be present.

	NSEC					NSEC3				
	Deny wildcard	ACK. wildcard	%	Candidates	%	Deny wildcard	ACK. wildcard	%	Candidates	%
.com	1878	227716	14.44%	325909	20.67%	2698	453649	6.75%	729193	10.85%
.net	212	18642	11.61%	33940	21.14%	247	39005	7.18%	63230	11.64%
.org	202	17723	12.11%	28985	19.81%	169	39130	7.03%	58701	10.55%
Umbrella	40	671	4.13%	4554	28.02%	16	1157	12.15%	1666	17.49%
Tranco	81	1883	3.84%	10232	20.85%	16	5250	17.44%	6866	22.80%
Radar	111	2791	4.29%	14686	22.58%	15	7241	19.98%	9598	26.48%
Majestic	72	2256	5.50%	8722	21.28%	4	5886	17.16%	7835	22.85%

Wildcard candidates: ~20% of NSEC and ~11% of NSEC3 domains in the TLD zones (17–26% for NSEC3 in the top lists). Explicit wildcard proofs: 11–14% of NSEC and ~7% of NSEC3 domains in the TLD zones.

NSEC/3 Variant for Domains with Wildcard Synthesis.

		NSEC		NSEC3	
		White Lies	*CDE*	*White Lies*	*CDE*
WWW	.com	0.85%	32.20%	43.23%	0.00%
	.net	1.00%	47.30%	38.50%	0.00%
	.org	0.96%	41.05%	46.03%	0.00%
	Umbrella	1.08%	85.19%	19.85%	0.00%
	Tranco	0.81%	81.16%	22.86%	0.00%
	Radar	0.58%	80.73%	22.86%	0.00%
	Majestic	0.86%	73.26%	21.69%	0.00%
Source	.com	0.85%	32.27%	38.43%	0.00%
	.net	1.00%	47.39%	34.69%	0.00%
	.org	0.95%	41.17%	37.29%	0.00%
	Umbrella	1.05%	85.27%	18.86%	0.00%
	Tranco	0.81%	81.09%	15.41%	0.00%
	Radar	0.59%	80.61%	16.59%	0.00%
	Majestic	0.86%	73.31%	20.81%	0.00%

NSEC/3 variants among wildcard-candidate domains: www vs. apex (source)

Shift from NODATA to NXDOMAIN

	NSEC			NSEC3	
	NODATA w.o. NXNAME	NODATA w. NXNAME	NXDOMAIN	NODATA	NXDOMAIN
.com	49.34%	**13.41%**	**37.24%**	55.04%	**44.96%**
.net	55.63%	**16.87%**	**27.51%**	60.74%	**39.26%**
.org	52.33%	**15.98%**	**31.68%**	54.58%	**45.42%**
Umbrella	63.57%	**28.67%**	**7.76%**	36.37%	**63.63%**
Tranco	56.50%	**31.77%**	**11.73%**	32.62%	**67.38%**
Radar	57.32%	**31.61%**	**11.07%**	35.42%	**64.58%**
Majestic	50.36%	**31.43%**	**18.21%**	30.75%	**69.25%**

Distribution of NODATA and NXDOMAIN responses in the **WWW** dataset. For NSEC, NODATA responses are further classified based on the presence of NXNAME.

Response shift:
In the TLD zones, 40–50% of www probes (for both NSEC and NSEC3) flip to NXDOMAIN or NODATA+NXNAME. In the top lists, ~31–36% flip for NSEC3 and ~36–50% for NSEC.

Why it happens:
Explicit subdomains can become the **closest encloser**, preventing an apex wildcard from applying beneath them.

What it reveals:
This exposes **limited zone-structure information**: wildcard presence, intermediate names, and wildcard coverage boundaries (but does not enable direct zone walking).

Conclusions

- NSEC/NSEC3 deployment has grown substantially since 2019
- CDE is prevalent in NSEC deployments
- We identify multiple minimally covering NSEC strategies
  - and map them to major authoritative DNS providers
- We characterize the current deployment of NXNAME
- Wildcard behavior is non-negligible
  - ~20% of NSEC and ~11% of NSEC3 domains in the TLD datasets are wildcard candidates
- NODATA → NXDOMAIN transitions can reveal limited zone-structure information
- Limitations
  - wildcard analysis focuses only on www subdomains
  - measurements are snapshot-based and rely on Google public resolver

Dataset: https://keyinfra.cs.virginia.edu/datasets/dns-nsec/

Paper and Acknowledgements

More detailed research paper:

Dissecting NSEC and NSEC3 Deployment in the Wild

Yizhe Zhang, Hyeonmin Lee, Shumon Huque, Yixin Sun

IMC '26: Proceedings of the 2026 ACM Internet Measurement Conference

Thanks to OpenINTEL (UTwente, SIDN, NLnet Labs, SURF) for their datasets.