usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

33RD USENIX SECURITY SYMPOSIUM

Rethinking the Security Threats of Stale DNS Glue Records

Yunyi Zhang, Baojun Liu, Haixin Duan, Min Zhang, Xiang Li,
Fan Shi, Chengxi Xu and Eihal Alowaisheq

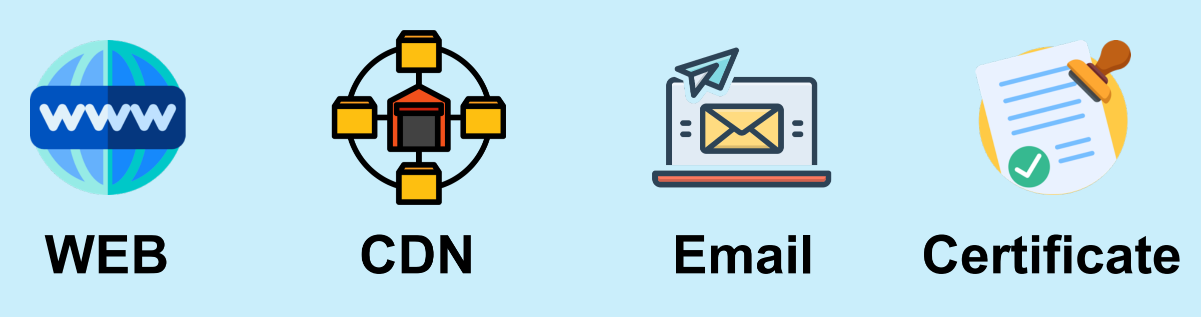
Presenter: **Chaoyi Lu**
Posdoctoral researcher, Tsinghua University
https://chaoyi.lu

Brief Summary

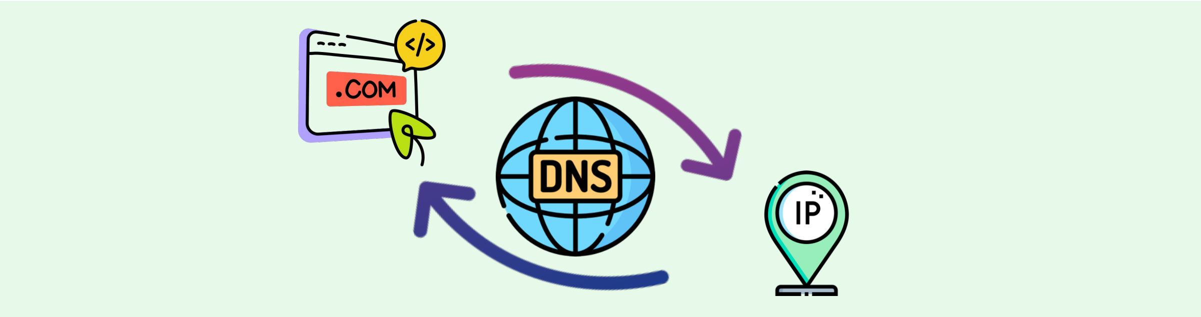
- **Stale glue records point to invalid nameserver IPs**
- **Nearly a quarter of the glue records are stale, affecting more than 6 million active domains.**

Domain Name System

❖ **Translating domain names to IP addresses**



WEB **CDN** **Email** **Certificate**

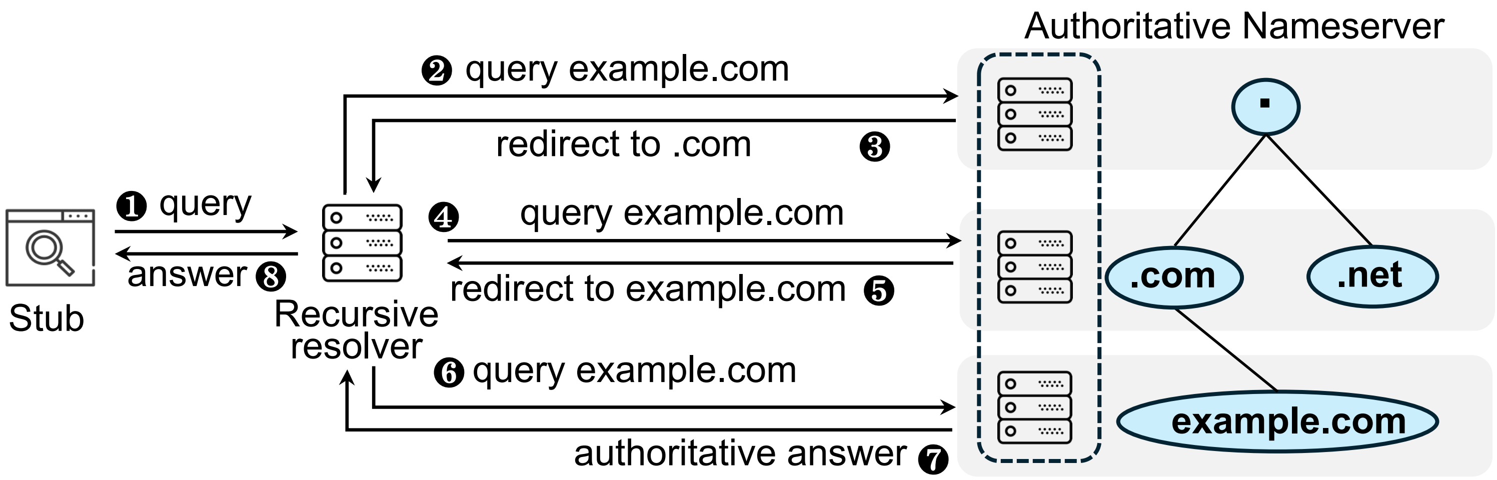


entry point of many Internet activities

Domain Name System

- ❖ Translating domain names to IP addresses

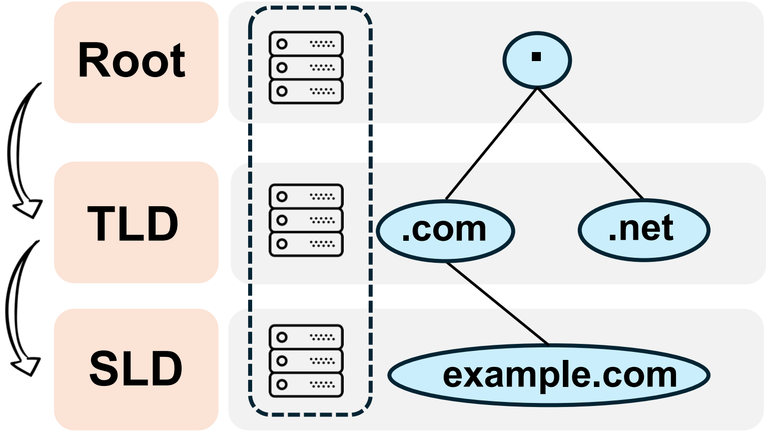
- ❖ Resolution process



Domain Name System

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

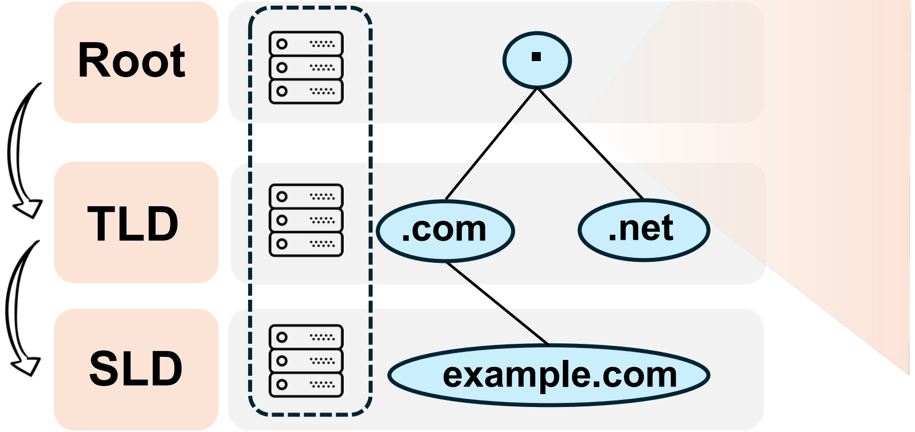
Parent zone maintains delegation records for their child zone.



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.



Types of delegation

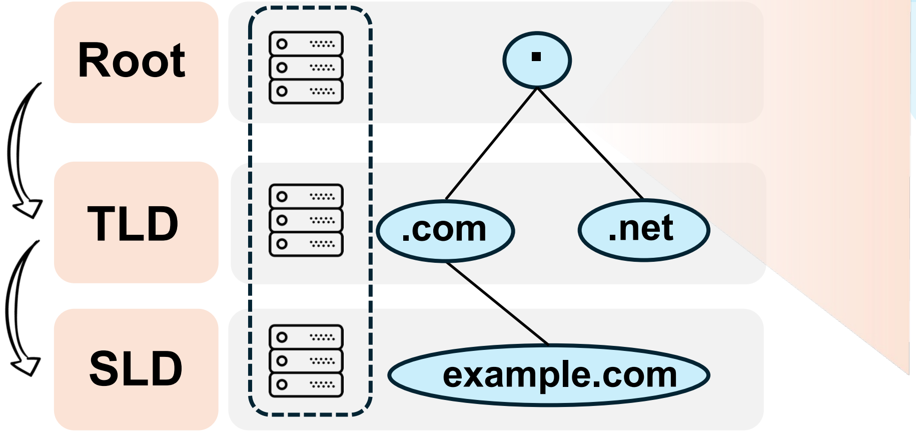
In-domain delegation

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

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.



Types of delegation

In-domain delegation

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

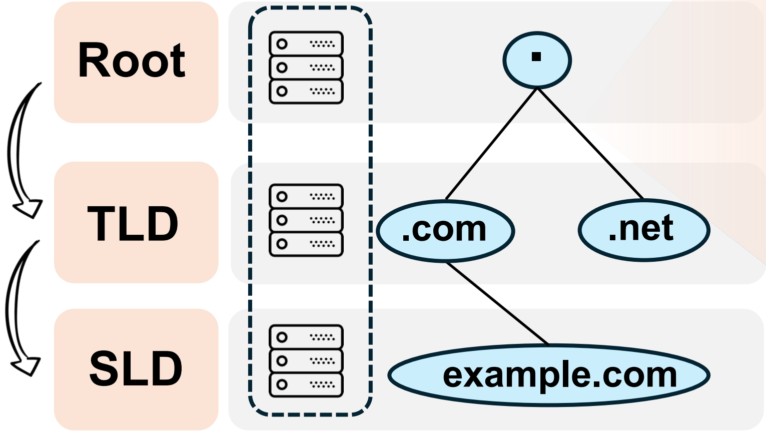
Sibling-domain delegation

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

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.



Types of 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

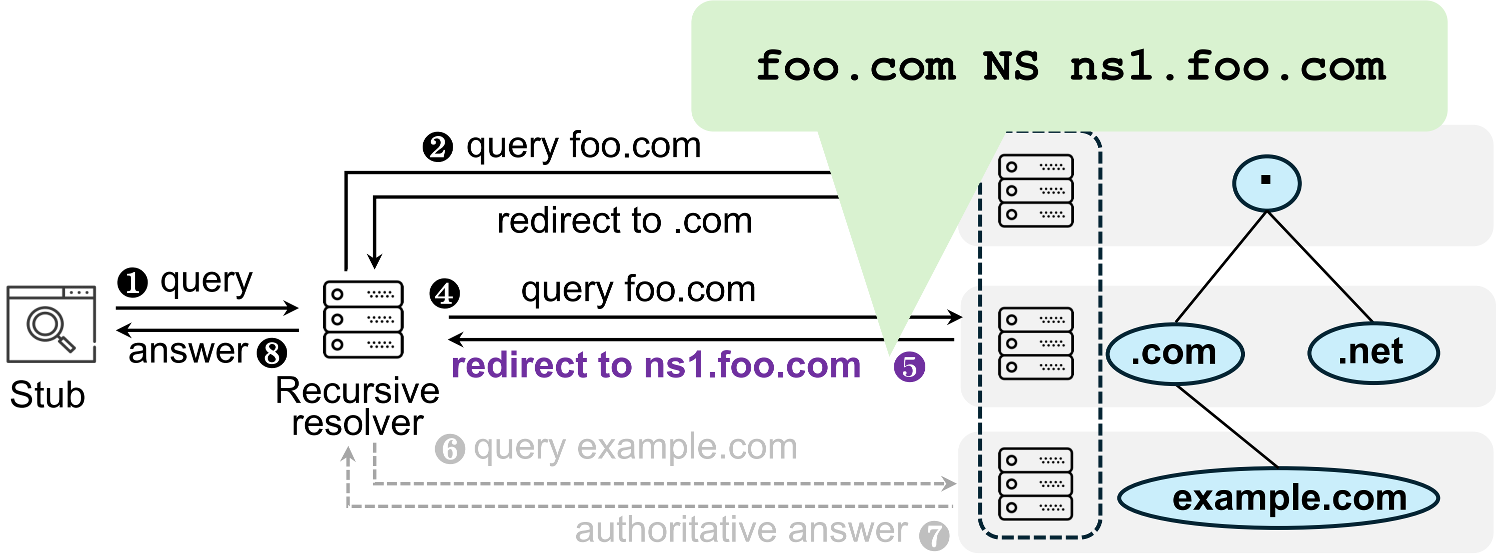
In-domain delegation

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

DNS Glue Records – Resolution Loop

In-domain delegation

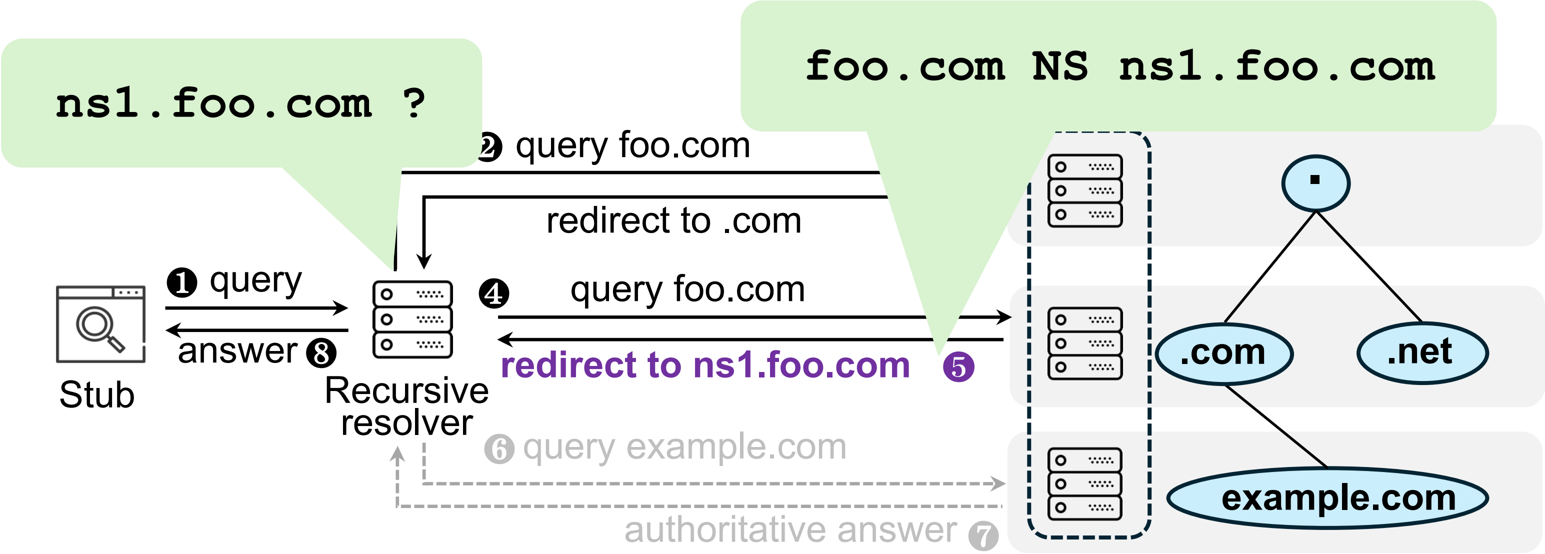
`foo.com NS ns1.foo.com`



DNS Glue Records – Resolution Loop

In-domain delegation

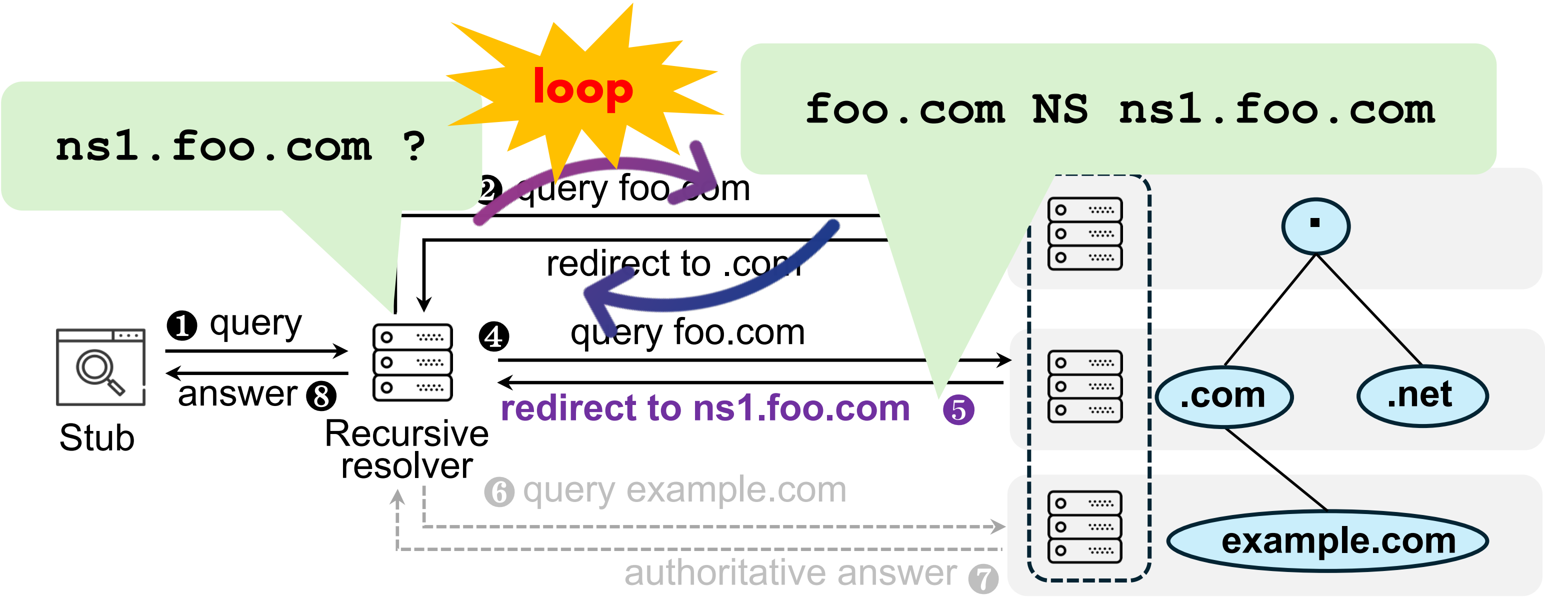
```
foo.com NS ns1.foo.com
```



DNS Glue Records – Resolution Loop

In-domain delegation

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



DNS Glue Records Prevent Resolution Loop

In-domain delegation

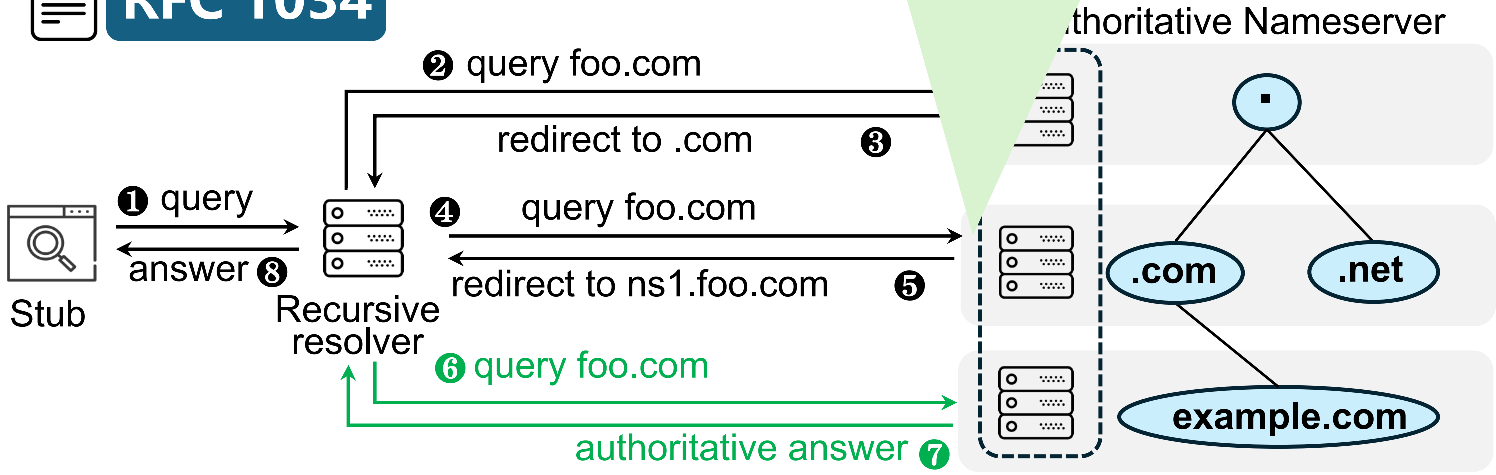
```
foo.com NS ns1.foo.com
```

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

RFC 1034

glue records →

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



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.

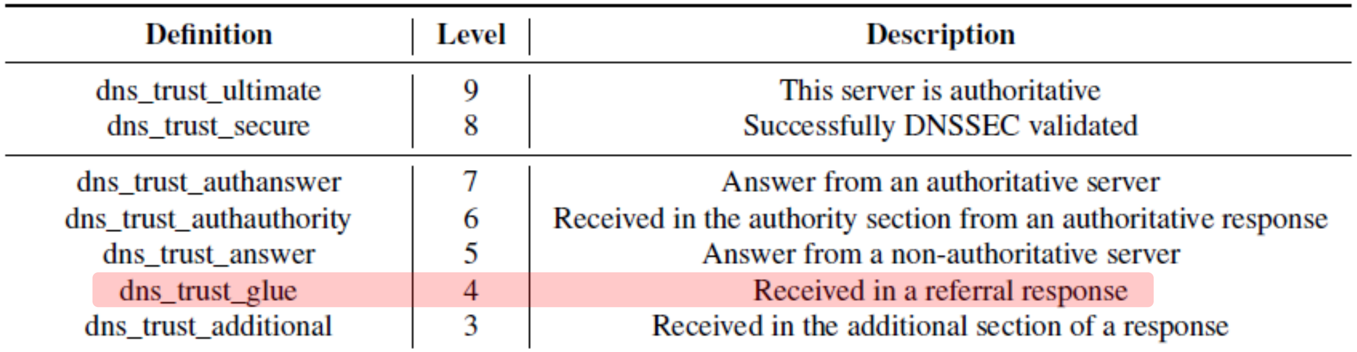
Why the Neglect of Glue Records?

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.***

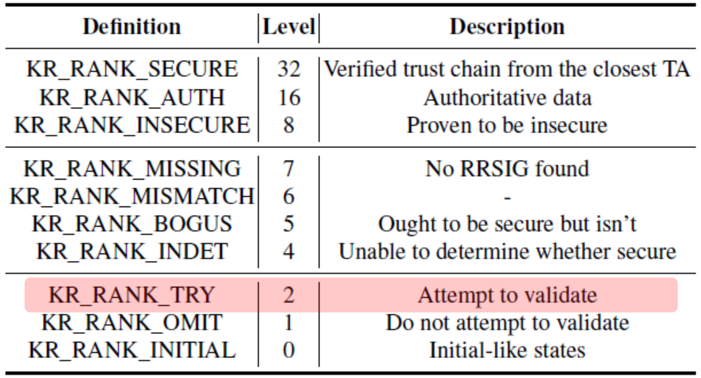
Mainstream DNS software assigns a low trust level to glue records

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 in Zone Files

1,096 TLDs

.com, .net, .org, …

300M+ domain names

2M+ glue records

DNS Glue Records in Zone Files

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 (Correct)
stale.com        NS      ns.stale.com
ns.stale.com     A       4.5.6.8
ns-old.stale.com A       8.8.9.9
```

```
; 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
```

DNS Glue Records in Zone Files

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 (Correct)
stale.com         NS      ns.stale.com
ns.stale.com      A       4.5.6.8 (Stale)
ns-old.stale.com  A       8.8.9.9
```

```
; 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
```

DNS Glue Records in Zone Files

1,096 TLDs

.com, .net, .org, …

300M+ domain names

2M+ glue records

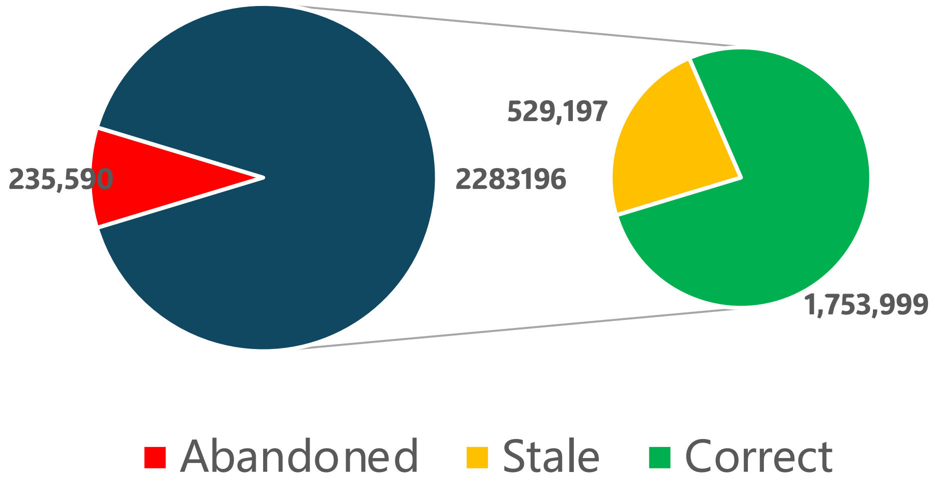
Glue

```
; .com zone file
example.com      NS     ns.example.com
ns.example.com  A      1.2.3.4 (Correct)
stale.com        NS     ns.stale.com
ns.stale.com     A      4.5.6.8 (Stale)
ns-old.stale.com A      8.8.9.9 (Expired)
```

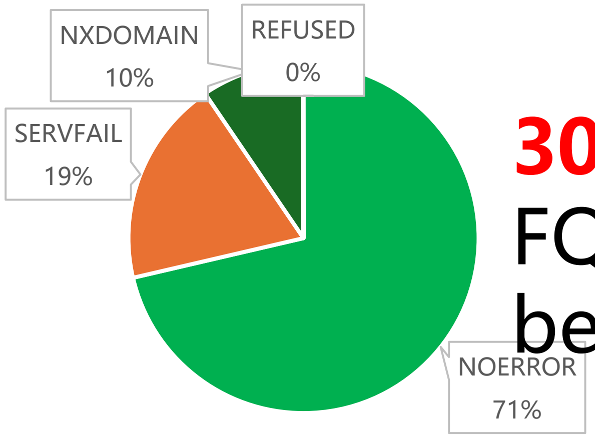
```
; example.com nameserver
example.com      NS     ns. example.com
ns.example.com  A      1.2.3.4
```

```
; stale.com nameserver
ns.stale.com     A      2.3.4.5
```

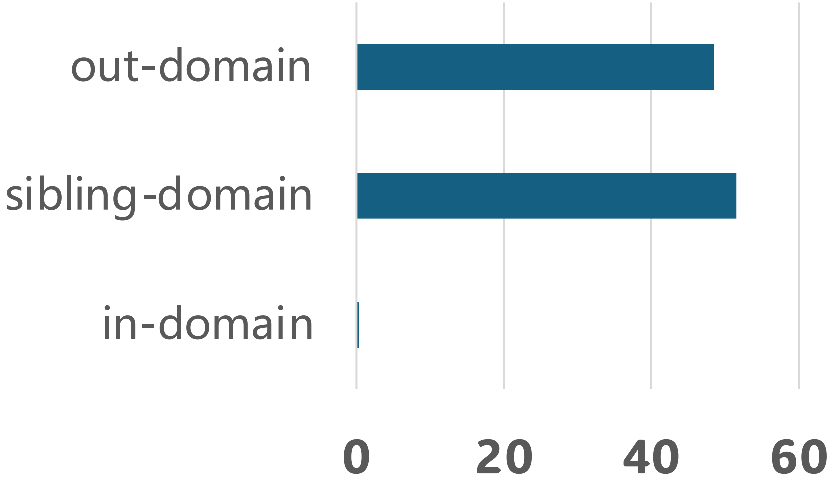
Significant # of Stale and Flawed Glue Records



23.18% of glue records are stale



30% of glue FQDNs cannot be resolved



0.29% of delegation are in-domain delegation

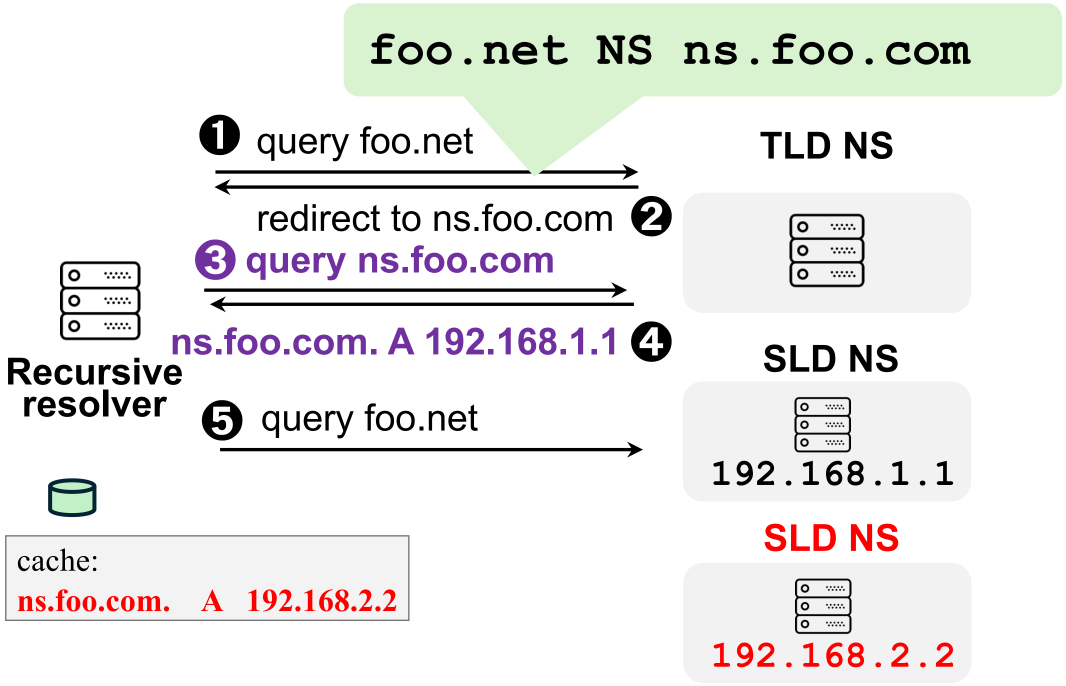
Question

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, out-domain lookups?

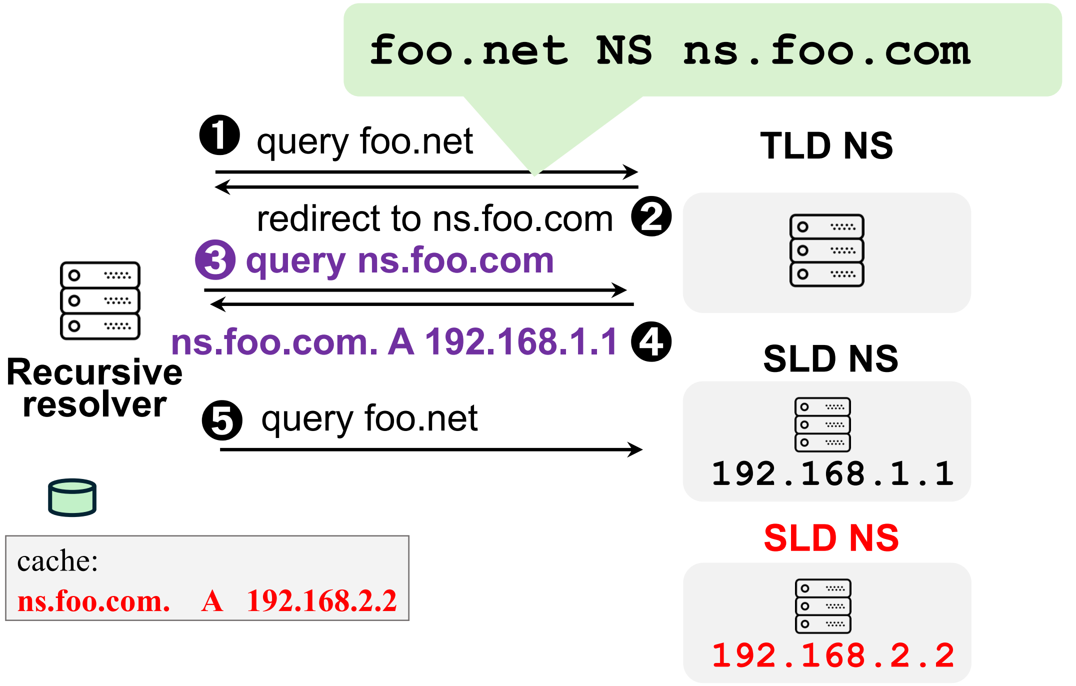


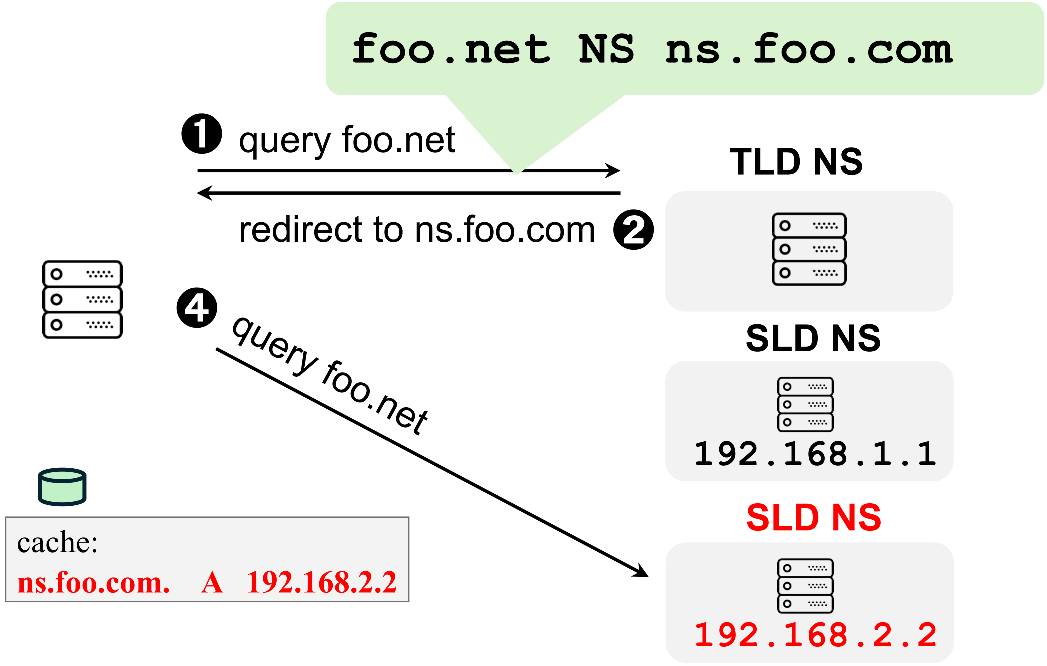
Trusts new glue?

Out-domain delegation

Glue Record Use in DNS software

❖ **Will cached glue records be used in future, out-domain lookups?**





Trusts new glue? ? **Use cached glue?**

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

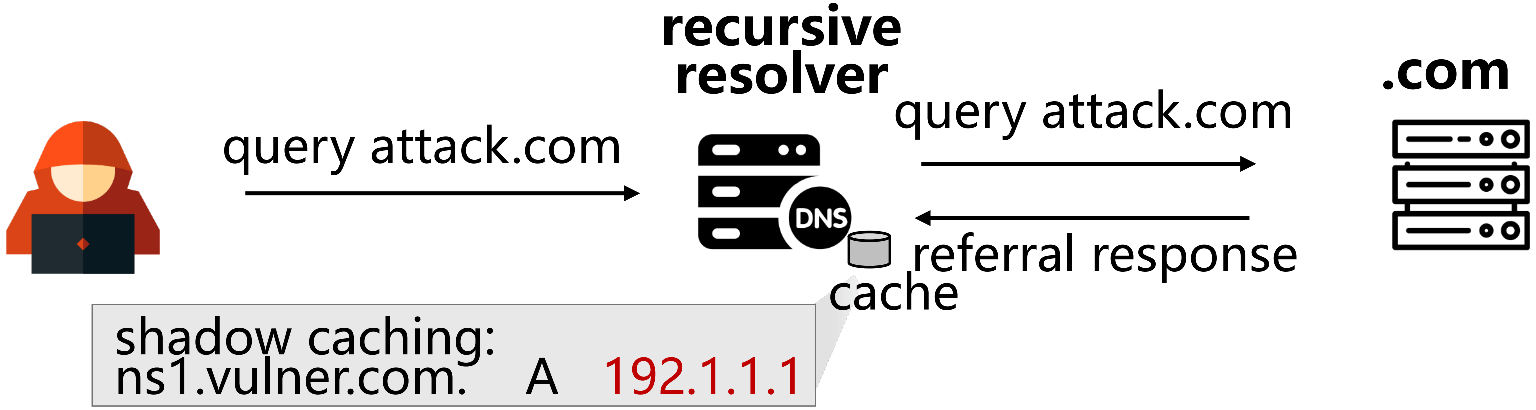
- ❖ **injecting stale glue records to target resolver**
  - ❖ **Step 1: configure delegation relationship**

```
.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**



recursive resolver

.com

query attack.com

query attack.com

referral response

cache

shadow caching:
ns1.vulner.com.   A   192.1.1.1

Shadow Caching – Attack

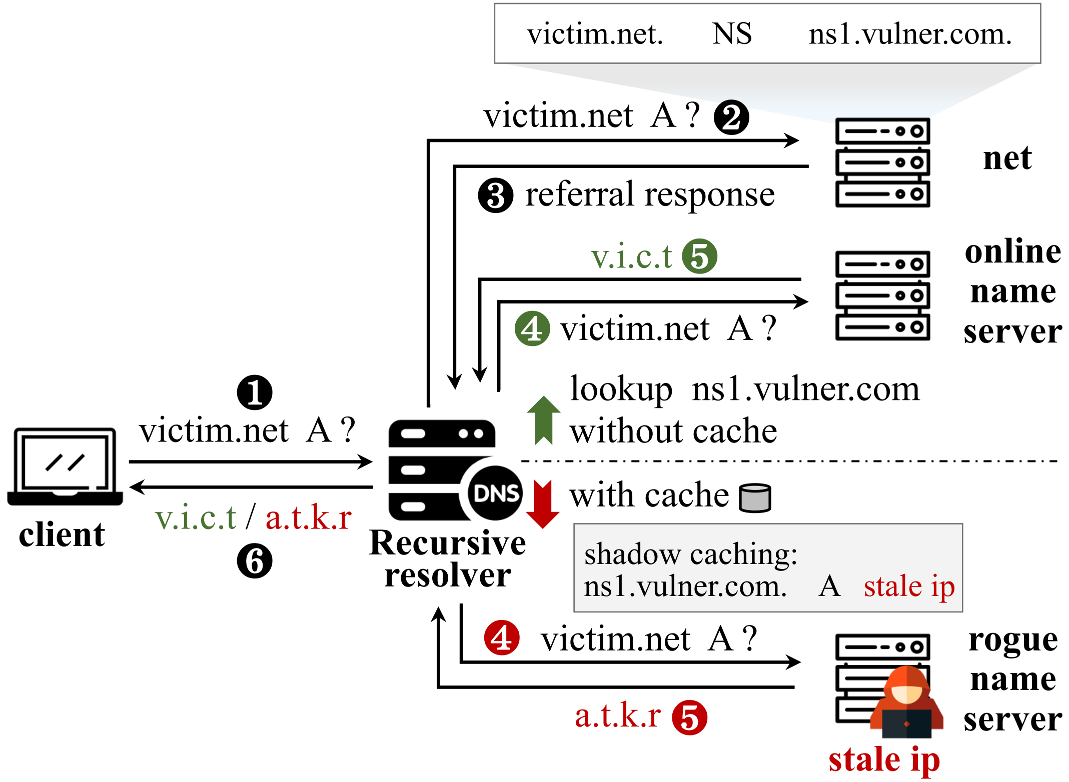
❖ Domain takeover

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

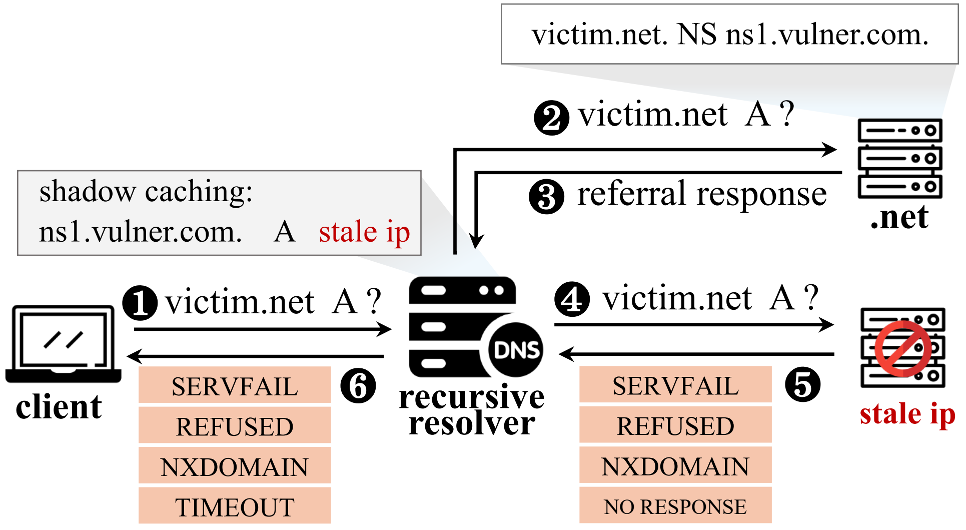
❖ Denial-of-Service

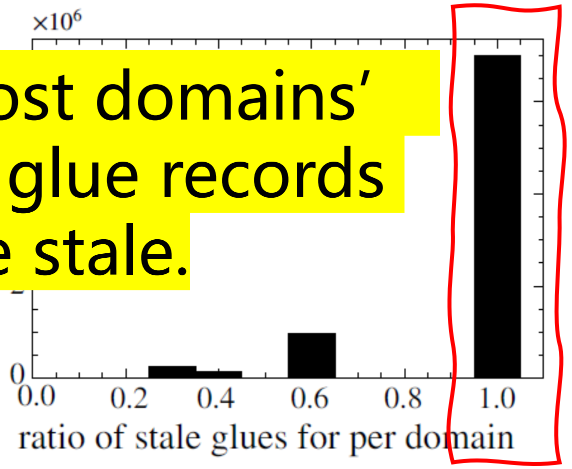
Assumption

- □ 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





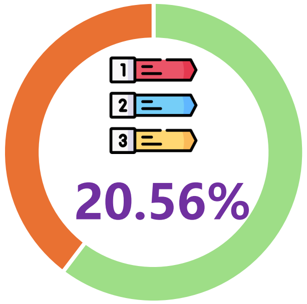
Most domains' all glue records are stale.

Vulnerable Glue Records and Domains

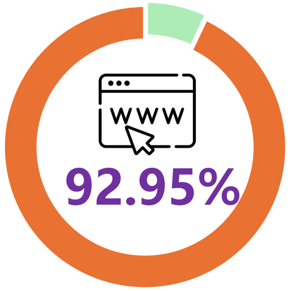
Domain takeover

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**

CoreDNS

BIND 9 POWERDNS KNOT DNS

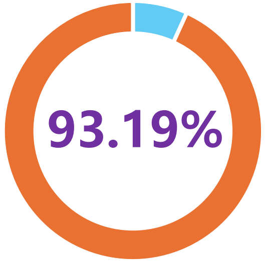
unbound

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

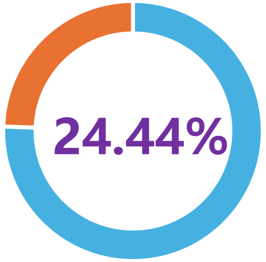
DynDNS Alibaba Cloud 8.8.8.8 quad9

1.1.1.1 Level(3) COMMUNICATIONS CleanBrowsing OpenDNS

- Open Resolvers



Domain takeover



DoS

Discussion & Mitigation

❖ Vulnerability Disclosure

- □ Acknowledged and remediated by **.info** and **.org registry**
- □ Confirmed by 4 affected vendors: PowerDNS, OpenDNS, and Alibaba Cloud DNS, etc.

❖ Root Cause

- □ Poor DNS glue records management
- □ Irregular DNS software behavior

❖ Mitigation Solution

- □ Enhance management of delegation records
- □ Avoid using glue record caching under out-domain delegation

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**
- **Comprehensive evaluation**
  - □ over 6 million domains are vulnerable
  - □ 90% of open resolvers and 14 public DNS are vulnerable

Thanks!
Questions?

Presenter: **Chaoyi Lu**, Tsinghua University
https://chaoyi.lu

Author Email:
zhangyyzyy@nudt.edu.cn