ICANN DNS Symposium 2024

Mitigating Stale Glue Records in TLD Zone Files
Analysis of Registry Practices and Recommendations

Yunyi Zhang

September 25th, 2024

国防科技大学
NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY

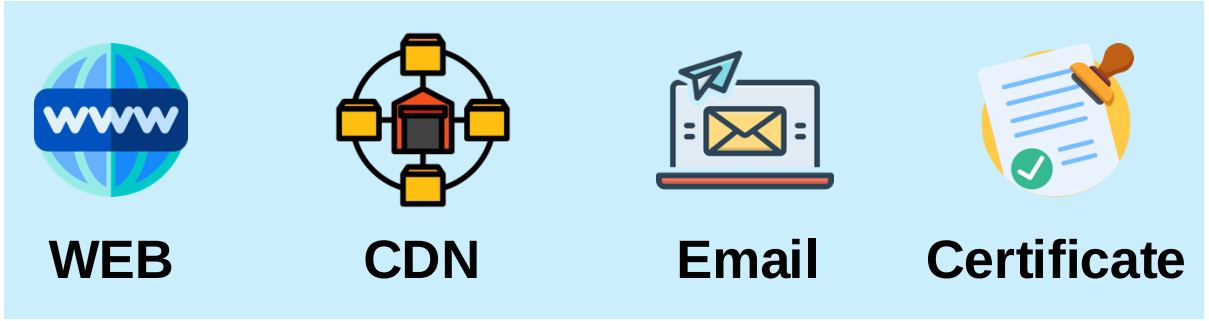
清華大學
Tsinghua University

Brief Summary

- Stale glue records point to invalid nameserver IPs
- Nearly a quarter of the glue records are stale, affecting more than 6 million active domains.
- Registry's management strategy for DNS host objects is a non-overlook cause of stale glue records in zone files.

Domain Name System

❖ **Translating domain names to IP addresses**

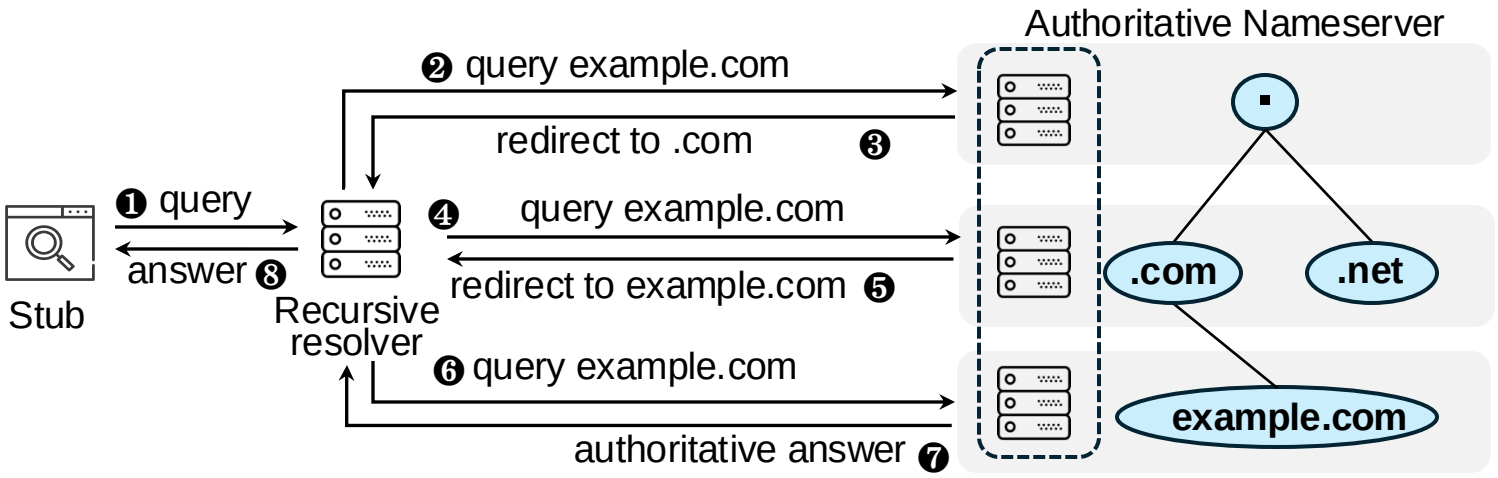


entry point of many Internet activities

Domain Name System

❖ **Translating domain names to IP addresses**

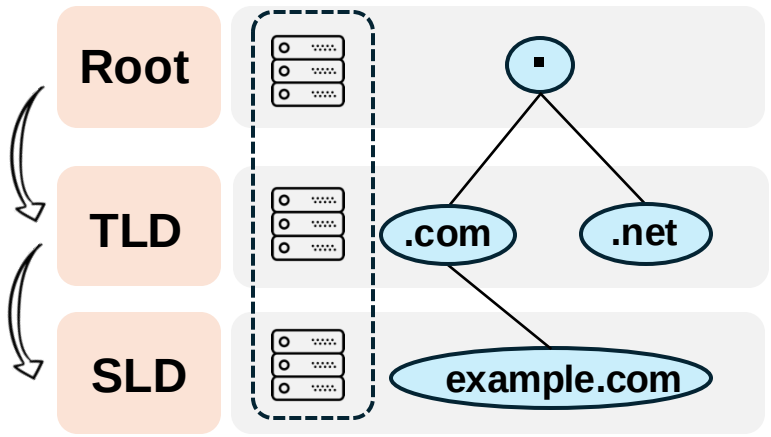
❖ **Resolution process**



Domain Name System

- Translating domain names to IP addresses
- Resolution process
- Hierarchical Name Space
  - Authoritative zones: root, TLD, SLD

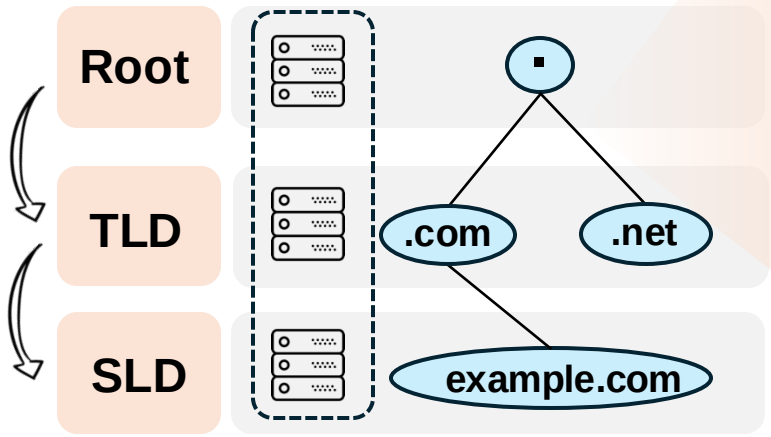
Parent zone maintains delegation records for their child zone.



Domain Name System

- Translating domain names to IP addresses
- Resolution process
- Hierarchical Name Space
  - Authoritative zones: root, TLD, SLD

Parent zone maintains delegation records for their child zone.



Domain delegation

In-domain delegation

```
foo.com NS ns1.foo.com
```

Sibling-domain delegation

```
foo.com NS ns1.exam.com
```

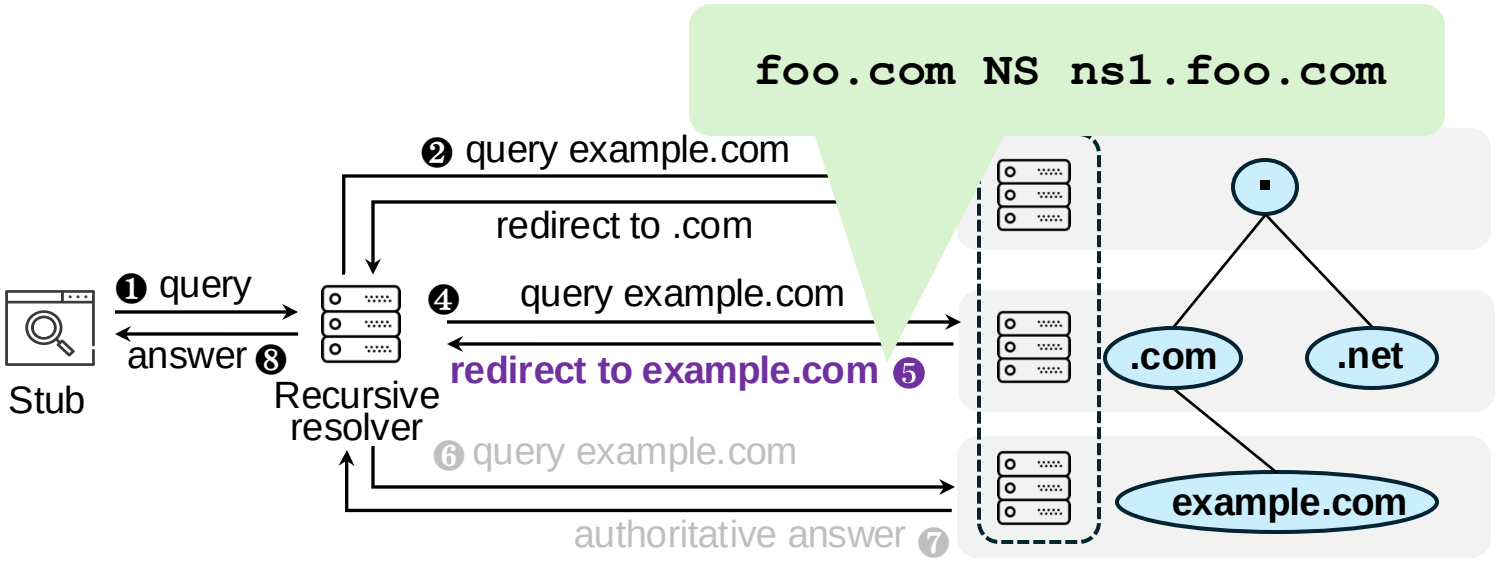
Out-domain delegation

```
foo.com NS ns1.foo.net
```

DNS Glue Records – Resolution Loop

In-domain delegation

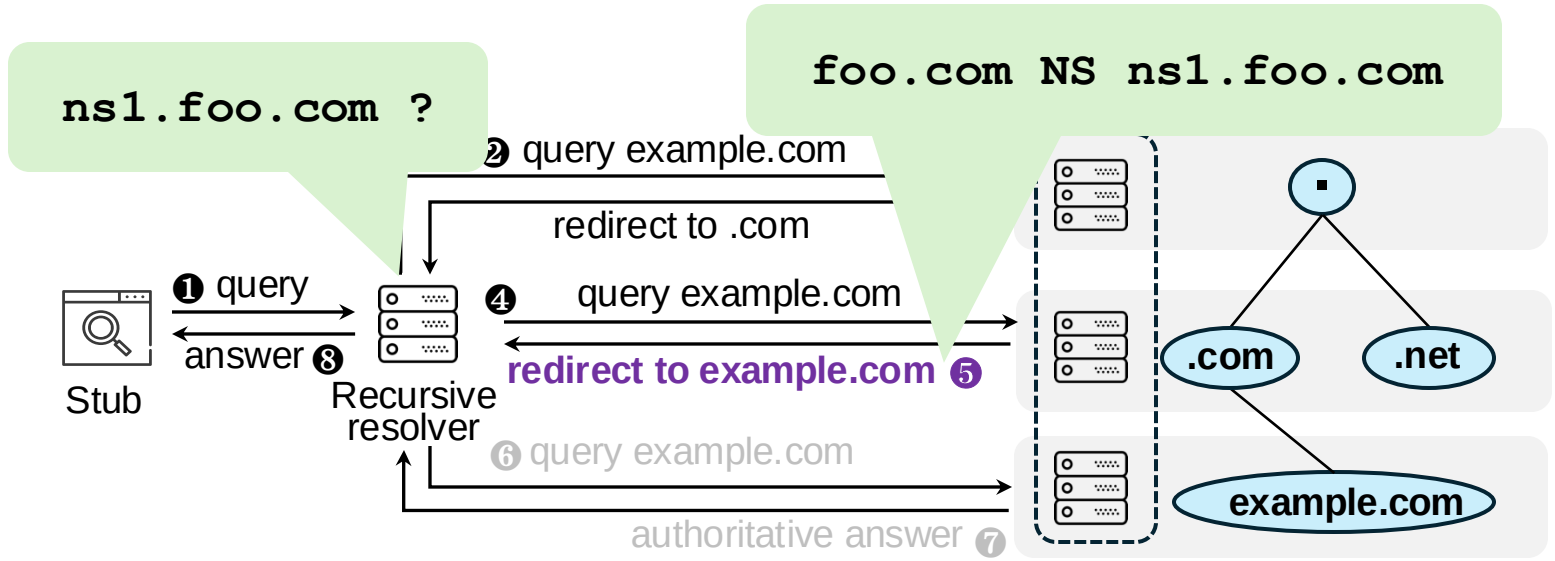
```
foo.com NS ns1.foo.com
```



DNS Glue Records – Resolution Loop

In-domain delegation

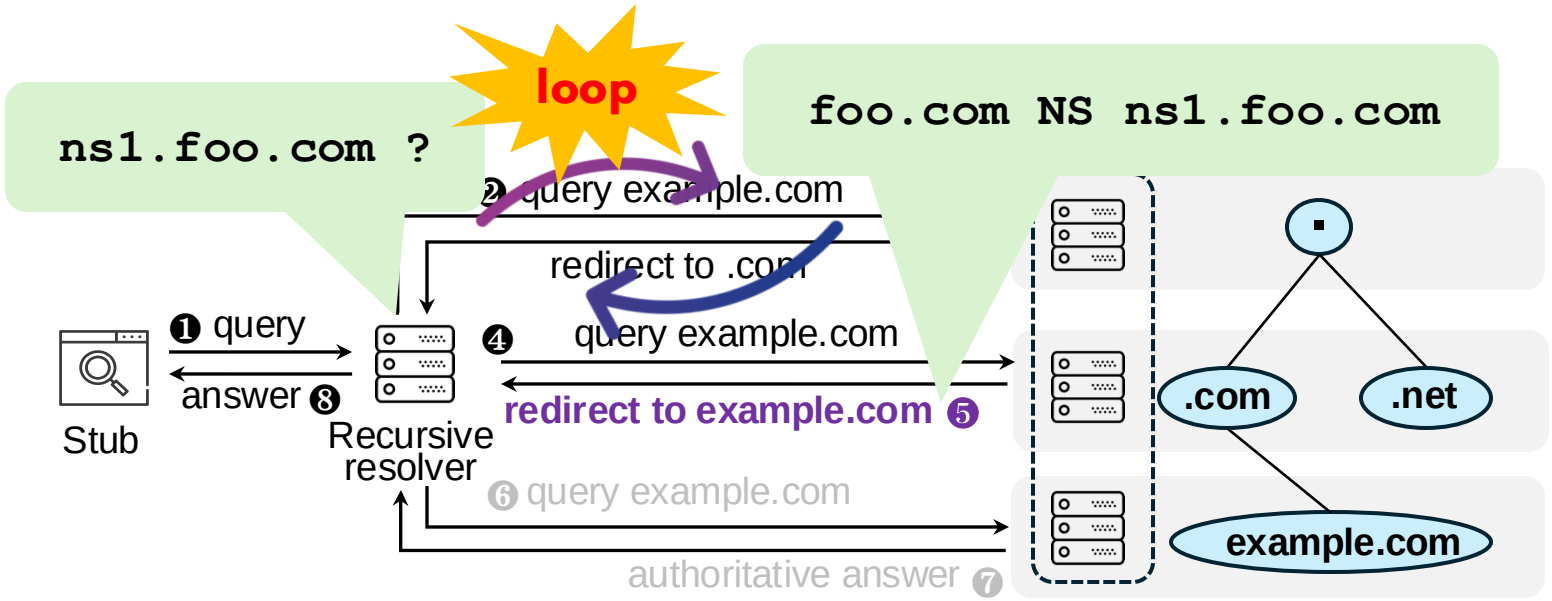
```
foo.com NS ns1.foo.com
```



DNS Glue Records Prevent Resolution Loop

In-domain delegation

```
foo.com NS ns1.foo.com
```



DNS Glue Records Prevent Resolution Loop

In-domain delegation

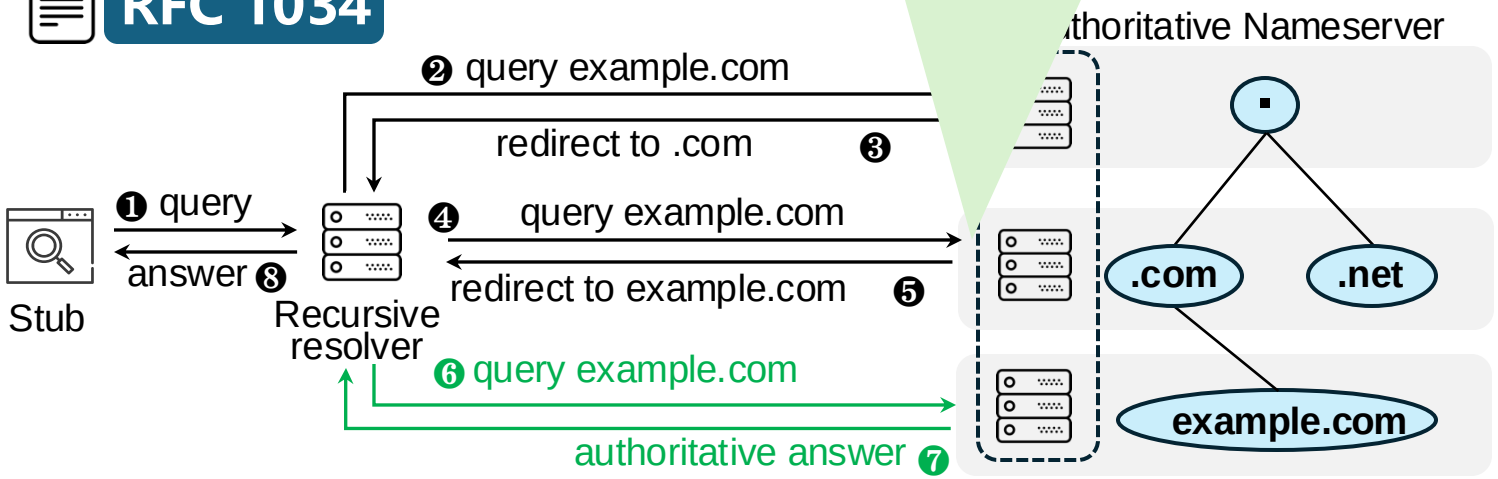
```
foo.com NS ns1.foo.com
```

To fix this problem, a zone contains "glue" RRs which **are not part of the authoritative data**, and are address RRs for the servers.

glue records →

```
foo.com NS ns1.foo.com
ns1.foo.com A 192.168.1.1
```

RFC 1034



Takeaway

Glue records are necessary resource records used to resolve resolution loops.

However, the community seldom pays attention to the security threats associated with them.

Why the Neglect of Glue Records?

In RFC 1034, the use of glue records is restricted

These RRs are only necessary if the name server's name is "below" the cut, and are only used as part of a referral response.

Mainstream DNS software assigns a low trust level to glue records

BIND9

Definition	Level	Description
dns_trust_ultimate	9	This server is authoritative
dns_trust_secure	8	Successfully DNSSEC validated
dns_trust_authanswer	7	Answer from an authoritative server
dns_trust_authauthority	6	Received in the authority section from an authoritative response
dns_trust_answer	5	Answer from a non-authoritative server
dns_trust_glue	4	Received in a referral response
dns_trust_additional	3	Received in the additional section of a response

Knot Resolver

Definition	Level	Description
KR_RANK_SECURE	32	Verified trust chain from the closest TA
KR_RANK_AUTH	16	Authoritative data
KR_RANK_INSECURE	8	Proven to be insecure
KR_RANK_MISSING	7	No RRSIG found
KR_RANK_MISMATCH	6	-
KR_RANK_BOGUS	5	Ought to be secure but isn't
KR_RANK_INDET	4	Unable to determine whether secure
KR_RANK_TRY	2	Attempt to validate
KR_RANK_OMIT	1	Do not attempt to validate
KR_RANK_INITIAL	0	Initial-like states

Question

Does the usage of glue records adhere to best practices?

No. Many stale glue records are left in zone files. Mainstream resolver software uses glue records in places beyond in-domain delegation.

DNS Glue Records - Configuration

- stored in the parent zone (e.g., .com)

DNS Glue Records - Configuration

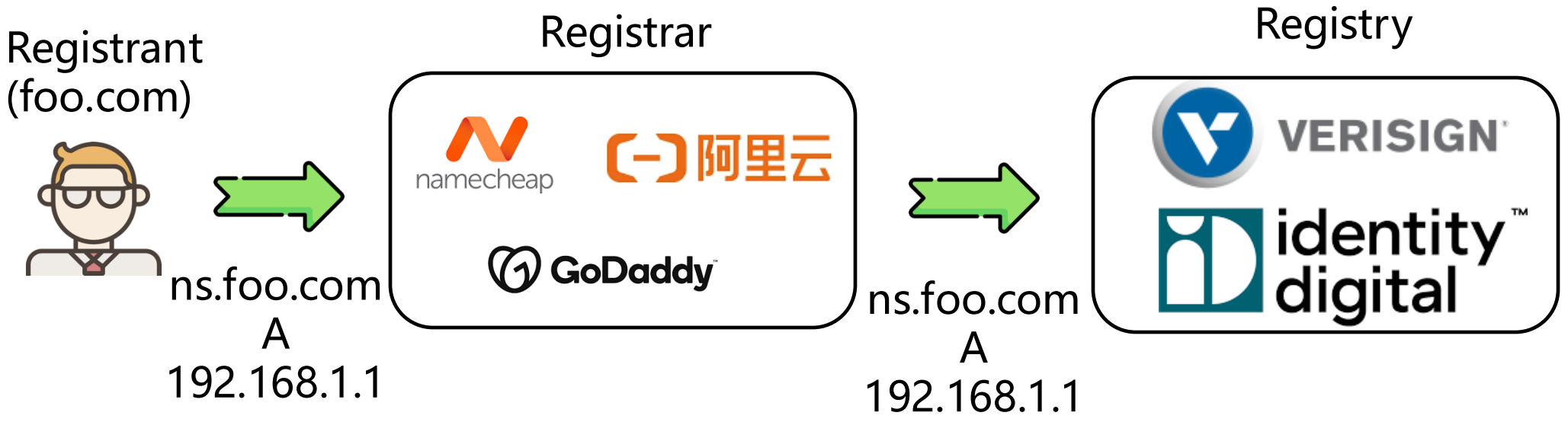
- stored in the parent zone (e.g., .com)

How to configure the glue records?

DNS Glue Records - Configuration

- stored in the parent zone (e.g., .com)

How to configure the glue records?



Takeaway

The configuration of glue records is complex, posing a comprehension barrier for ordinary users,

We have discovered **incorrectly configured glue records** in the zone files.

DNS Glue Records in Zonefiles

1,096 TLDs

.com, .net, .org, …

300M+ domain names

2M+ glue records

Glue

; .com zone file

example.com	NS	ns. example.com
ns. example.com	A	1.2.3.4
example2.com	NS	ns.stale.com
ns.stale.com	A	4.5.6.8
ns.abandoned.com	A	4.5.6.8

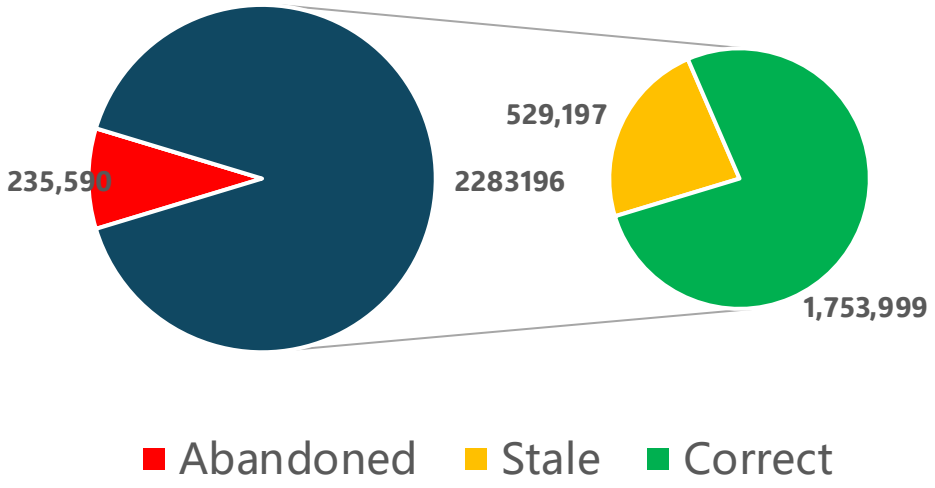
; example.com nameserver

example.com	NS	ns. example.com
ns. example.com	A	1.2.3.4

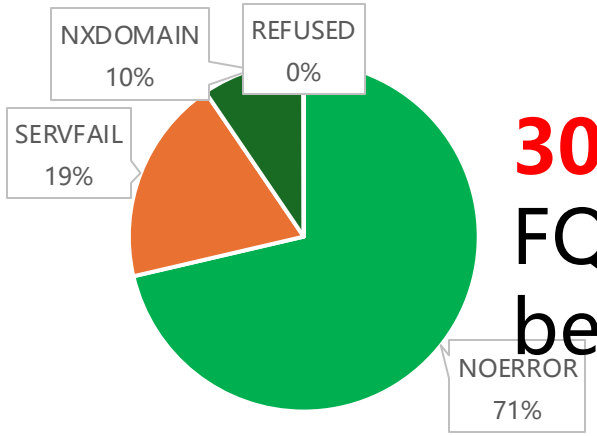
; stale.com nameserver

ns.stale.com	A	2.3.4.5

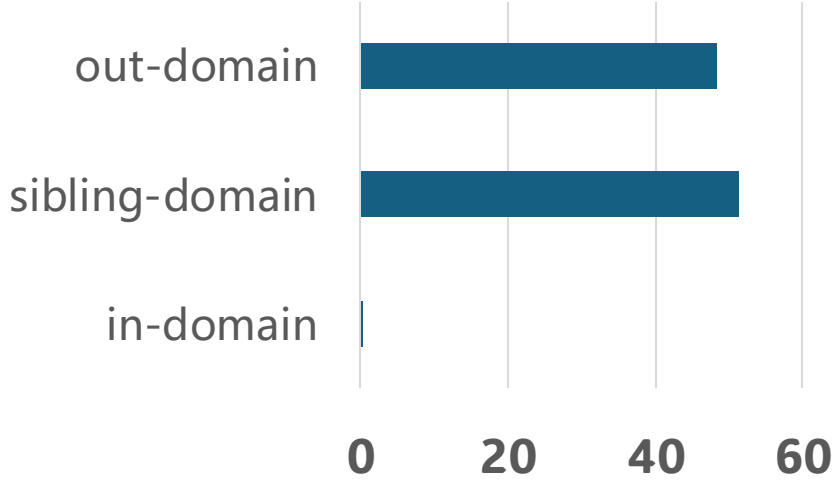
Abundant Stale and Flawed Glue Records



23.18% of glue records are stale



30% of glue FQDNs cannot be resolved



0.29% of delegation are in-domain delegation

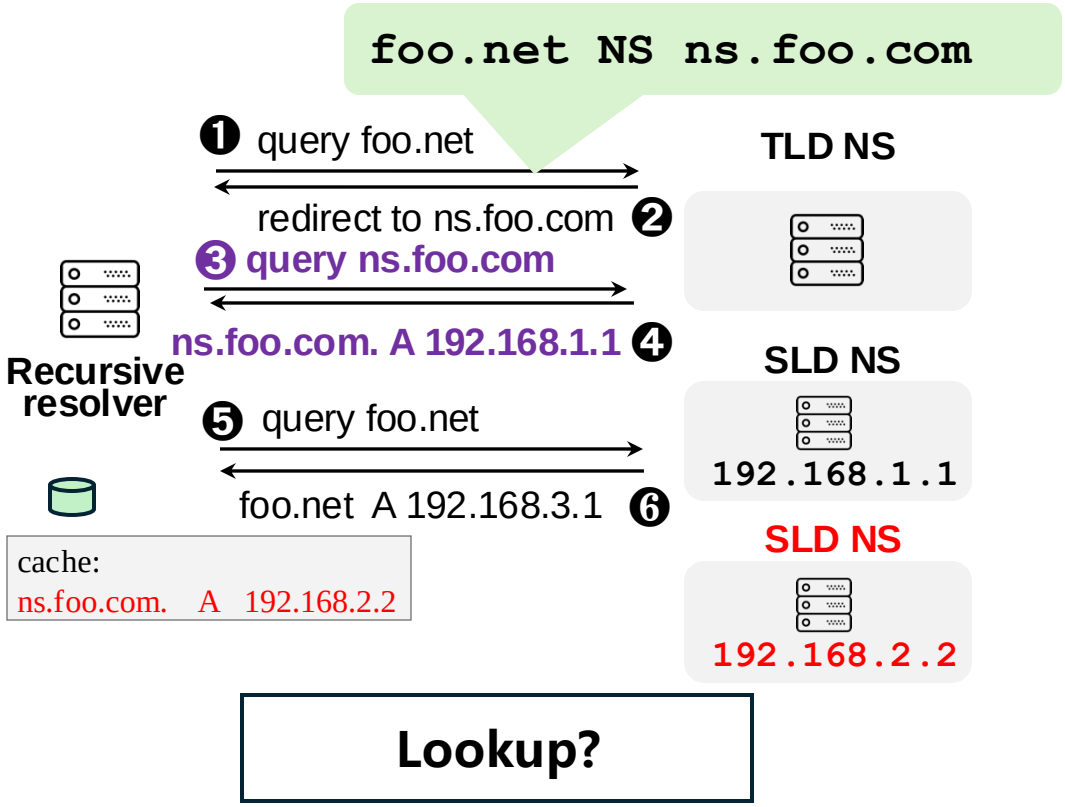
Question

Can these forgotten stale glue records be exploited ?

Yes, mainstream DNS software **directly uses glue records** without verification.

Glue Record Use in DNS software

- **Will cached glue records be used in future resolution processes?**

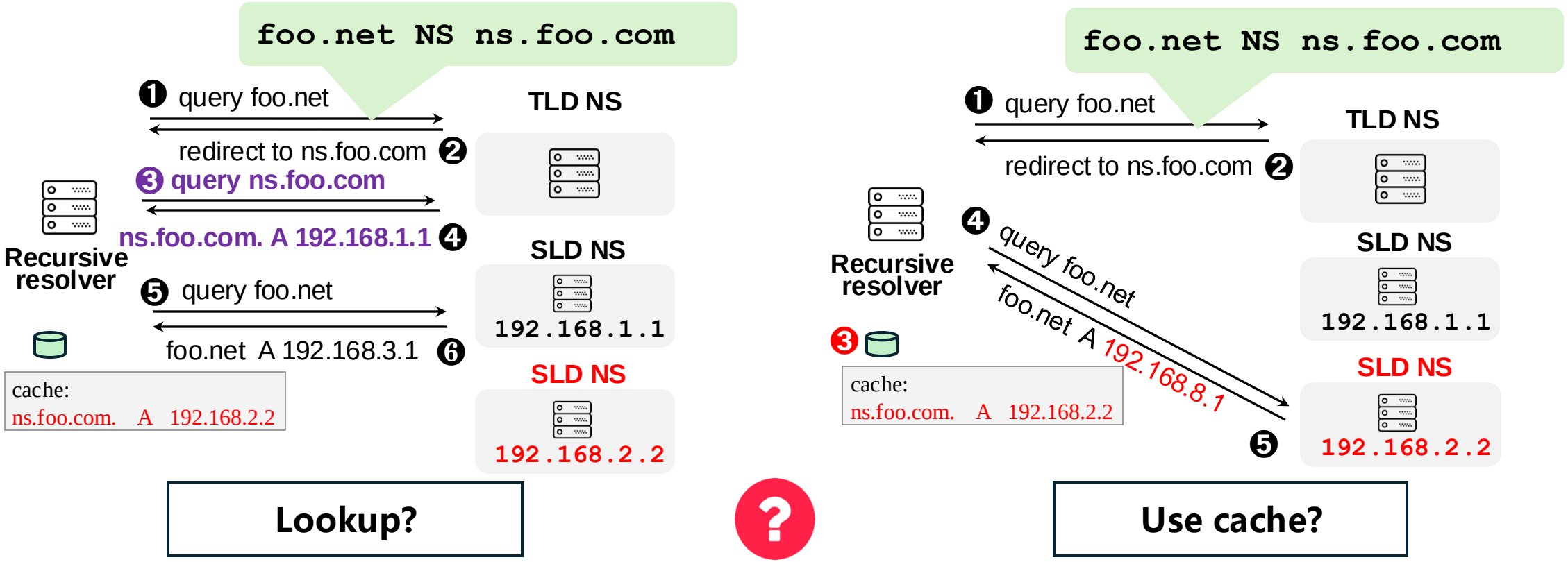


Lookup?

Out-domain delegation

Glue Record Use in DNS software

❖ **Will current glue records be used in future resolution processes?**



Out-domain delegation

DNS software uses cache without validation

- Caching and using glue without validation.

  All DNS software

- Misplaced trust for unvalidated glue records.

  BIND9, PowerDNS, Knot, Microsoft DNS, Simple DNS Plus

Question

How to exploit the abundant stale glue records?

Shadow caching

Shadow Caching – Awaking stale glue records

- injecting stale glue records to target resolver
  - Step 1: configure delegation relationship

```
.com zone file
ns1.vulner.com A 192.1.1.1
attack.com NS ns1.vulner.com
```

```
.net zone file
victim.net NS ns1.vulner.com
```

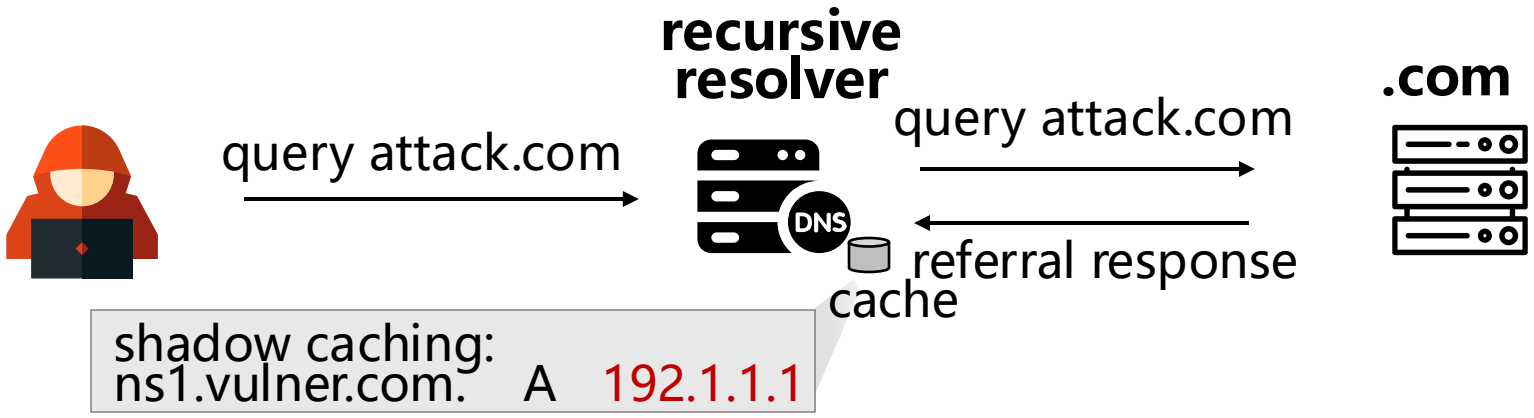
Shadow Caching – Awaking stale glue records

- injecting stale glue records to target resolver
  - Step 1: configure delegation relationship

```
.com zone file
ns1.vulner.com A 192.1.1.1
attack.com NS ns1.vulner.com
```

```
.net zone file
victim.net NS ns1.vulner.com
```

  - Step 2: lookup to target resolvers



Shadow Caching – Attack

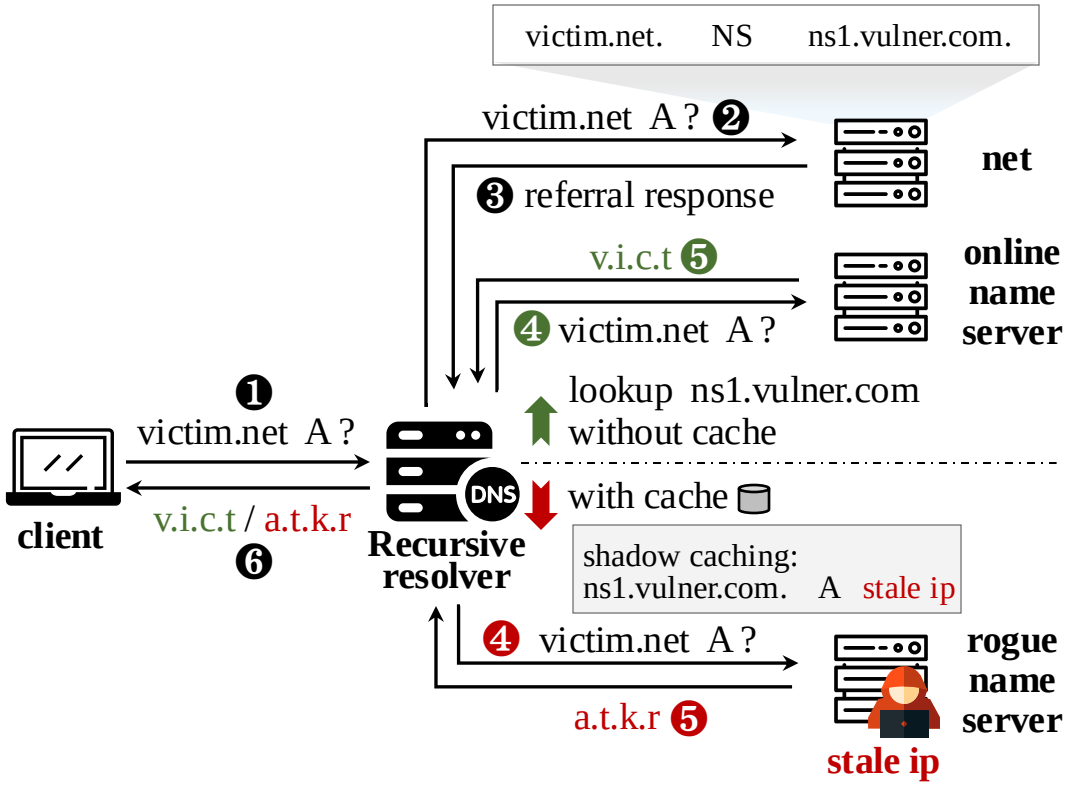
❖ Domain takeover

Assumption

- Exploitable stale glue records
- Assignable cloud IPs

Exploiting Idea

- Injecting the *shadow caching* by attack.com
- Resolvers applies shadow caching directly, if it exists



Shadow Caching – Attack

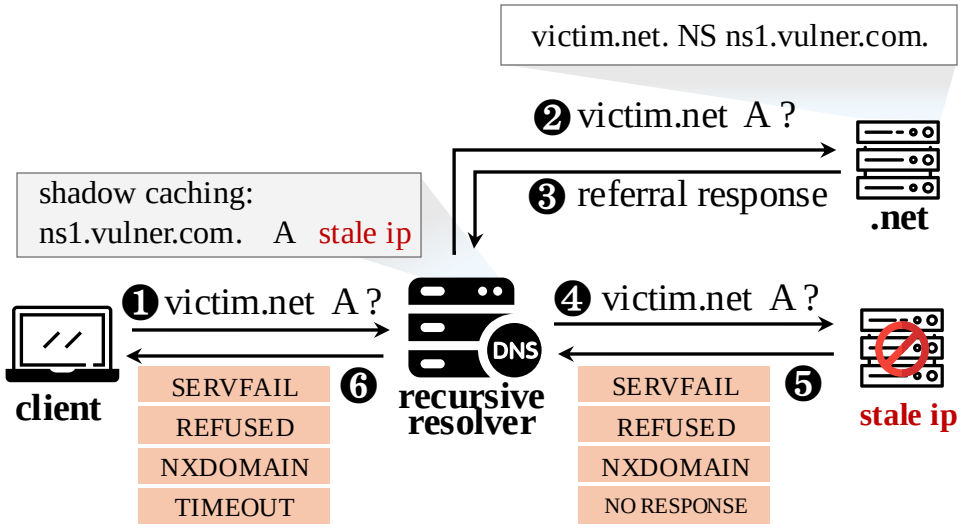
❖ Denial-of-Service

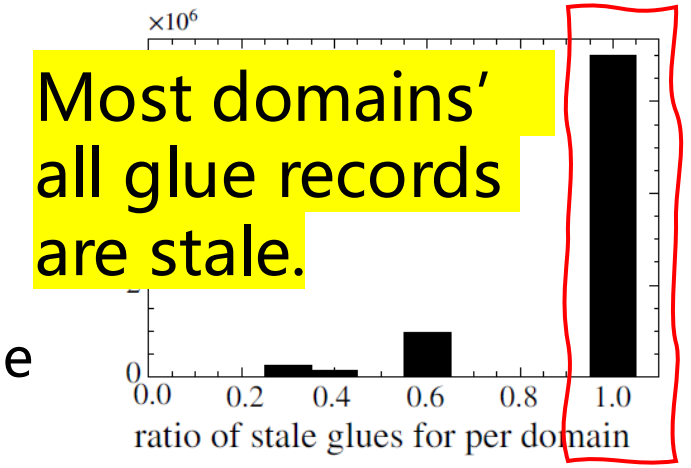
Assumption

- Exploitable stale glue records
- The domain is out-domain delegation and all GlueFQDNs of nameservers are stale.

Exploiting Idea

- Injecting the *shadow caching* by attack.com
- After multiple retries, resolvers returns a failed response





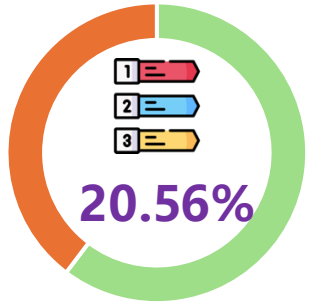
Most domains' all glue records are stale.

Vulnerable Glue Records and Domains

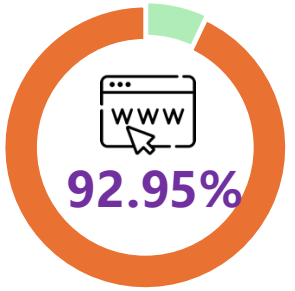
Domain takeover

193,558 exploitable stale glue records mapping to 100,258 cloud IPs.

6,398,631 domain names susceptible to takeover.



Tranco Top 1M



Active domains

Denial-of-Service

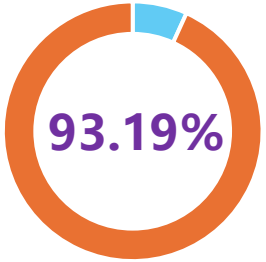
784,693 active domains susceptible to denial-of-service attacks

Vulnerable Software and Resolver

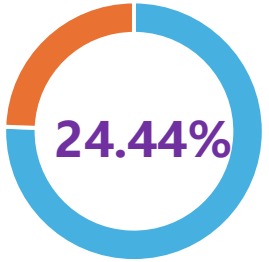
- 9/9 DNS resolver software vulnerable to **domain takeover，DoS**

- 14/14 DNS Public DNS vulnerable to **domain takeover, DoS**

- Open Resolvers



Domain takeover



DoS

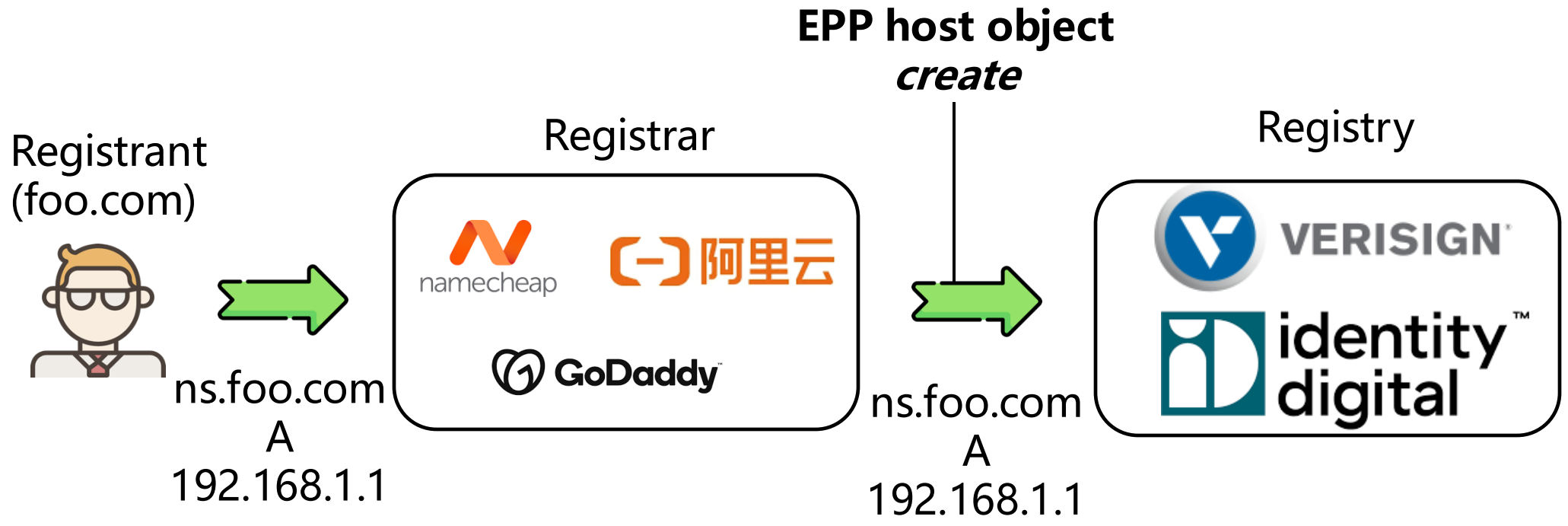
Question

Why are there are so many stale glue records in the zone file?

Creating DNS Host

Glue records and DNS host object

The user configures the glue record, and the registry creates the corresponding DNS host object



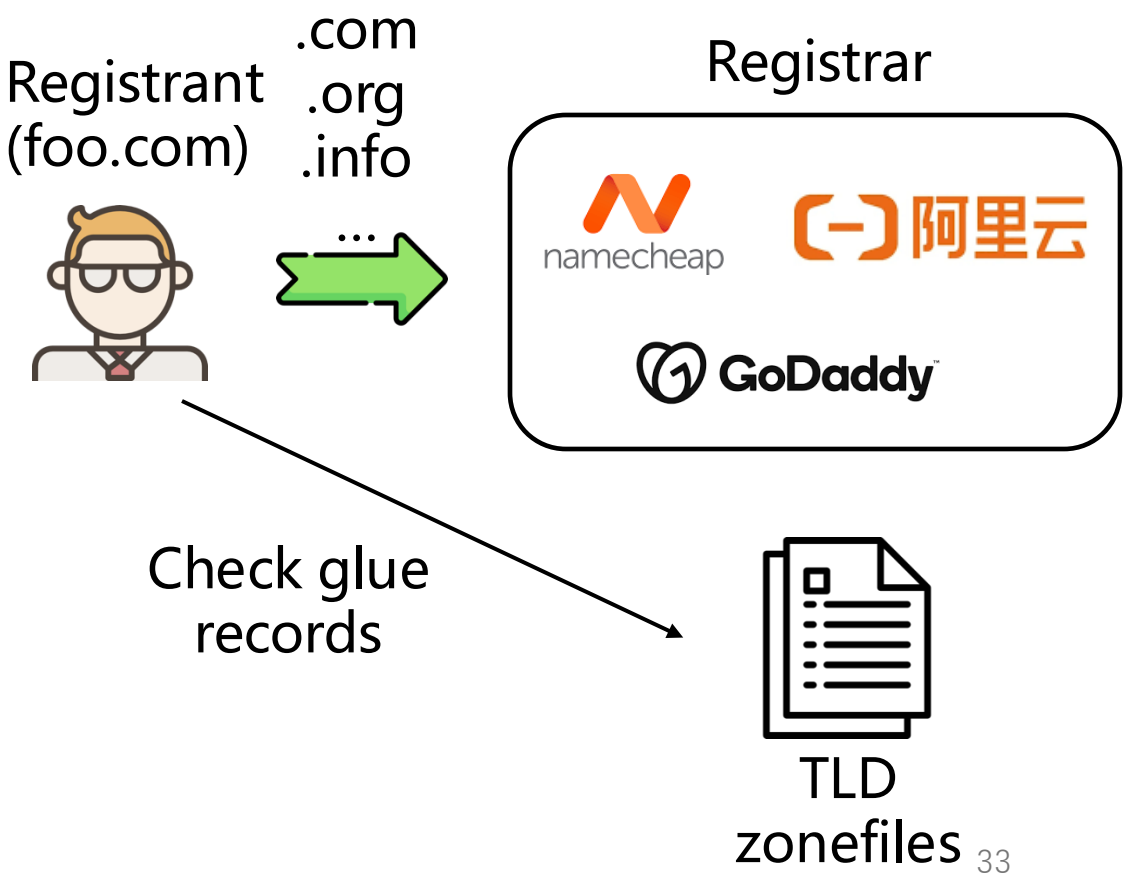
DNS Host Management

How do registries manage these DNS host objects?

Dynamic analysis

We purchase test domain names across various TLDs and registrars, and then register DNS host objects.

We check glue records in latest TLD zonefiles to determine the TLD management strategies.



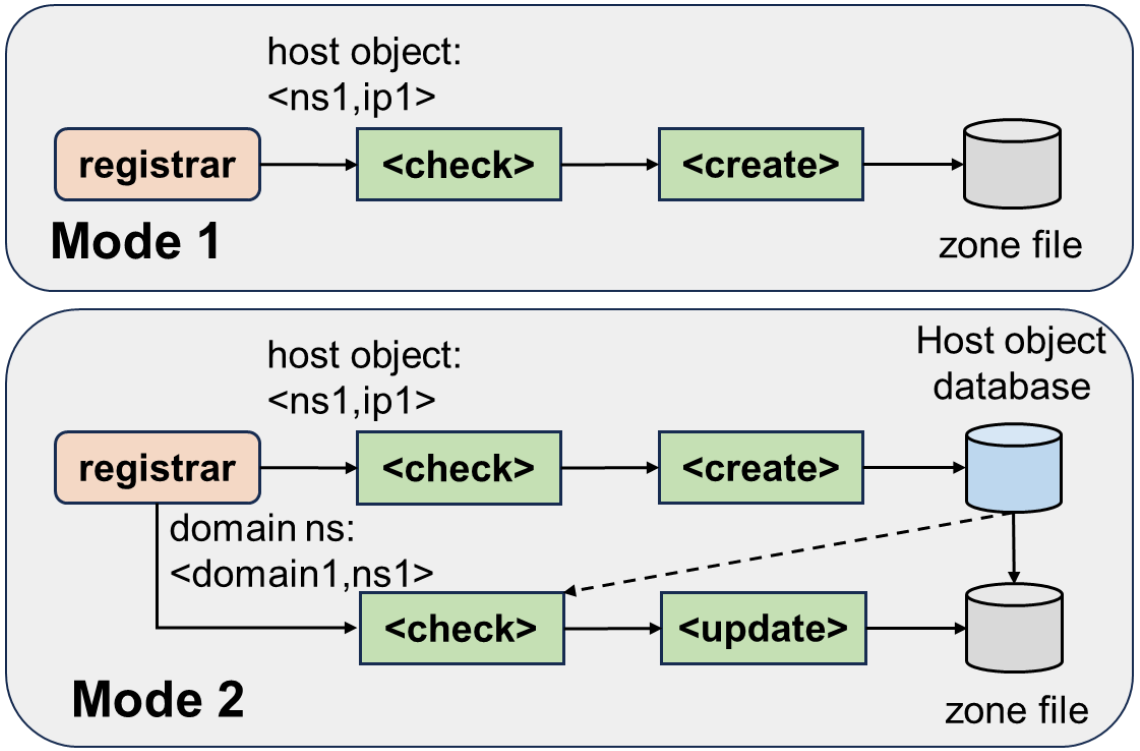
DNS Host Management Mode

Mode1

Once the registry completes the registration, the host object is unconditionally written into the zone file.

; .com zone file		
example.com	NS	ns. example.com
ns. example.com	A	1.2.3.4
ns1.example.com	A	4.5.6.8

.com, .org, and .net



DNS Host Management Mode

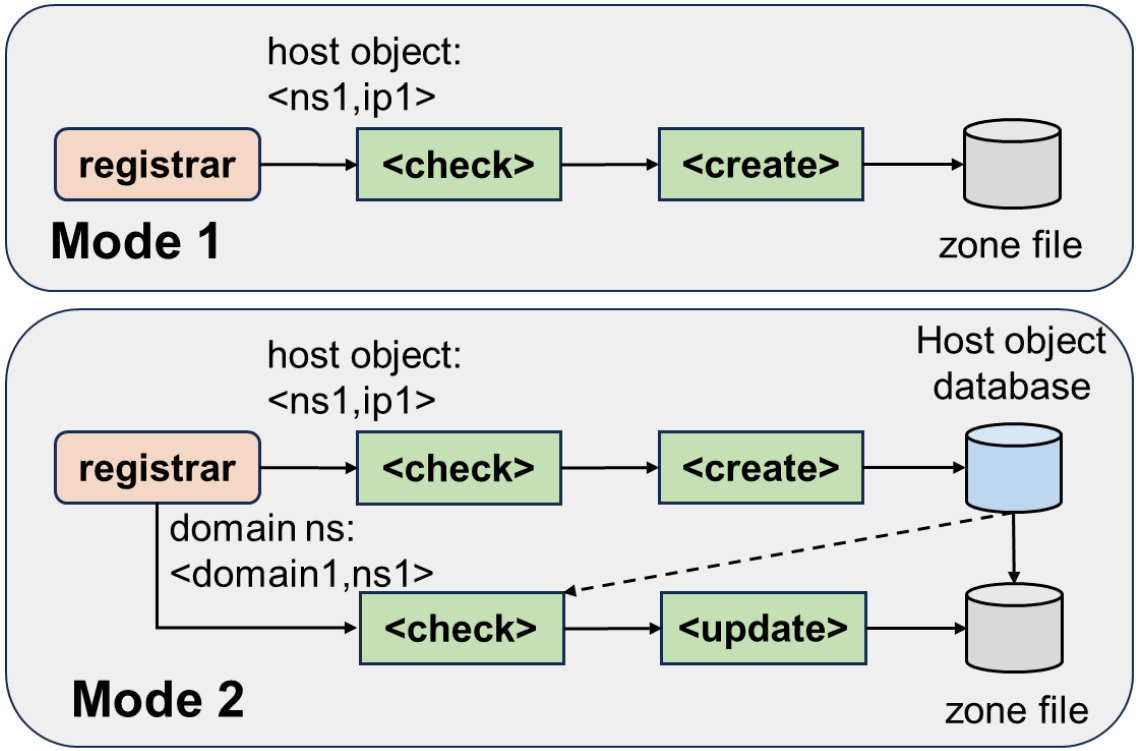
Mode1

Once the registry completes the registration, the host object is unconditionally written into the zone file.

Mode2

When a DNS host object is utilized in an in-domain delegation, registries save it into the zone file.

.com, .org, and .net



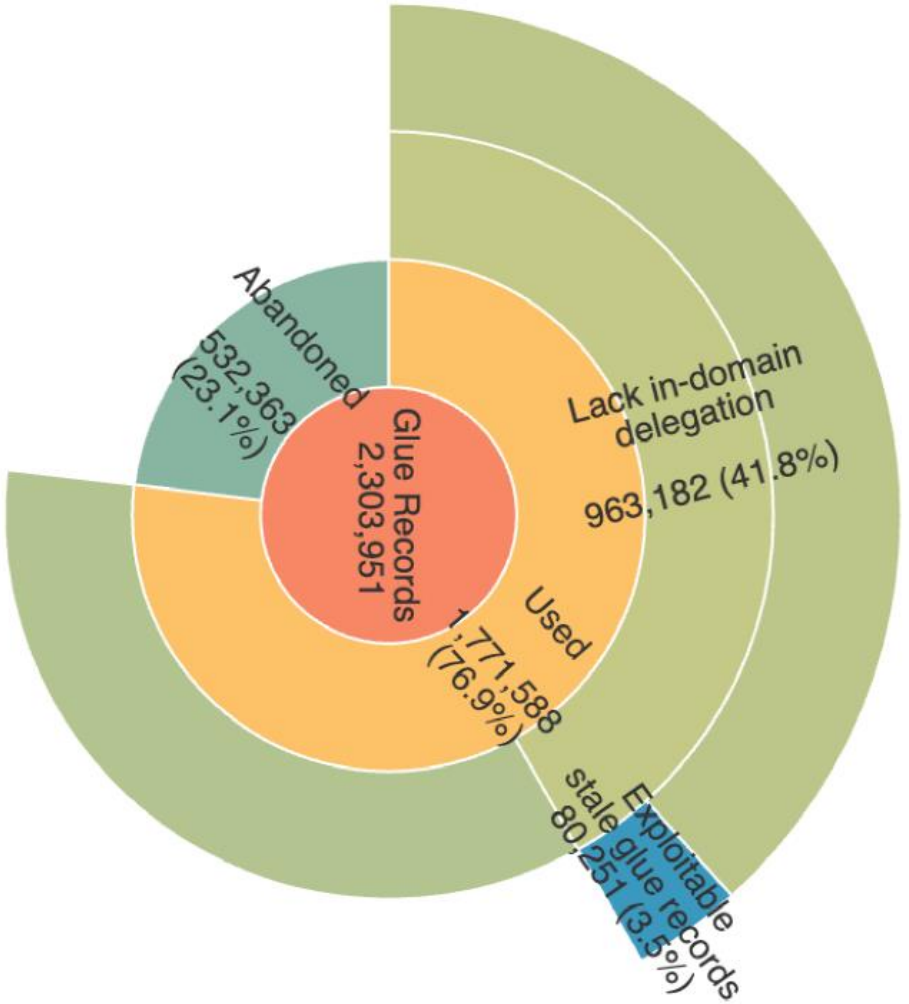
.xyz and .site

DNS Host Management Mode Impact

We extracted a total of **2,303,951** glue records from zone files of **1,109 TLDs.**

963,182 (54.37%) of the glue records lack in-domain delegation. **(Mode1)**

430,820 glue records exhibit sibling-domain delegation or out-domain delegation.
(used by other domains)



DNS Host Management Mode Impact

80,251 (43.54%) lacked in-domain delegation, affecting **1,600,253 (26.37%)** domain names.

The .com zone file contains **356,762** M1 glue records, among which **47,593** glue records are exploitable by attackers.

TLD	# Glue record[1]	# Exploitable[2]	Percentage
.com	356,762	47,593	13.34%
.org	287,758	18,926	6.58%
.info	96,668	4,157	4.31%
.wtf	83,479	19	0.02%
.net	47,262	3,707	7.84%
.top	13,581	1,645	12.11%
.live	8,525	384	4.50%
.pro	7,838	324	4.13%
.life	5,231	915	17.49%
.digital	3,533	86	2.43%

[1]: Glue records lacking in-domain delegation.
[2]: Exploitable stale glue records.

Discussion

- **Mitigation Solution**
  - Avoid using glue record caching under out-domain delegation
  - Enhance management of delegation records
    - Mode 2 instead of Mode 1

Conclusion

- **Systematic analysis of glue records**
  - across 1,096 TLDs and 9 major DNS software
- **Novel attack**
  - new exploitation method for stale glue records, especially under **out-domain delegation, affecting** over 6 million domains
- **Exploring the root causes of stale glue records**

Thanks for listening!
Any question?

Yunyi Zhang

Email: zhangyyzyy@nudt.edu.cn

国防科技大学
NATIONAL UNIVERSITY
OF DEFENSE TECHNOLOGY

清華大學
Tsinghua University