MMLAB Main Seminar

*** stale*** (of food) no longer fresh and pleasant to eat.

Rethinking the Security Threats of Stale* DNS Glue Records

Yunyi Zhang (National University of Defense Technology, Tsinghua University), Et Al

Distinguished Paper Award
USENIX Security Symposium 2024 (August 14-16, 2024)

清華大學
Tsinghua University

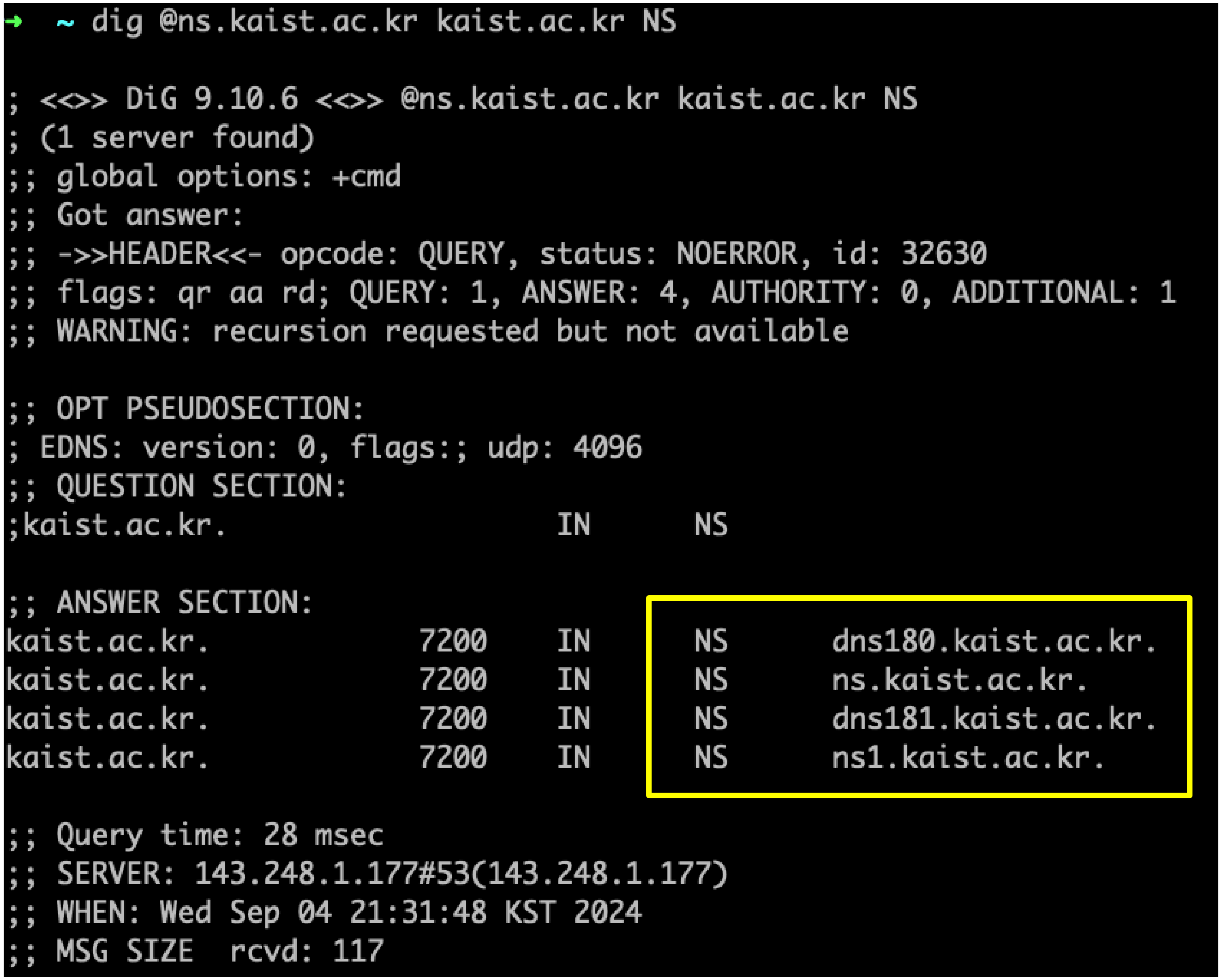
Hyunsoo Kim (hskim@mmlab.snu.ac.kr)

2024. 09. 10

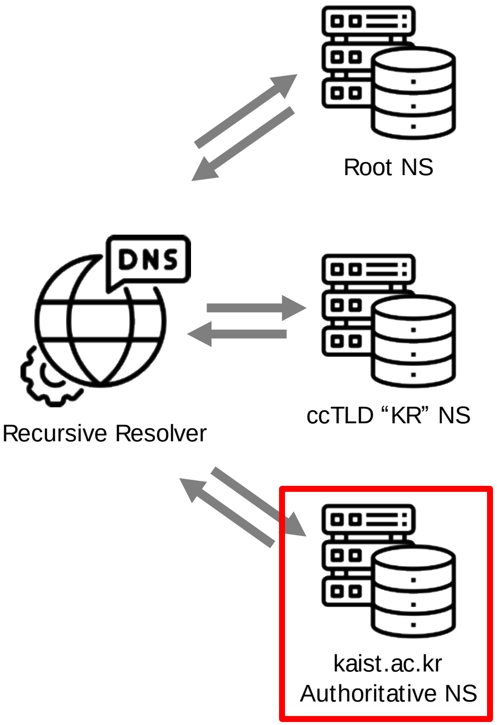
서울대학교
SEOUL NATIONAL UNIVERSITY

MMLab
Network Convergence & Security Lab

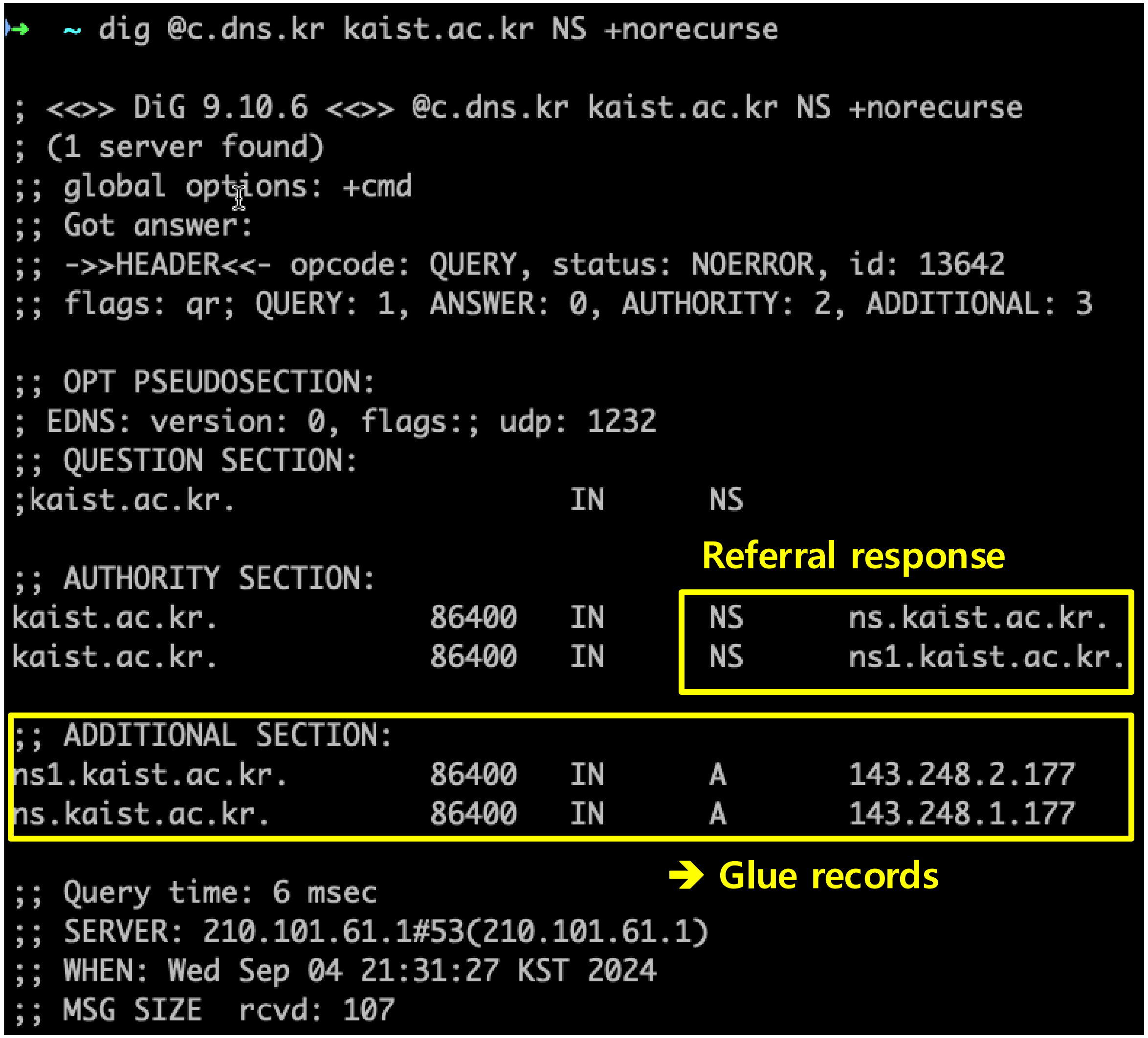
NS Records of kaist.ac.kr @ns.kaist.ac.kr



```
➜  ~ dig @ns.kaist.ac.kr kaist.ac.kr NS

; <<>> DiG 9.10.6 <<>> @ns.kaist.ac.kr kaist.ac.kr NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32630
;; flags: qr aa rd; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;kaist.ac.kr.                   IN      NS

;; ANSWER SECTION:
kaist.ac.kr.            7200    IN      NS      dns180.kaist.ac.kr.
kaist.ac.kr.            7200    IN      NS      ns.kaist.ac.kr.
kaist.ac.kr.            7200    IN      NS      dns181.kaist.ac.kr.
kaist.ac.kr.            7200    IN      NS      ns1.kaist.ac.kr.

;; Query time: 28 msec
;; SERVER: 143.248.1.177#53(143.248.1.177)
;; WHEN: Wed Sep 04 21:31:48 KST 2024
;; MSG SIZE  rcvd: 117
```



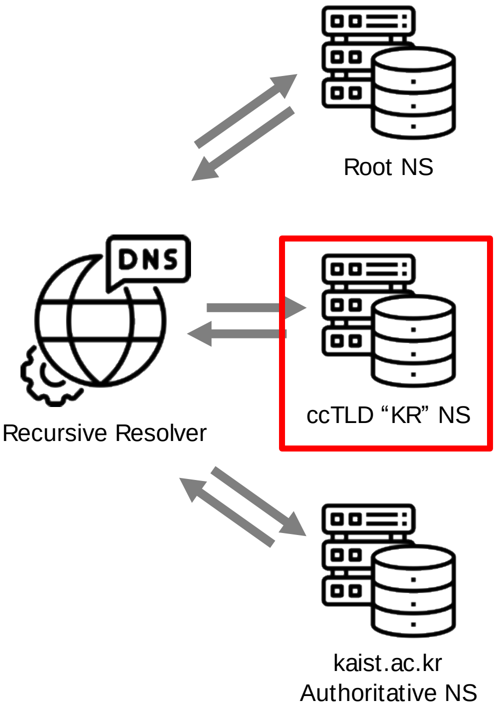
NS Records of kaist.ac.kr @KR ccTLD [Parent Zone]



```
→  ~ dig @c.dns.kr kaist.ac.kr NS +norecurse

; <<>> DiG 9.10.6 <<>> @c.dns.kr kaist.ac.kr NS +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13642
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;kaist.ac.kr.                   IN      NS

;; AUTHORITY SECTION:
kaist.ac.kr.            86400   IN      NS      ns.kaist.ac.kr.
kaist.ac.kr.            86400   IN      NS      ns1.kaist.ac.kr.

;; ADDITIONAL SECTION:
ns1.kaist.ac.kr.        86400   IN      A       143.248.2.177
ns.kaist.ac.kr.         86400   IN      A       143.248.1.177

;; Query time: 6 msec
;; SERVER: 210.101.61.1#53(210.101.61.1)
;; WHEN: Wed Sep 04 21:31:27 KST 2024
;; MSG SIZE  rcvd: 107
```

Referral response

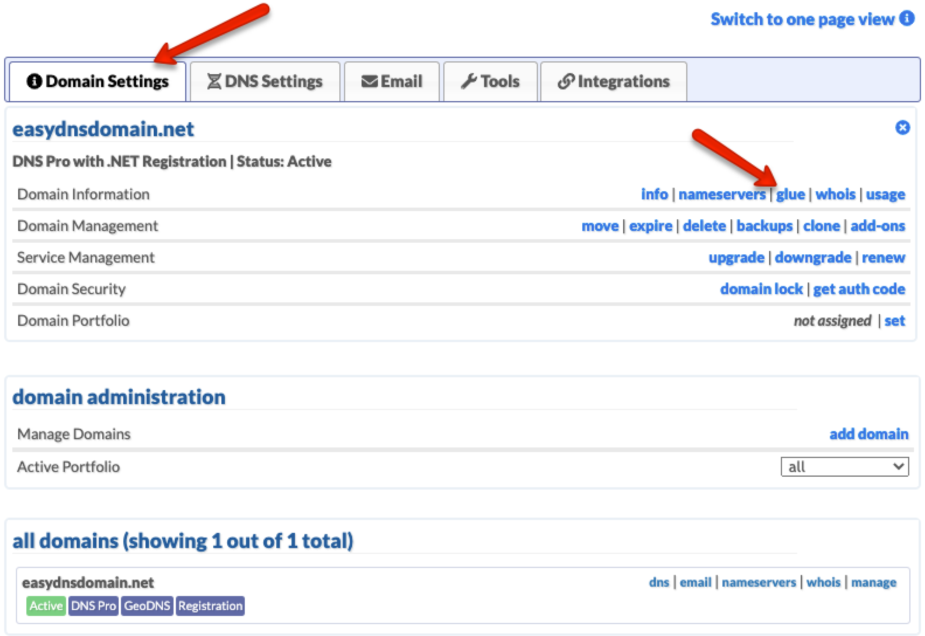
→ Glue records



Background – Glue Records

- Specific **A records** of delegated nameservers in the DNS zone
  - Prevents resolution loop in “in-domain delegation” or “in-bailiwick”
  - RFC states that glue records are only used as part of a referral response
- Domain owners may configure their glue records via web interface

figuration of glue records



easydnsdomain.net

DNS Pro with .NET Registration | Status: Active

Domain Information	info | nameservers | glue | whois | usage
Domain Management	move | expire | delete | backups | clone | add-ons
Service Management	upgrade | downgrade | renew
Domain Security	domain lock | get auth code
Domain Portfolio	*not assigned* | set

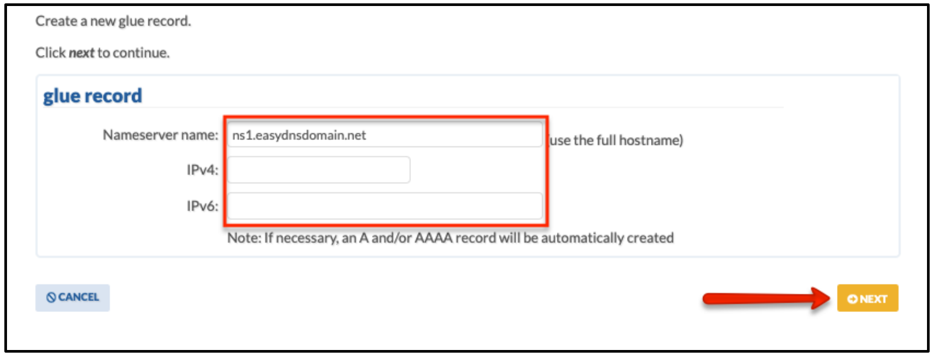
domain administration

Manage Domains	add domain
Active Portfolio	all

all domains (showing 1 out of 1 total)

easydnsdomain.net — dns | email | nameservers | whois | manage

Active DNS Pro GeoDNS Registration



Create a new glue record.

Click *next* to continue.

glue record

Nameserver name: ns1.easydnsdomain.net use the full hostname)

IPv4:

IPv6:

Note: If necessary, an A and/or AAAA record will be automatically created

Background – Domain Delegations (1)

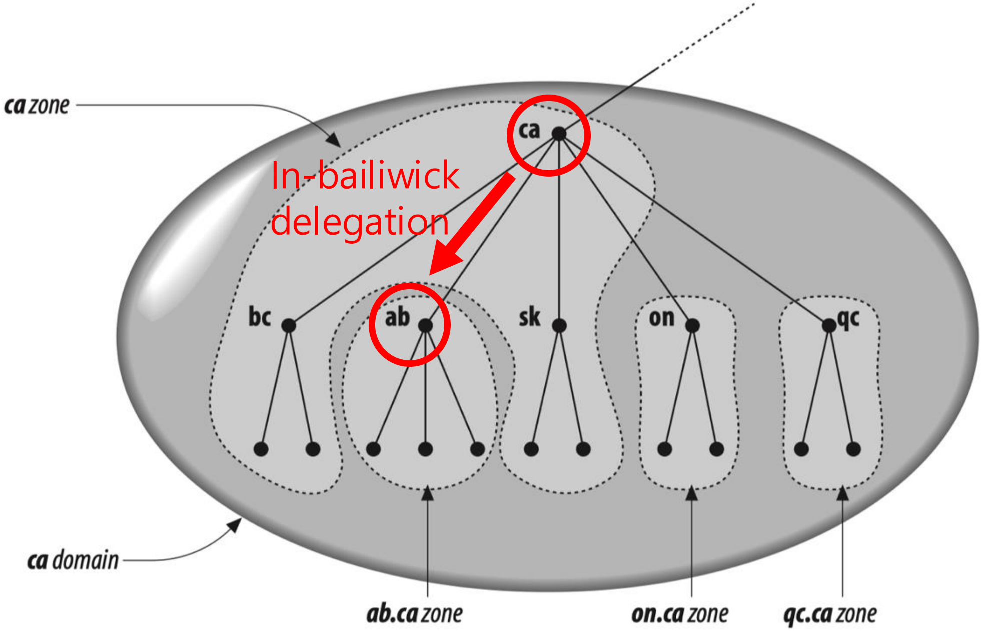
- "In-bailiwick" or "In-domain" delegation

;;NS RR

ab.ca.	NS	ns.ab.ca

;;Glue records in .ca zone

ns.ab.ca A	9.5.6.6

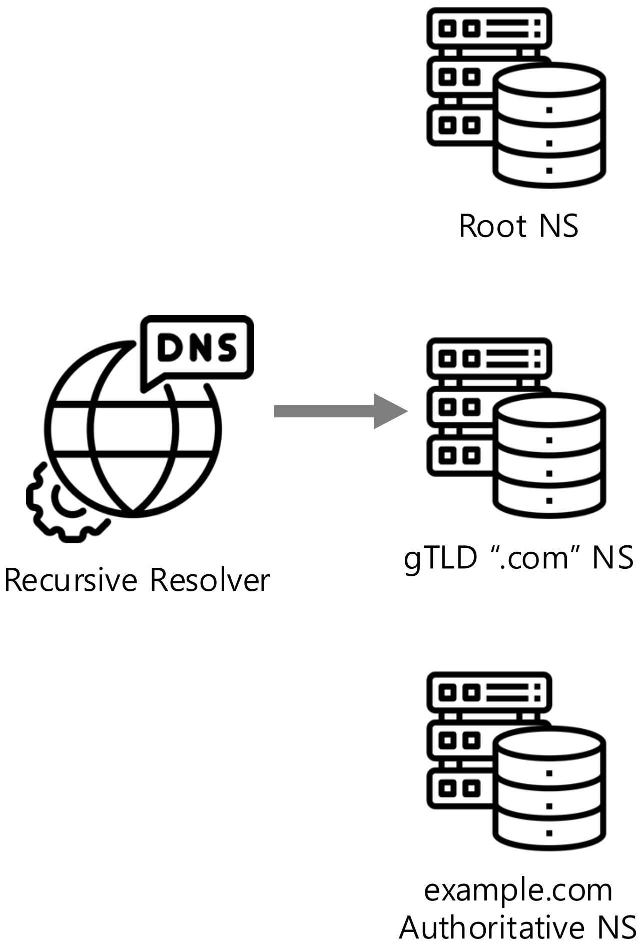


Glue Records Prevents Resolution Loop

- Assume no glue record,
  i.e. A record of ns.example.com

1. The recursive resolver queries the .com TLD for example.com
2. .com TLD gives the referral response where it tells the NS record of example.com is ns.example.com
3. The recursive resolver now needs to resolve ns.example.com which is a subdomain of example.com
4. The recursive resolver queries the .com TLD for example.com

➔ Loop



Background – Domain Delegations (2)

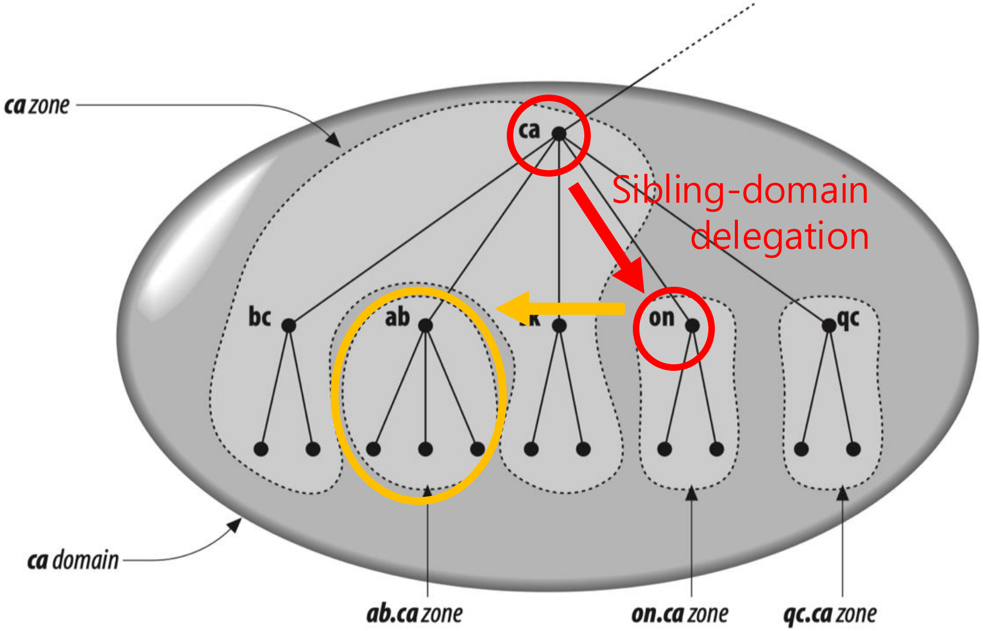
- "Out-of-bailiwick" → "Sibling-domain" delegation

;;NS RR

ab.ca.   NS   ns.on.ca

;;Glue records in .ca zone

ns.on.ca A   9.8.4.1



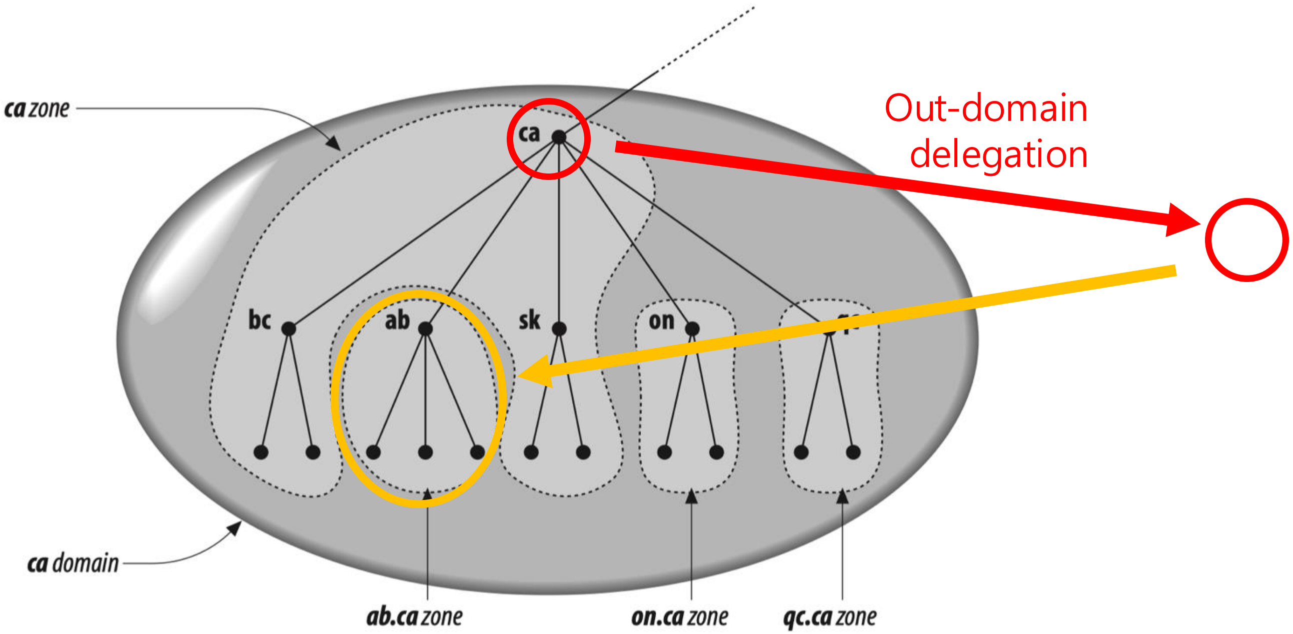
Background – Domain Delegations (3)

- "Out-of-bailiwick" → "out-domain" delegation

;;NS RR

ab.ca.   NS   ns.ya.hoo

[No glue records]



Out-domain delegation

Stale Glue Records

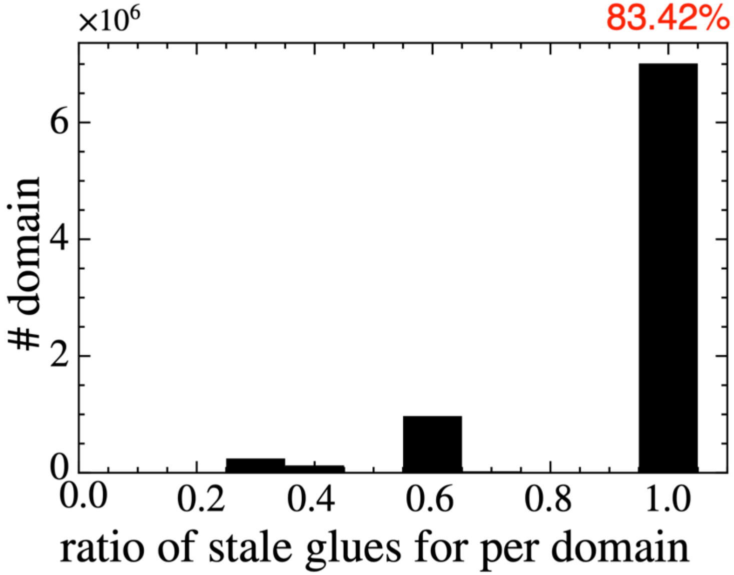
- Abandoned glue records
  - When domain owners change their authoritative nameserver's IP
  - When the domain is expired or the nameserver is deprecated

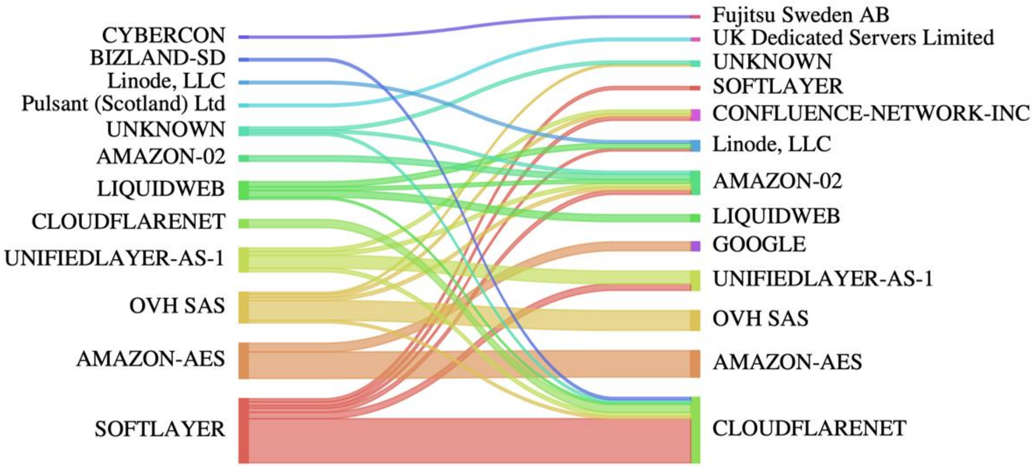
- Finding stale glue records

1. Glue record IP does not match the authoritative nameserver's IP
   - Authoritative nameserver's IP can be found by actively resolving the NS record
2. Glue record domain does not provide services for the delegated domains

Stale Glue Records Measurement

- Dataset: ICANN Centralized Zone Data Service (CZDS)
  - Authorized zone files for 1,096 TLDs (e.g., com, net, org, …)
  - Delegation information for all its associated SLDs
- 2,283,196 glue records found
- 529,197 stale glue records (23.18%)
  - Glue record IP (Old) → Current IP migration occurs in cloud platforms





Glue Records Usage of DNS Implementaion

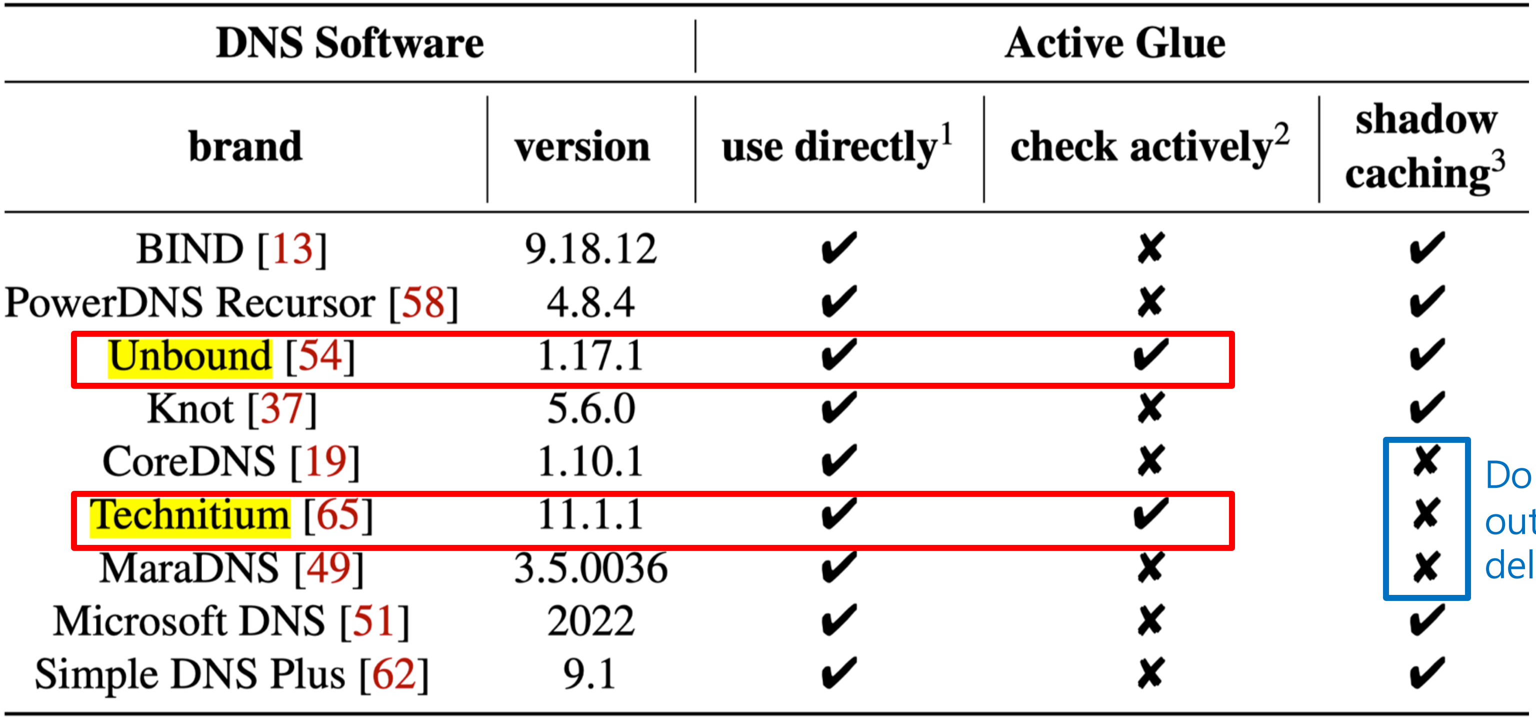
- A typical user (stub resolver) sending recursive queries will never see glue records

- DNS software usage of glue records
  - Does DNS software validate glue records before use?
  - Whether the software caches unvalidated glue records?
  - How does the software handle it when no response is received from the Glue IP?

- DNS resolvers' usage of glue records
  - Public DNS: 14 (1.1.1.1, 8.8.8.8, 9.9.9.9, …)
  - Open DNS resolvers: 895,674

Glue Records Usage of DNS Implementaion

- Most DNS software cache and use glue records without validation
- For out-domain delegation, this behavior results in ***shadow caching***, which enables domain hijacking and DoS attacks

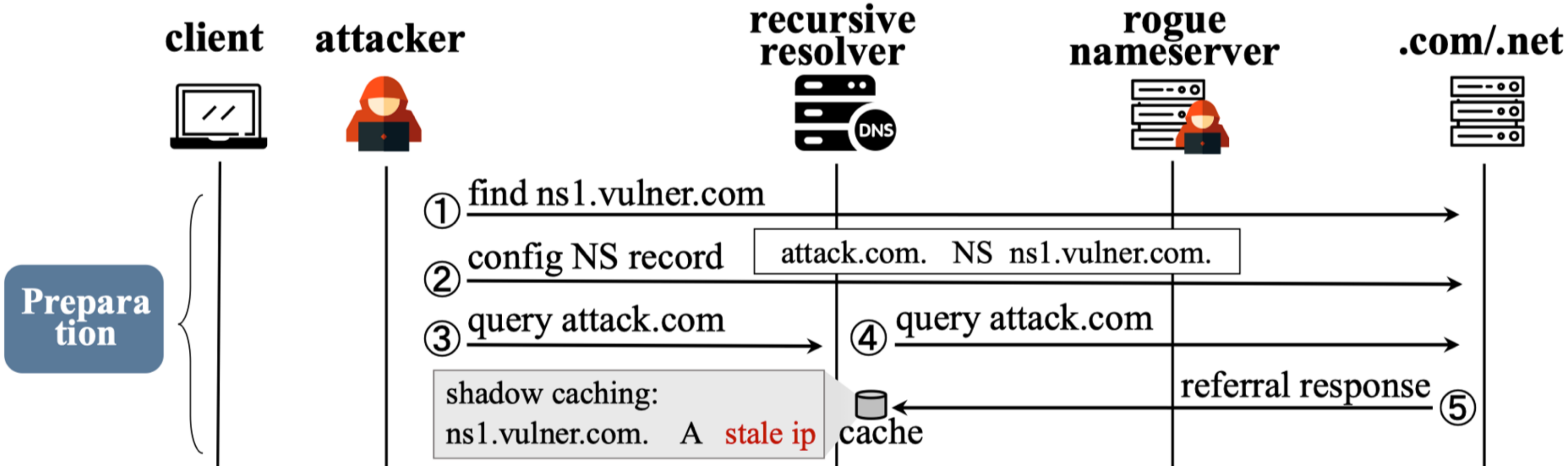


DNS Software		Active Glue		
brand	version	use directly[1]	check actively[2]	shadow caching[3]
BIND [13]	9.18.12	✔	✘	✔
PowerDNS Recursor [58]	4.8.4	✔	✘	✔
Unbound [54]	1.17.1	✔	✔	✔
Knot [37]	5.6.0	✔	✘	✔
CoreDNS [19]	1.10.1	✔	✘	✘
Technitium [65]	11.1.1	✔	✔	✘
MaraDNS [49]	3.5.0036	✔	✘	✘
Microsoft DNS [51]	2022	✔	✘	✔
Simple DNS Plus [62]	9.1	✔	✘	✔

Does not cache out-domain delegation records

Shadow Caching

- Glue records are only allowed to be used under in-domain or sibling-domain delegation
  - For out-domain delegation, the referral response should not contain glue records
- Mainstream DNS software caches the glue records in the referral response
- By creating sibling-domain delegation, we can inject specific stale glue records into the target resolver in advance → *shadow*



Preparation Phase (1)

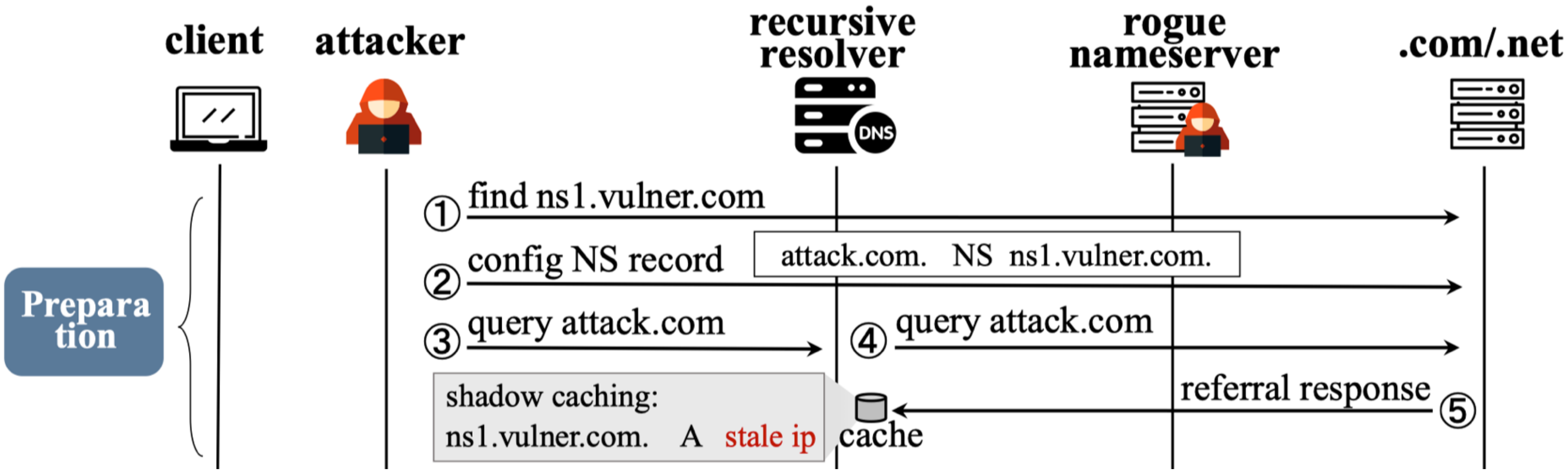
- Find stale glue record that matches the victim's NS

;;NS RR

victim.net. NS ns1.vulner.com

➔ Stale glue record found

ns1.vulner.com A (stale IP)



Preparation Phase (2)

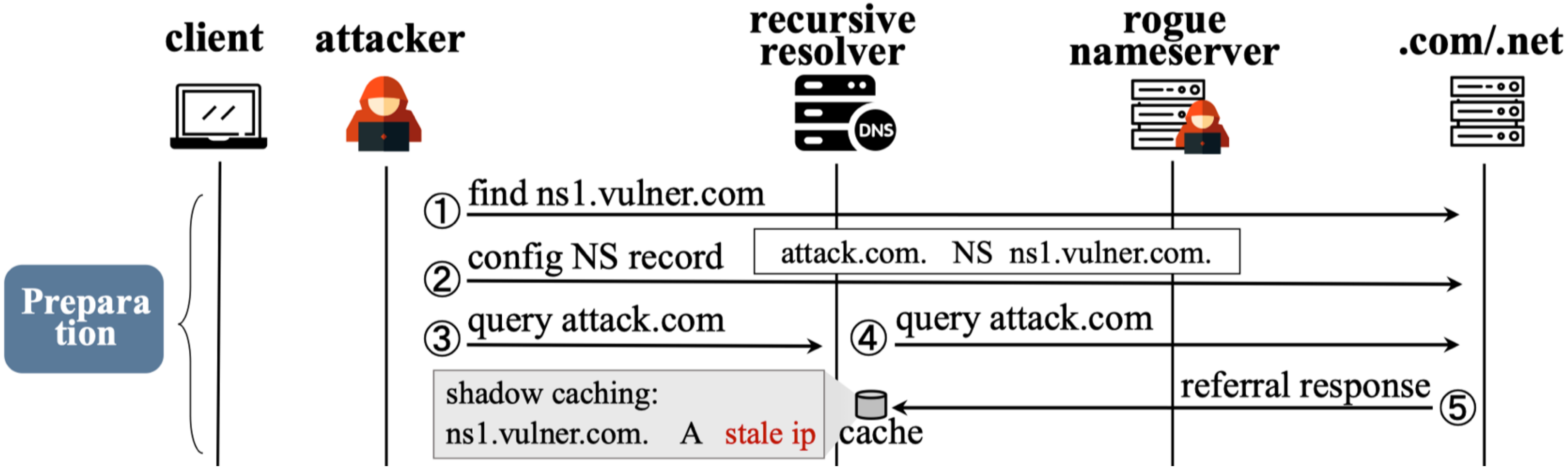
- Register attack.com and the following sibling-domain glue record

;;NS RR

attack.com. NS ns1.vulner.com

;;Glue records in .com zone

ns1.vulner.com A (stale IP)

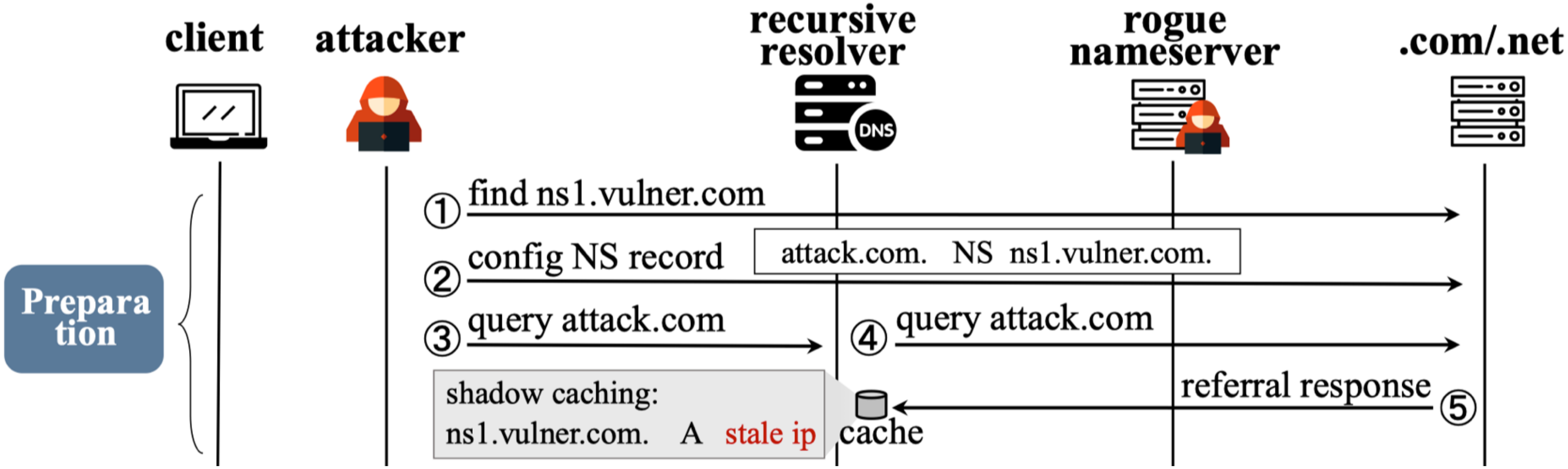


Preparation Phase (3) – (4)

- Query attack.com

➔ Glue record is now cached in the recursive resolver

ns1.vulner.com A (stale IP)

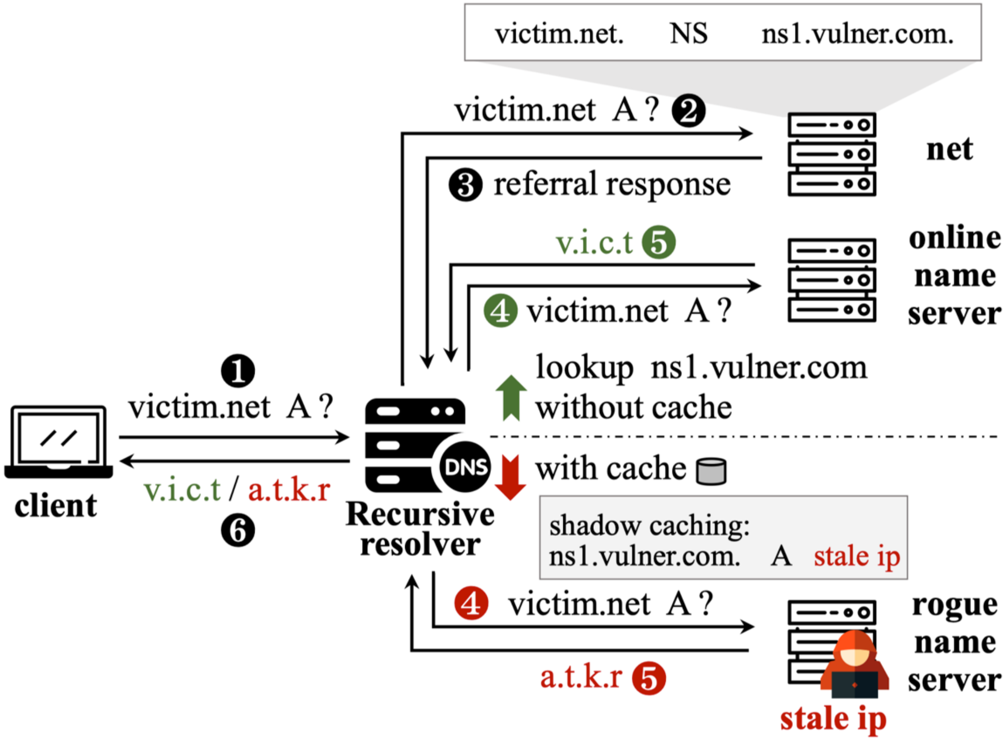


Attack vectors

- If (stale IP) is obtainable
  - E.g., Acquiring and releasing cloud IPs for (stale IP)

➔ Domain hijacking

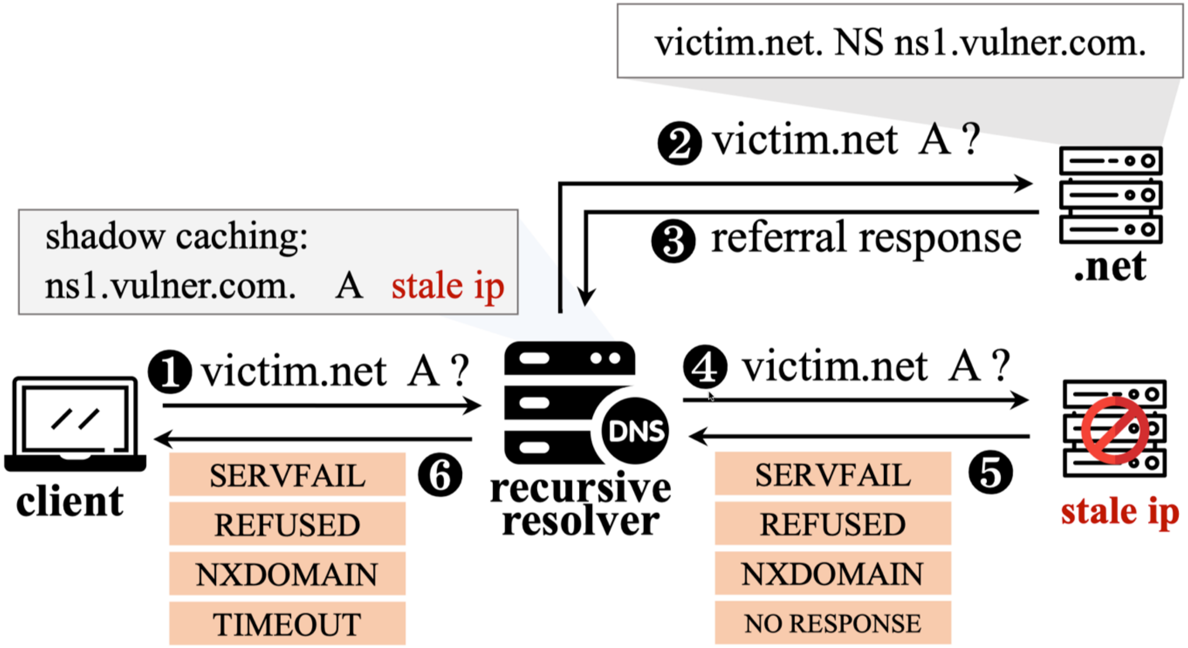
victim.net. NS ns1.vulner.com → (stale IP)



Attack vectors

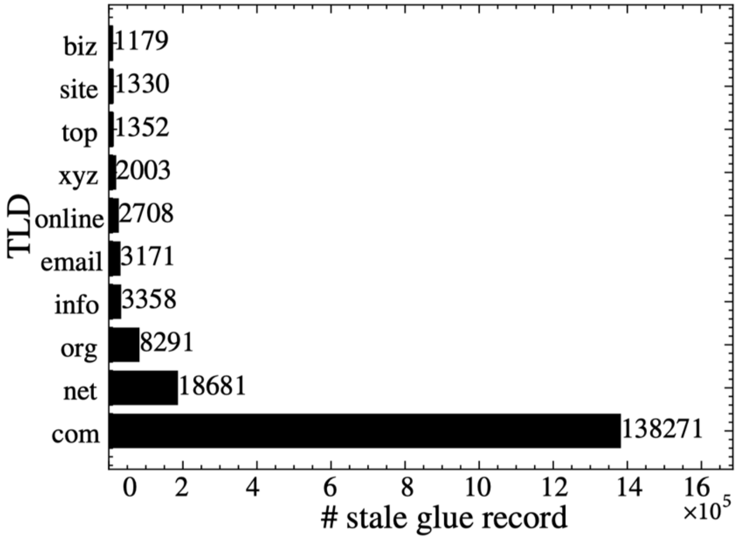
- If (stale IP) is not obtainable

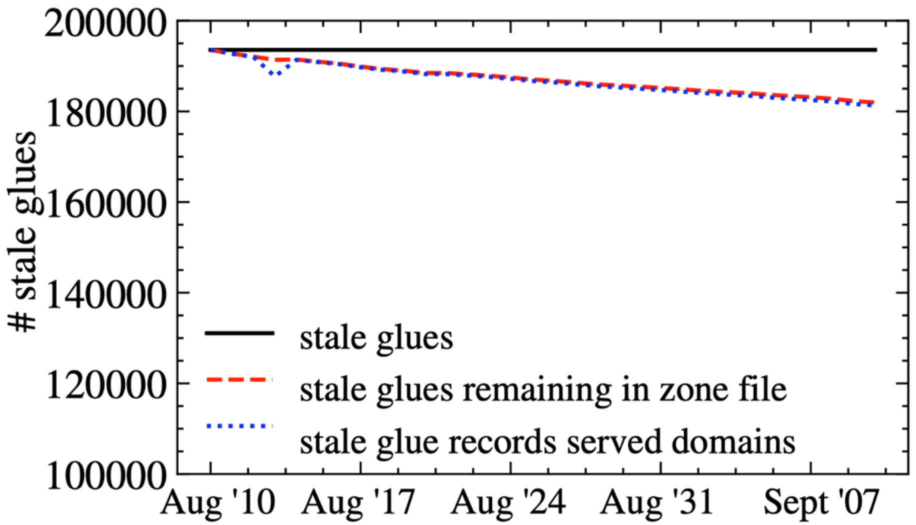
➔ Denial of Service (DoS)



Exploitable Stale Glue Records Measurement

- 2,283,196 glue records found → 529,197 stale glue records
- 193,558 exploitable stale glue records
  - 6M domain names, among 5,395 were ranked in Tranco Top 1M
- Acquiring (stale IP)s within two weeks
  - Successfully applied for 27 stale IPs, costing $2.3 total





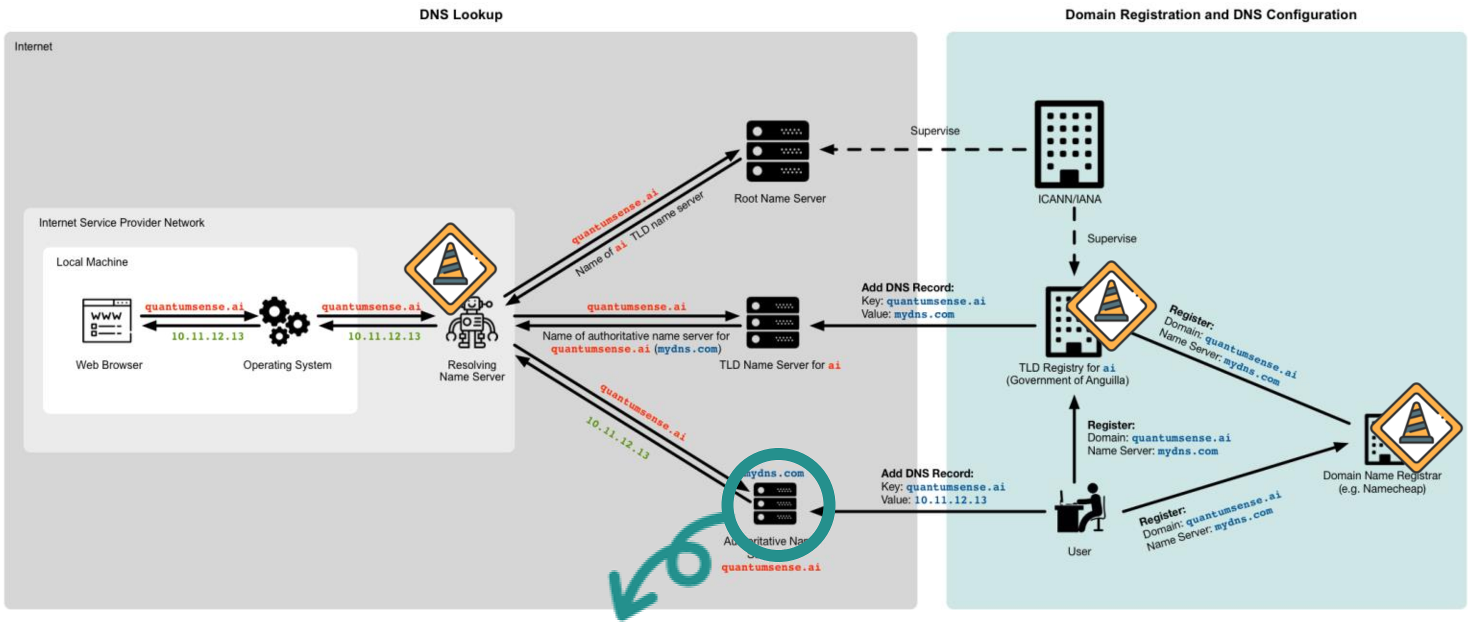
Glue Records Usage of DNS Implementaion

- Public resolvers: 14
  - All 14 public DNS resolvers are vulnerable to in-domain and sibling-domain hijacking
  - Only 1.1.1.1 (Cloudflare) and 8.8.8.8 (Google) trust the records they resolve actively instead of using glue records under out-domain delegation

- Open DNS resolvers: 895,674
  - Over 90% of resolvers cache and use unvalidated glue records

Mitigations

- Registrars and Registries
  - Registrars comprehensive cleanup of all invalid glue records
  - Standardization of proper operations on expired domains
- Resolver software
  - For sibling-domain and out-domain delegations
    → Actively query the IP of the glued nameserver domain



감사합니다

Thank you~!