Ghost Domain Reloaded: Vulnerable Links in Domain Name Delegation and Revocation

Xiang Li, Baojun Liu, Xuesong Bai, Mingming Zhang, Qifan Zhang,
Zhou Li, Haixin Duan, and Qi Li

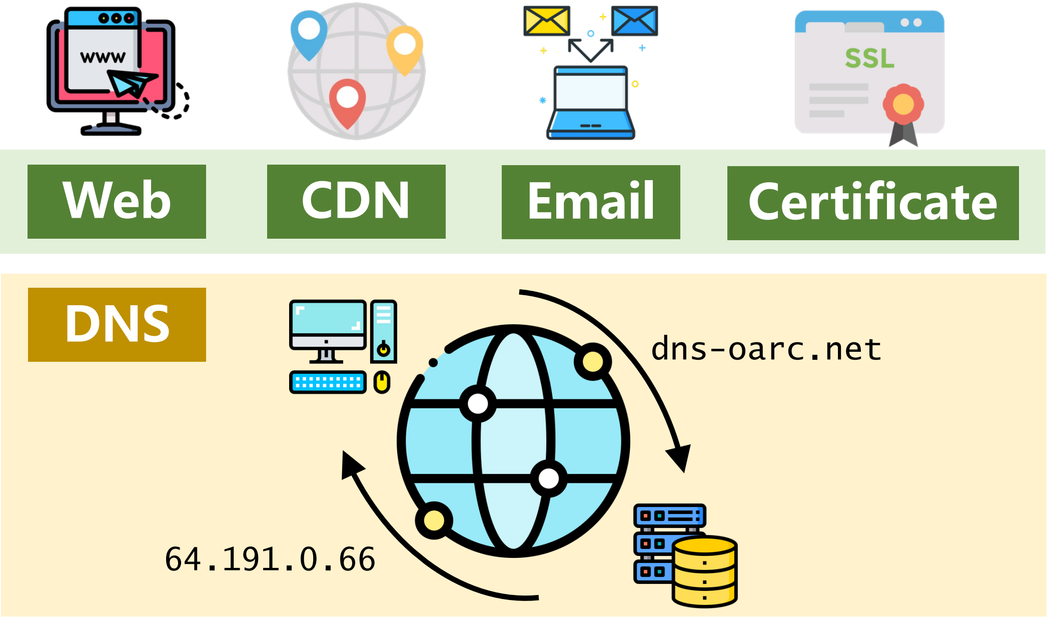
(Accepted by [NDSS 2023])

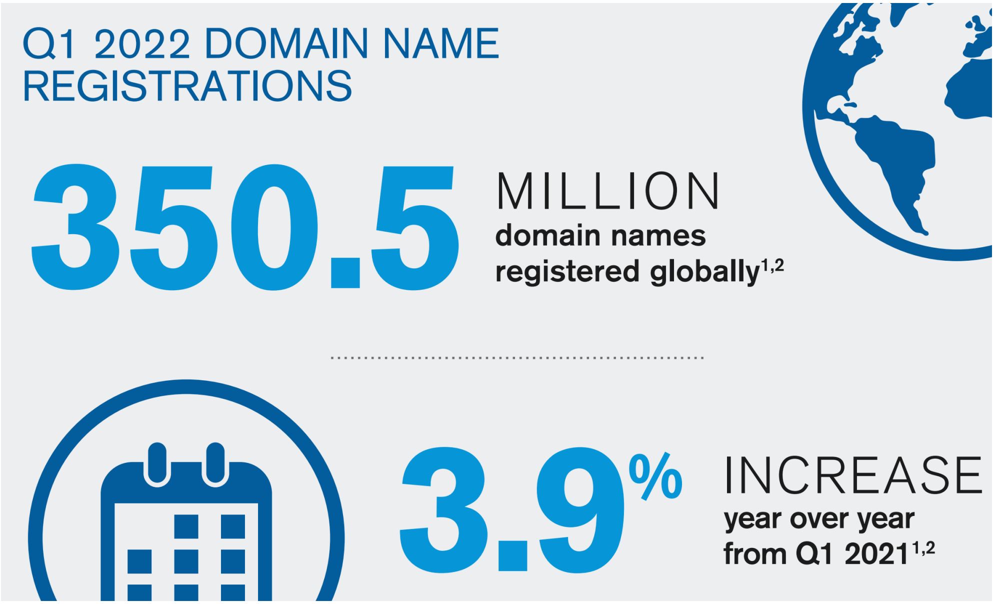
Presenter: **Xiang Li**, Tsinghua University
October 23rd, 2022

Domain Name

➢Domain name system (DNS)

- ➢Entry point of many Internet activities
- ➢Security guarantee of multiple application services
- ➢Domain names are widely registered





Q1 2022 DOMAIN NAME REGISTRATIONS

350.5 MILLION domain names registered globally[1,2]

3.9% INCREASE year over year from Q1 2021[1,2]

Cited from verisign.com/dnib

Domain Name Abuse

- **Also abused by criminal activities**
  - Botnet, phishing, malware distribution

Cited from bleepingcomputer.com

Cited from scmp.com

YOU WIN!
Malvertising
Viruses
Worms
{>_}
Fileless malware
Trojans
Rootkits
Ransomware
Spyware
Adware
Bots or botnets

Cited from norton.com

Domain Name Abuse

- **Also abused by criminal activities**
  - Botnet, phishing, malware distribution
- **ICANN Domain abuse activity reporting (DAAR)**
  - In August 2022
  - Check 215,648,084 domain names within 406 gTLDs

468,562 domains showing security threats

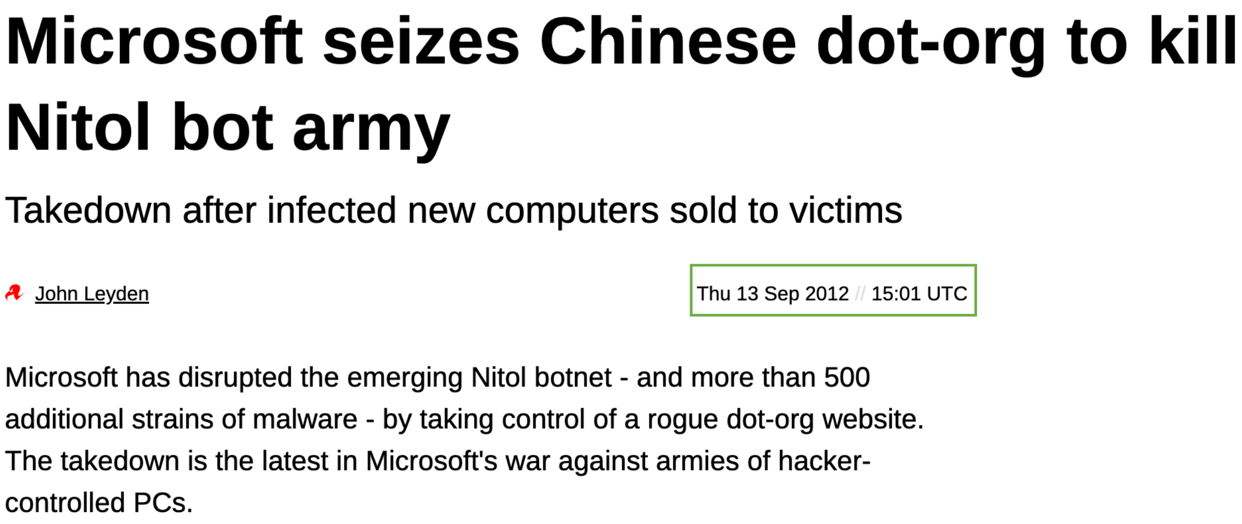
Domain Name Revocation

- **Fighting against malicious domain names**
- **Mechanism**
  - Domain name revocation
  - Operated by registries or registrars
  - Deleting or changing domain name registration (delegation)
- **Result**
  - Domains are no longer controlled by original registrants/attackers

Domain Name Revocation

➢Domain name seizure activity

- ➢Best security practice
- ➢Widely adopted



Microsoft seizes Chinese dot-org to kill Nitol bot army

Takedown after infected new computers sold to victims

John Leyden

Thu 13 Sep 2012 // 15:01 UTC

Microsoft has disrupted the emerging Nitol botnet - and more than 500 additional strains of malware - by taking control of a rogue dot-org website. The takedown is the latest in Microsoft's war against armies of hacker-controlled PCs.

Cited from theregister.com

US leads seizure of one of world’s largest hacker forums and arrests administrator

ENTERPRISE SECURITY GOVERNMENT LATEST THREATS TOP STORIES

Alix Pressley | 14 April, 2022

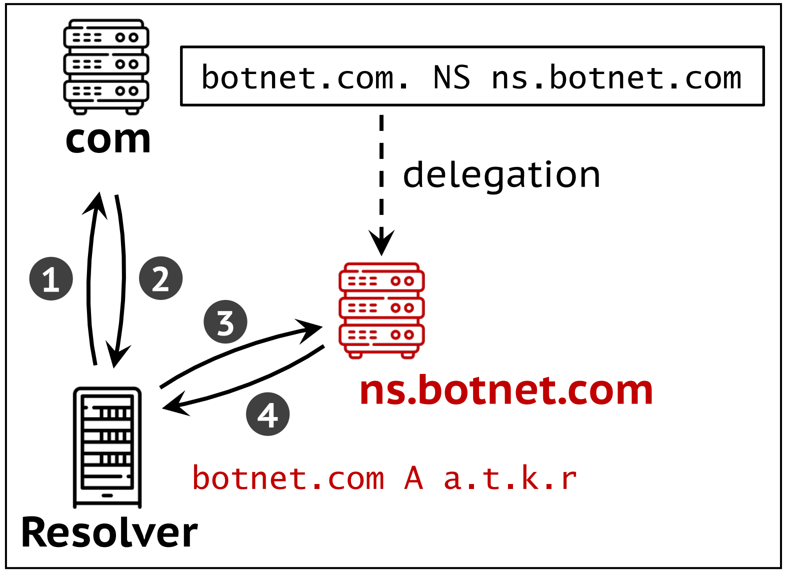
Cited from intelligentciso.com

How does domain name revocation work on domain name registration (delegation)?

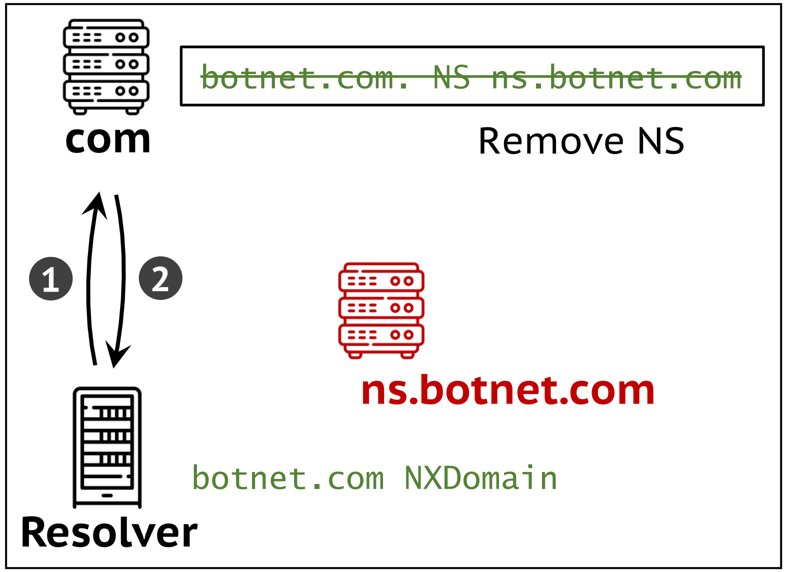
It is the reverse process of delegation.

Domain Name Revocation

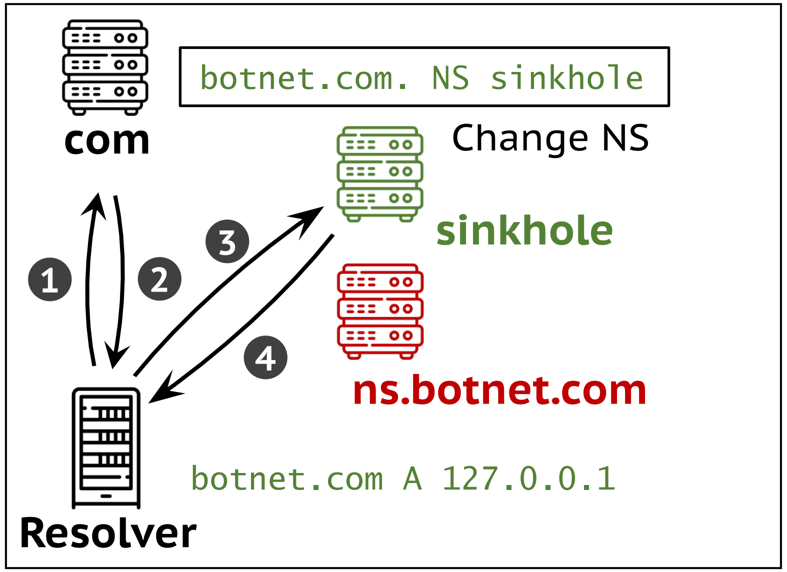
- **Normal resolution**
- **Revocation**
  - Domain delisting
  - Domain sinkholing



Normal resolution



Domain delisting



Domain sinkholing

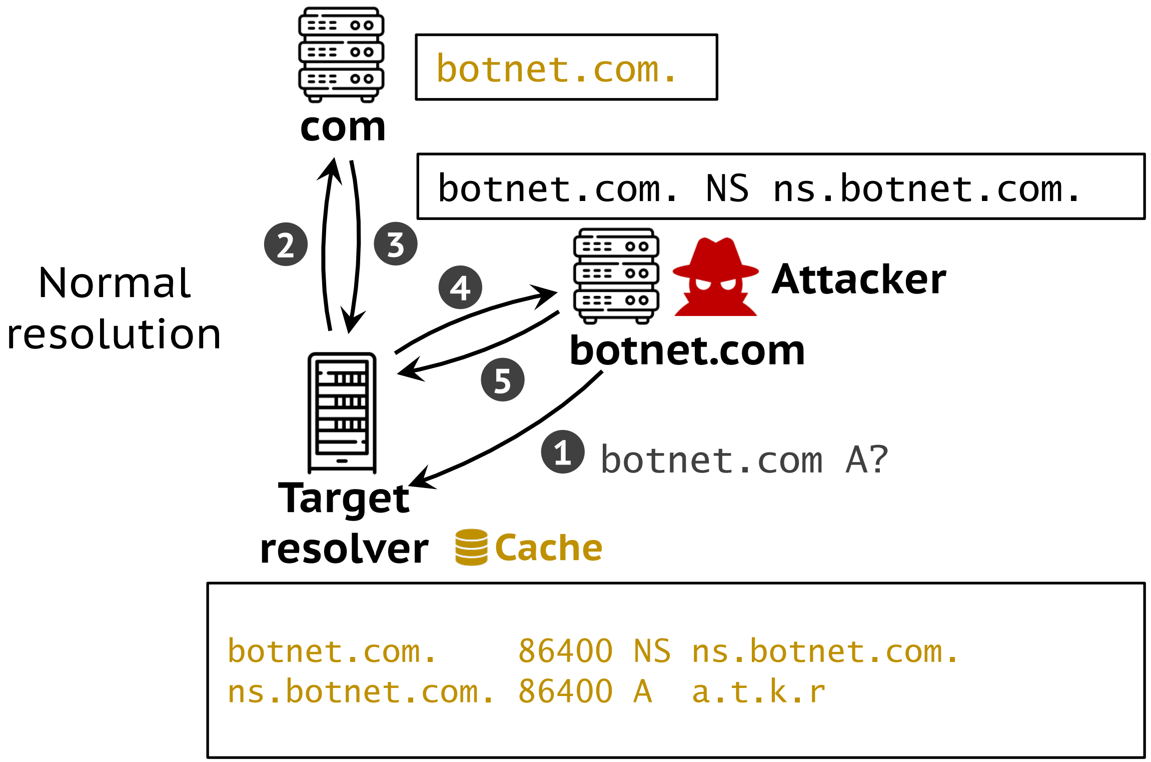
Does domain name revocation function as desired?

No. Ghost domain broke this guarantee.

Ghost Domain

➢Ghost domain attack

- ➢Proposed in NDSS 2012 by our NISL lab
- ➢Making revoked domain names still resolvable on resolvers



Normal resolution

com

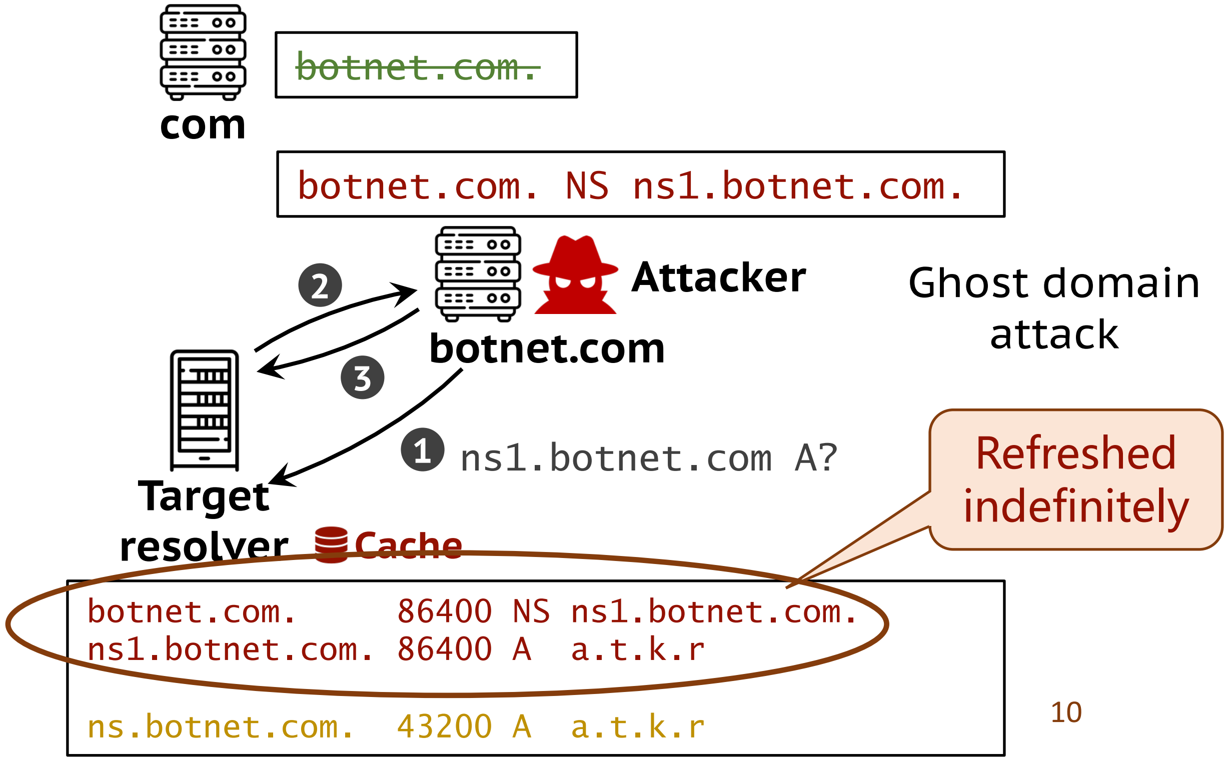
```
botnet.com.
```

```
botnet.com. NS ns.botnet.com.
```

❶ botnet.com A?

Cache

```
botnet.com.     86400 NS ns.botnet.com.
ns.botnet.com.  86400 A  a.t.k.r
```



Ghost domain attack

com

~~botnet.com.~~

```
botnet.com. NS ns1.botnet.com.
```

❶ ns1.botnet.com A?

Cache

```
botnet.com.      86400 NS ns1.botnet.com.
ns1.botnet.com.  86400 A  a.t.k.r

ns.botnet.com.   43200 A  a.t.k.r
```

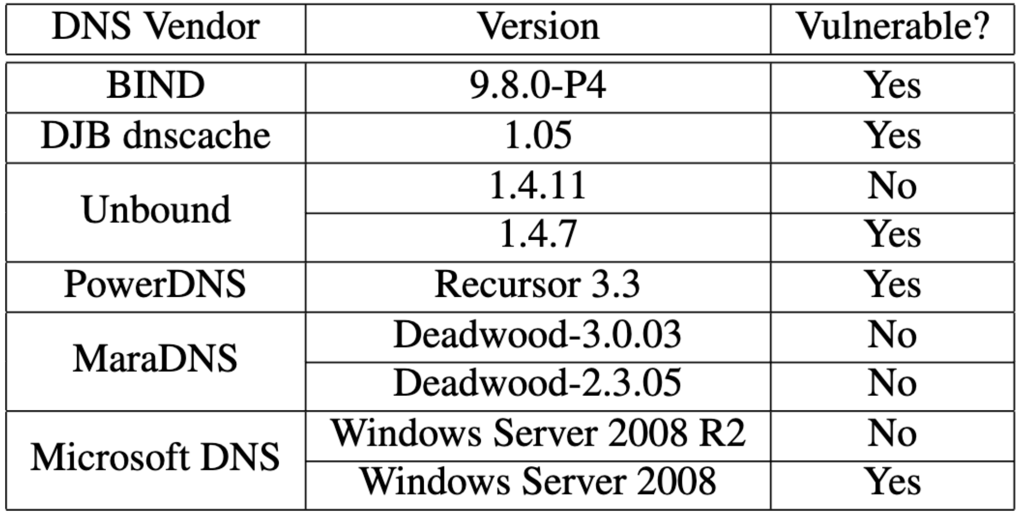
Refreshed indefinitely

With ghost domain, even after revocation, malicious domains can still be resolvable.

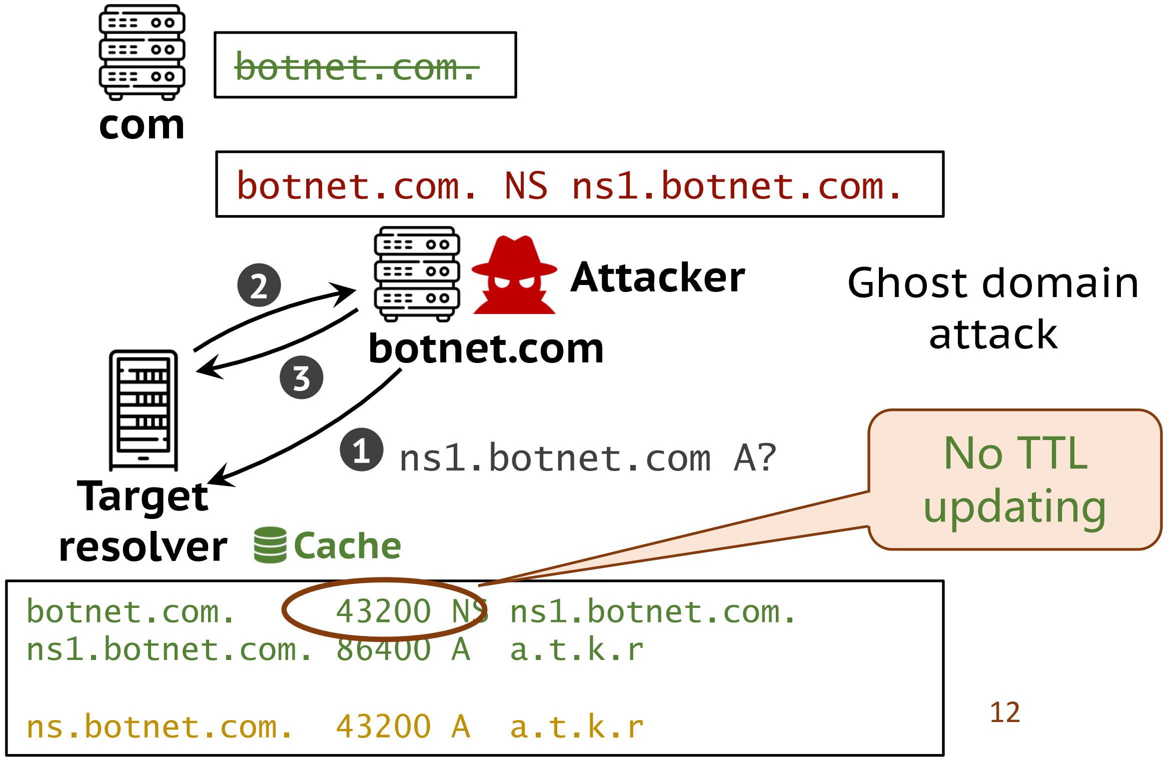
Attackers can use it to evade domain take-down or domain expiration.

Ghost Domain

- **Vulnerable software**
  - Not all software: BIND, PowerDNS, etc.
- **Mitigation**
  - TTL field cannot be prolonged



DNS Vendor	Version	Vulnerable?
BIND	9.8.0-P4	Yes
DJB dnscache	1.05	Yes
Unbound	1.4.11	No
	1.4.7	Yes
PowerDNS	Recursor 3.3	Yes
MaraDNS	Deadwood-3.0.03	No
	Deadwood-2.3.05	No
Microsoft DNS	Windows Server 2008 R2	No
	Windows Server 2008	Yes



Ghost domain attack

```
botnet.com.      43200 NS ns1.botnet.com.
ns1.botnet.com.  86400 A  a.t.k.r

ns.botnet.com.   43200 A  a.t.k.r
```

10 years later, does domain name revocation work as desired after fixing ghost domain?

No. Phoenix domain still breaks this guarantee with a broader attack surface.

Phoenix Domain

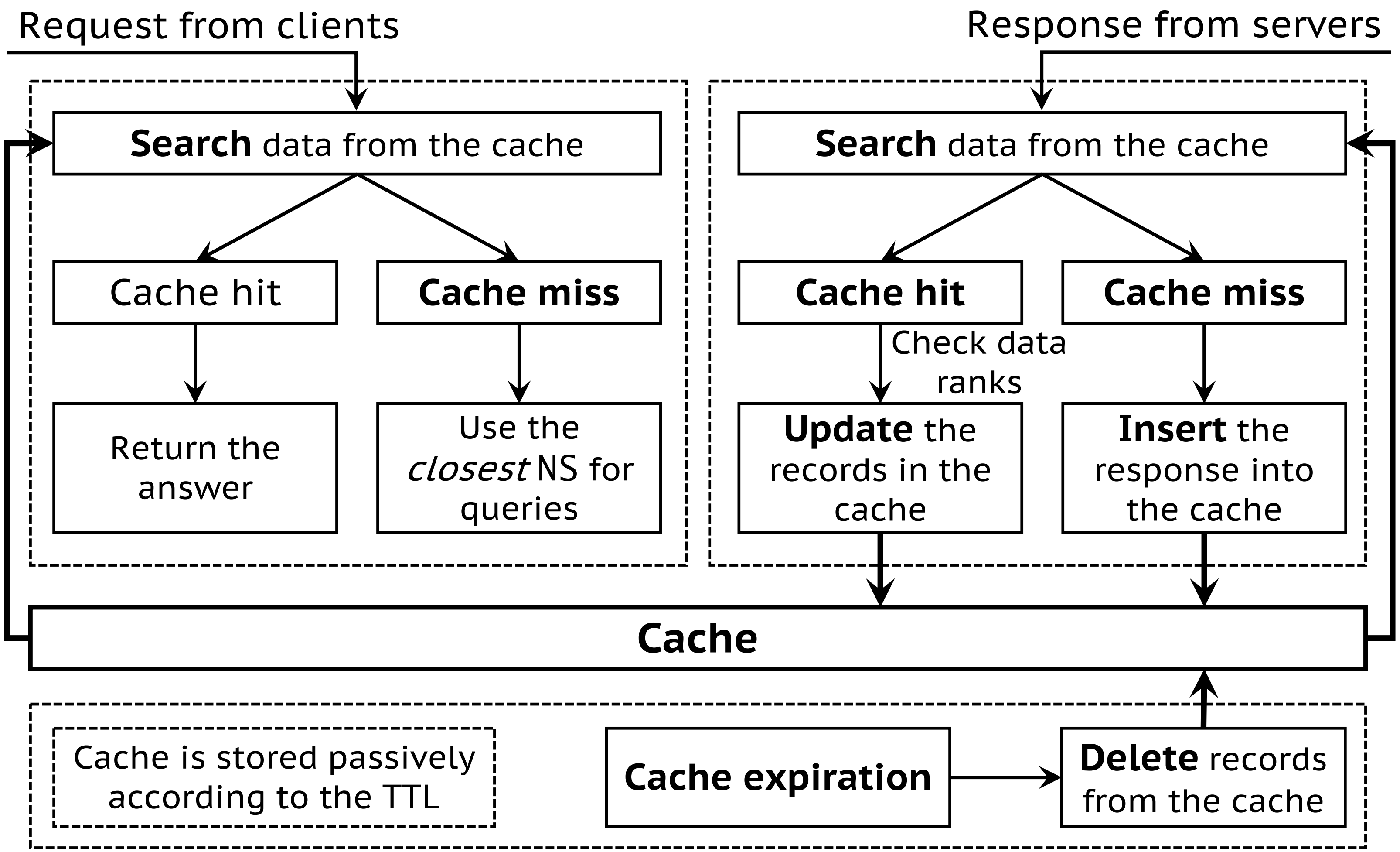
- **What is phoenix domain**
  - Proposed in NDSS 2023 by our NISL lab
  - Also making revoked domain names still resolvable on resolvers
  - Two new vulnerabilities in protocols or implementations
  - Two variations (T1 and T2)
  - Affecting all DNS implementations

Why is domain name revocation still vulnerable?

We find that the entire attack surface remains unclear now.

DNS Cache Operations

- **Summary**



Request from clients

Response from servers

Search data from the cache

Cache hit

Cache miss

Return the answer

Use the *closest* NS for queries

Search data from the cache

Cache hit

Cache miss

Check data ranks

Update the records in the cache

Insert the response into the cache

Cache

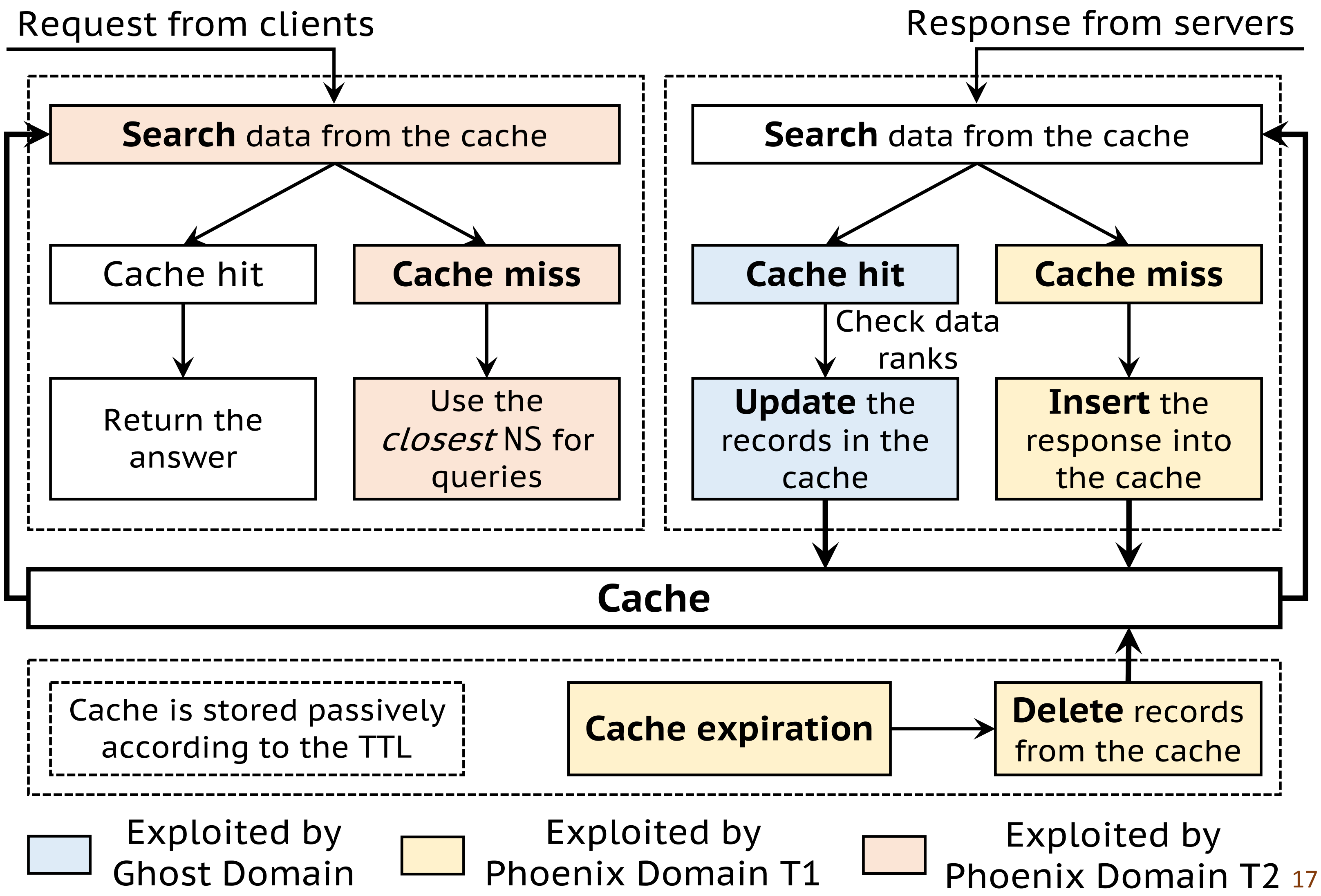
Cache is stored passively according to the TTL

Cache expiration

Delete records from the cache

DNS Cache Operations

- **Attack Surface**
  - Updating
  - Insertion
  - Searching



Request from clients

Search data from the cache

Cache hit

Return the answer

Cache miss

Use the *closest* NS for queries

Response from servers

Search data from the cache

Cache hit

Check data ranks

Update the records in the cache

Cache miss

Insert the response into the cache

Cache

Cache is stored passively according to the TTL

Cache expiration

Delete records from the cache

🟦 Exploited by Ghost Domain

🟨 Exploited by Phoenix Domain T1

🟧 Exploited by Phoenix Domain T2

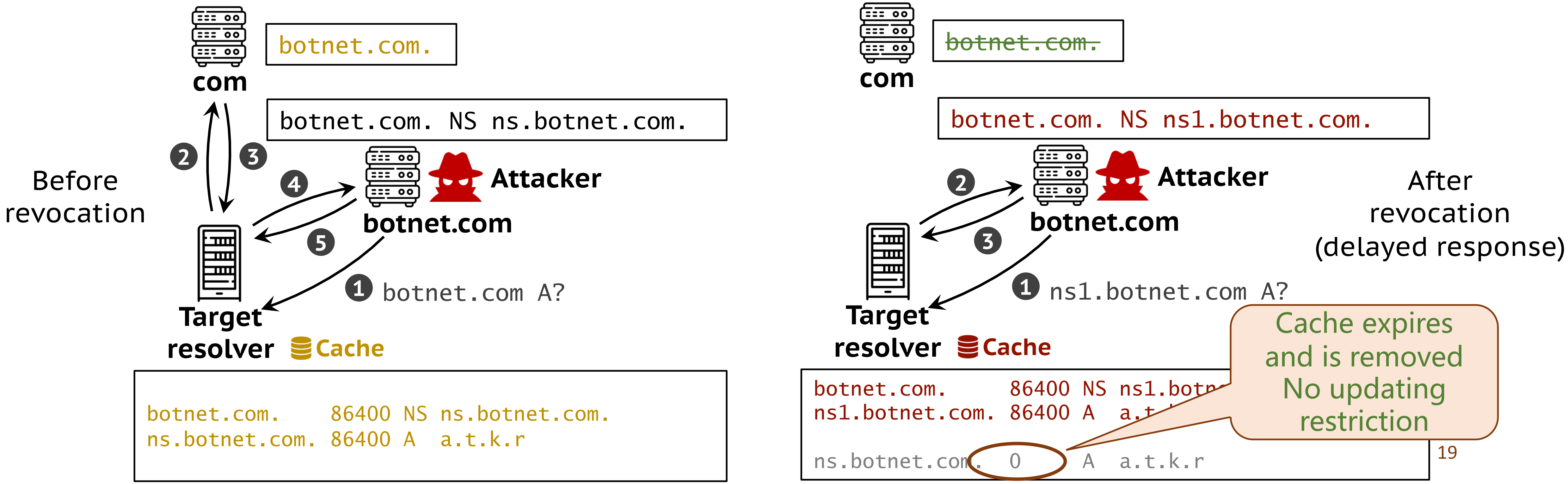
How does phoenix domain work?

Two variations, two ways.

Phoenix Domain T1

➢T1 attack

- ➢Exploiting vulnerable cache insertion implementations
- ➢Inserting new NS records when the old is about to expire



```
botnet.com.
```

```
botnet.com. NS ns.botnet.com.
```

```
botnet.com.     86400 NS ns.botnet.com.
ns.botnet.com.  86400 A  a.t.k.r
```

~~botnet.com.~~

```
botnet.com. NS ns1.botnet.com.
```

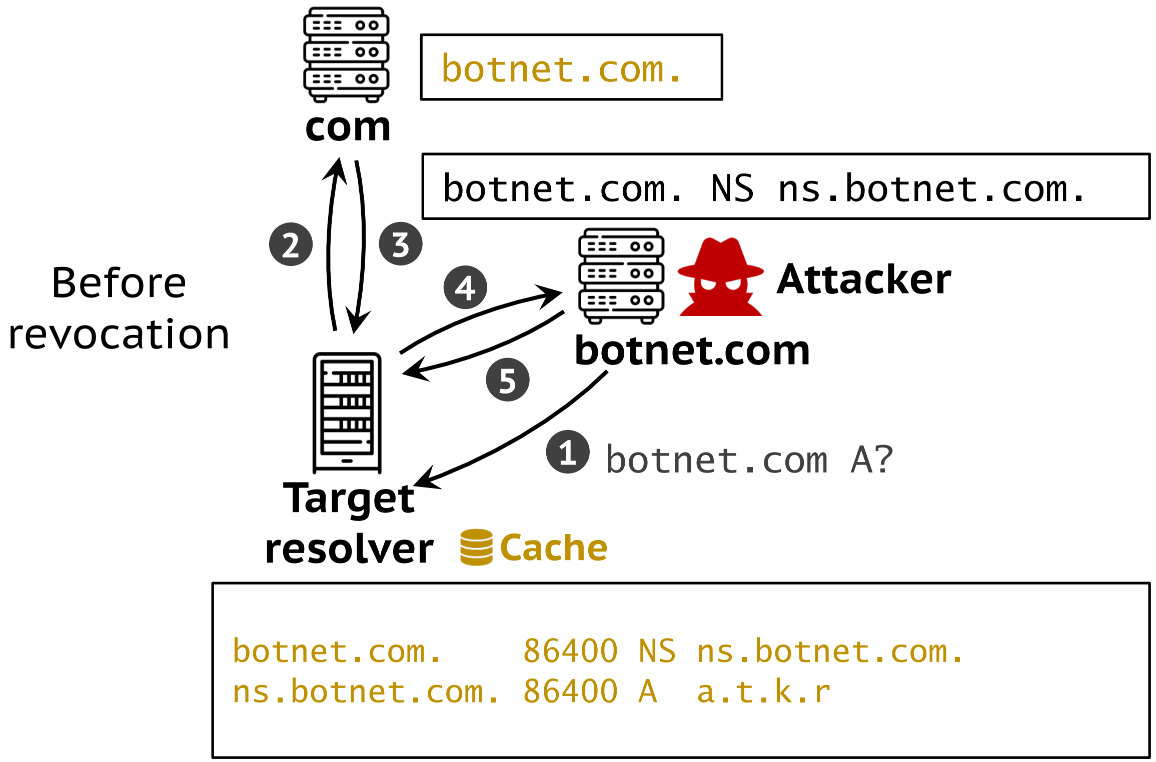
```
botnet.com.      86400 NS ns1.botn
ns1.botnet.com.  86400 A  a.t

ns.botnet.com.   0     A  a.t.k.r
```

Cache expires and is removed
No updating restriction

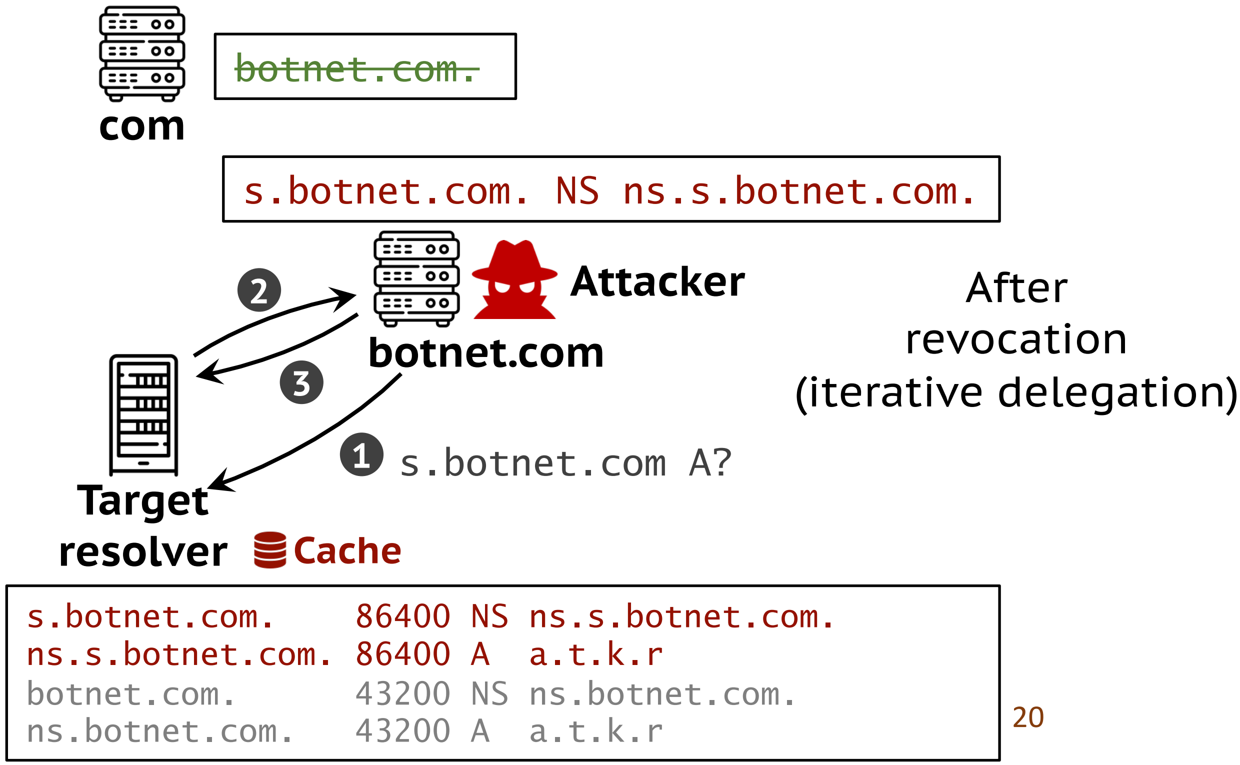
Phoenix Domain T2

➢T2 attack

- ➢Exploiting vulnerable cache searching operations
- ➢Inserting new NS records of subdomains



```
botnet.com.     86400 NS ns.botnet.com.
ns.botnet.com.  86400 A  a.t.k.r
```

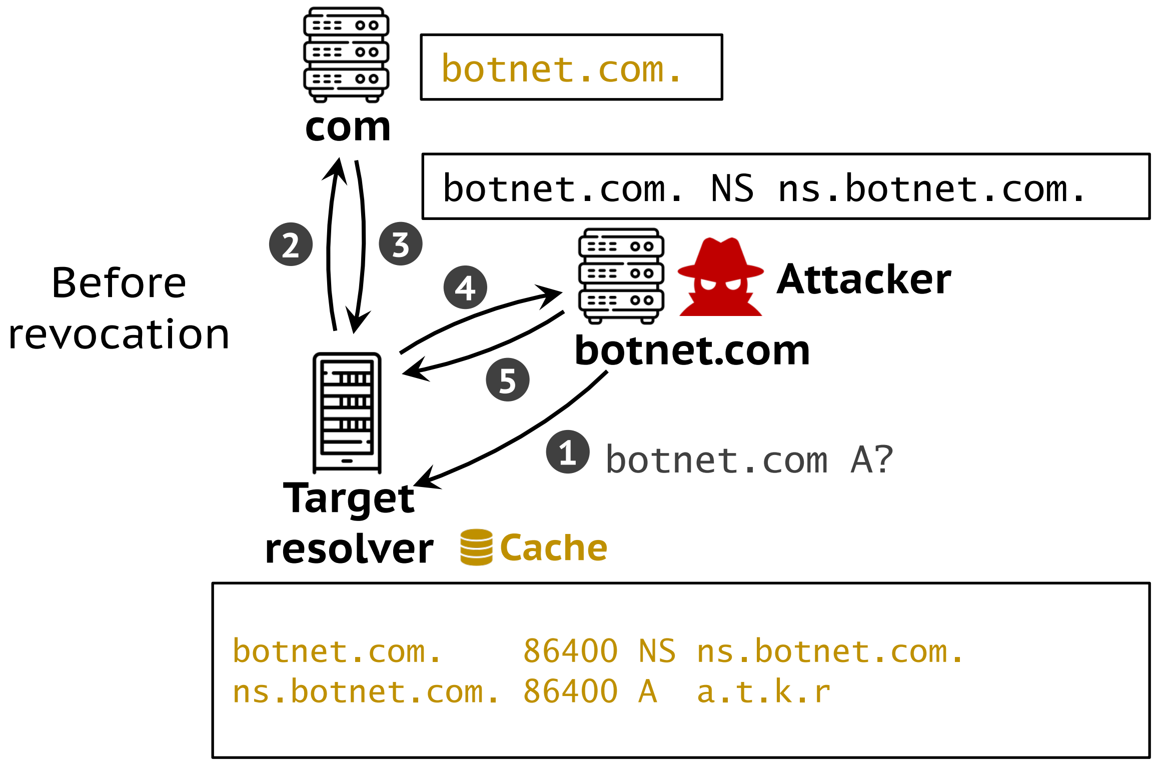


```
s.botnet.com.     86400 NS ns.s.botnet.com.
ns.s.botnet.com.  86400 A  a.t.k.r
botnet.com.       43200 NS ns.botnet.com.
ns.botnet.com.    43200 A  a.t.k.r
```

Phoenix Domain T2

T2 attack

- Exploiting vulnerable cache searching operations
- Inserting <u>new NS records of subdomains</u>

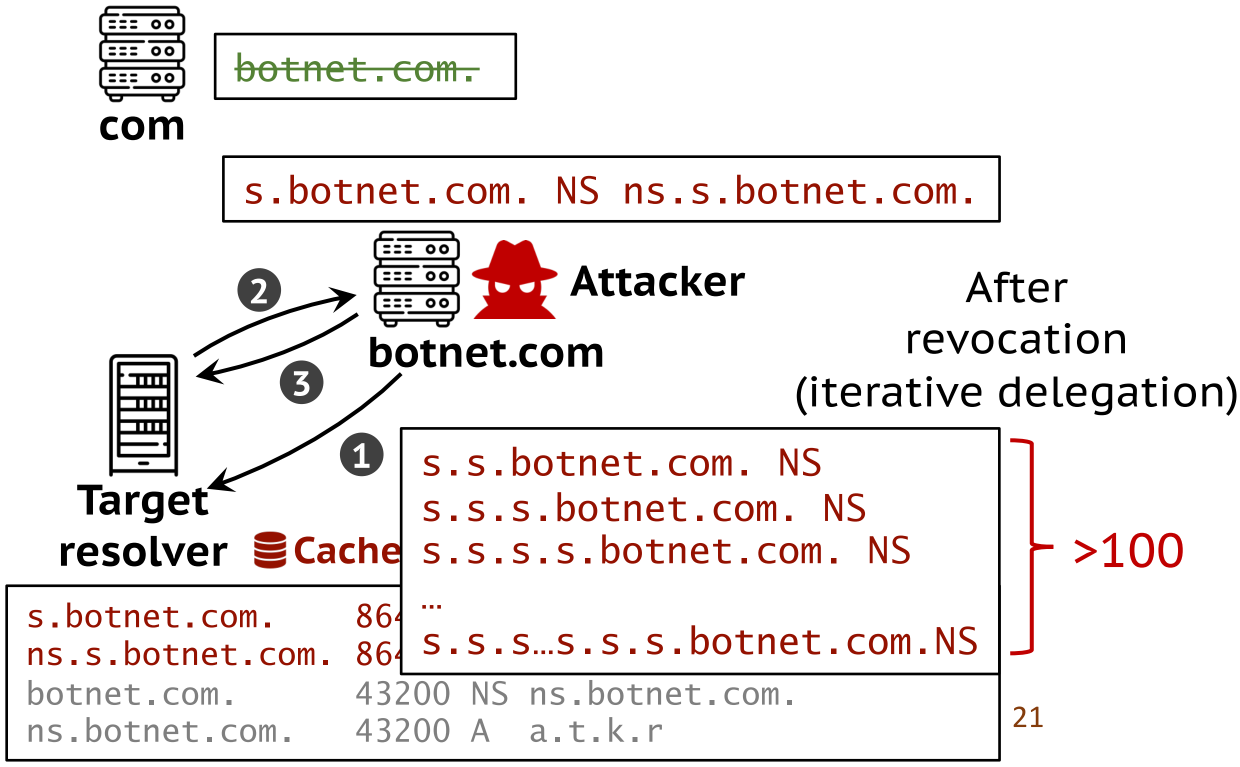


```
botnet.com.
```

```
botnet.com. NS ns.botnet.com.
```

```
botnet.com A?
```

```
botnet.com.     86400 NS ns.botnet.com.
ns.botnet.com.  86400 A  a.t.k.r
```



~~botnet.com.~~

```
s.botnet.com. NS ns.s.botnet.com.
```

```
s.s.botnet.com. NS
s.s.s.botnet.com. NS
s.s.s.s.botnet.com. NS
…
s.s.s…s.s.s.botnet.com.NS
```

```
s.botnet.com.     864
ns.s.botnet.com.  864
botnet.com.       43200 NS ns.botnet.com.
ns.botnet.com.    43200 A  a.t.k.r
```

Vulnerable Software

- **Phoenix domain T1**
  - BIND9, Knot Resolver, Unbound, and Technitium
- **Phoenix domain T2**
  - All tested 8 software

BIND 9

KNOT RESOLVER

unbound

POWERDNS

Microsoft DNS

MaraDNS

Simple DNS Plus

Technitium DNS Server

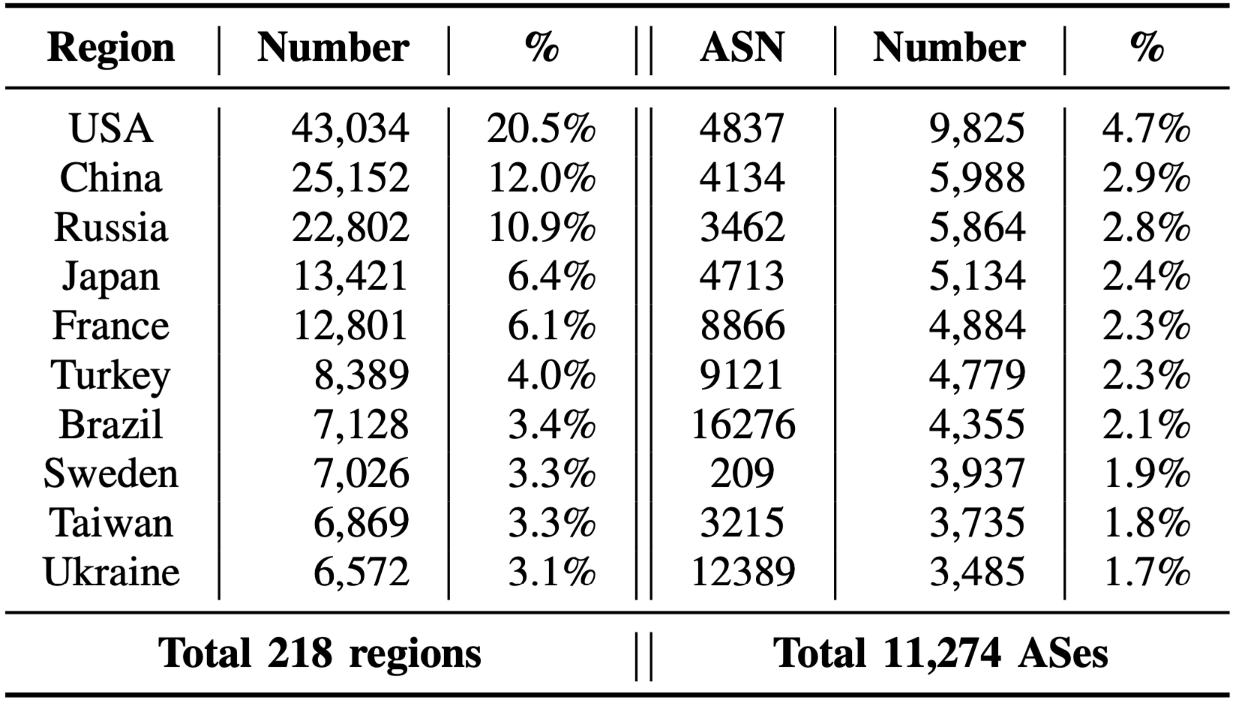
Vulnerable Public Resolvers

- **Phoenix domain T1 and/or T2**
  - We test 41 public resolver vendors
  - All resolvers are vulnerable to T1 and/or T2
  - Such as Google, Cloudflare, Akamai, AdGuard, etc.

Vulnerable Open Resolvers

➢Recursive resolver list

- ➢Through scanning, we collected 1.2M resolvers
- ➢210k recursive resolvers are selected

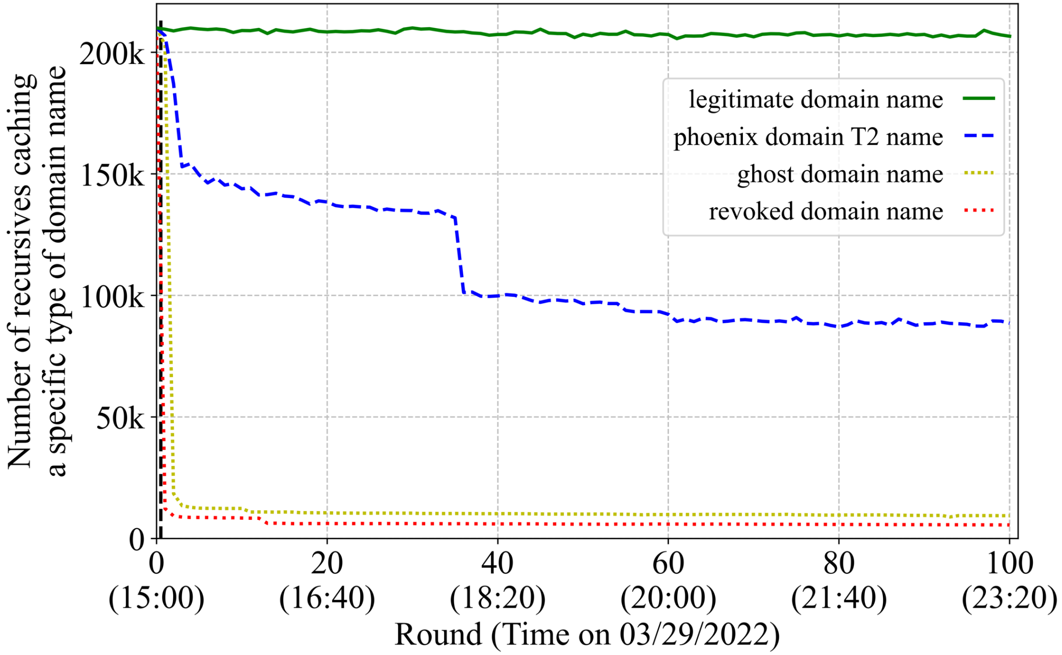


Region	Number	%	ASN	Number	%
USA	43,034	20.5%	4837	9,825	4.7%
China	25,152	12.0%	4134	5,988	2.9%
Russia	22,802	10.9%	3462	5,864	2.8%
Japan	13,421	6.4%	4713	5,134	2.4%
France	12,801	6.1%	8866	4,884	2.3%
Turkey	8,389	4.0%	9121	4,779	2.3%
Brazil	7,128	3.4%	16276	4,355	2.1%
Sweden	7,026	3.3%	209	3,937	1.9%
Taiwan	6,869	3.3%	3215	3,735	1.8%
Ukraine	6,572	3.1%	12389	3,485	1.7%
Total 218 regions			**Total 11,274 ASes**		

Experiments for T2

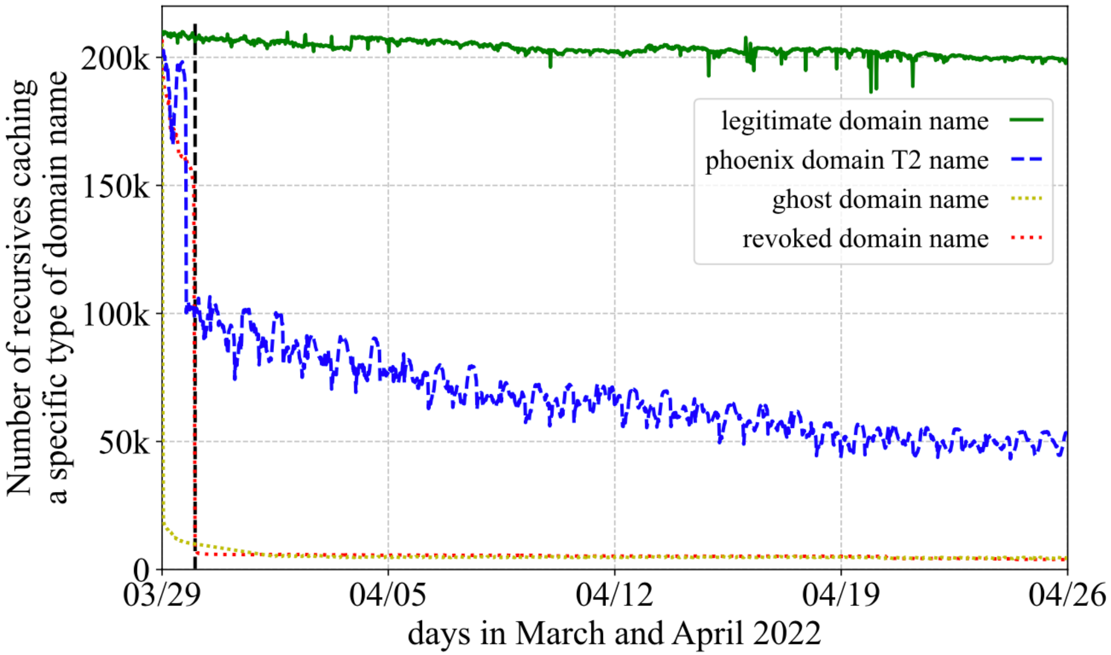
Short-term experiments

- Check how many labels are supported
- 89% are vulnerable
- After 100 rounds, 42% are vulnerable



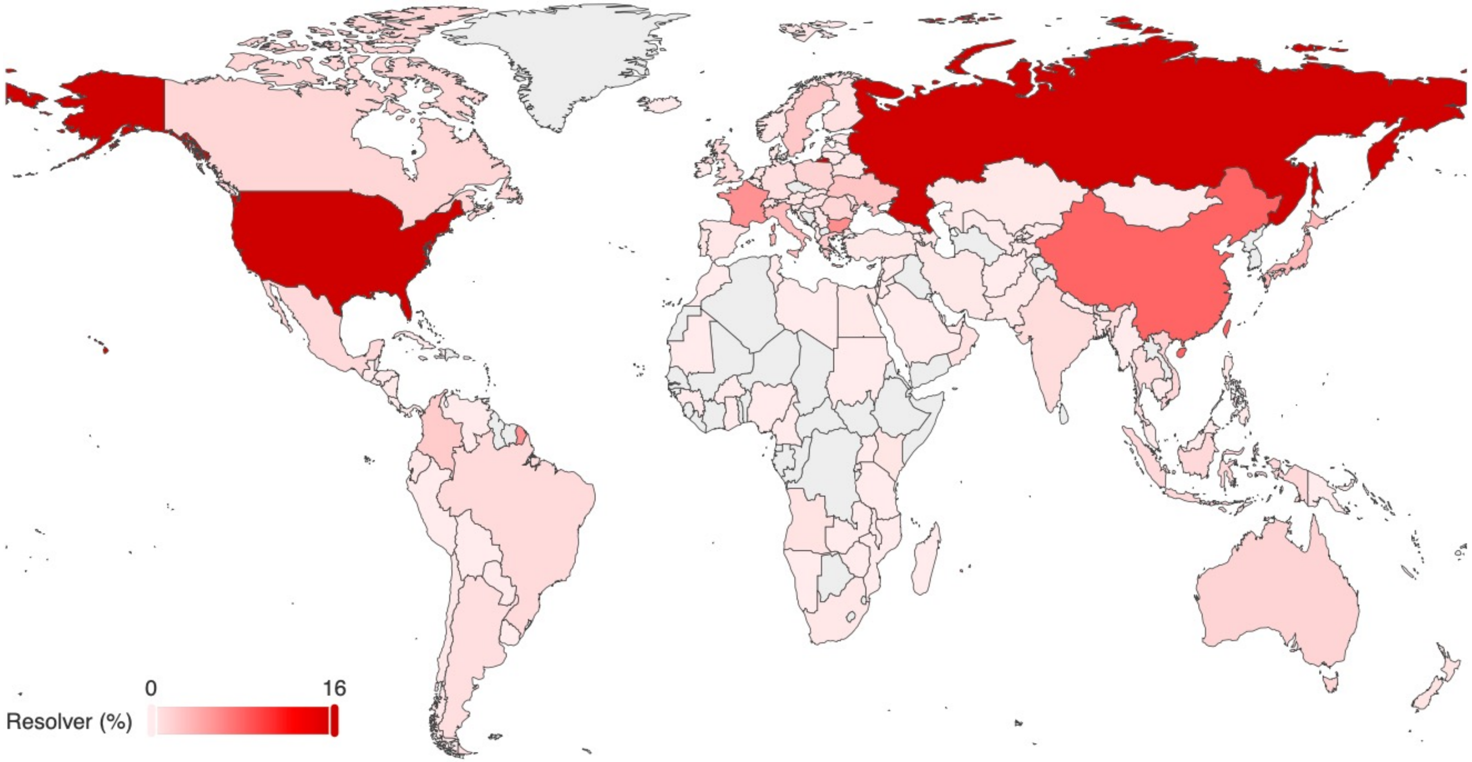
Experiments for T2

- **Long-term experiments**
  - Check how long phoenix domain can be alive
  - After one week, 40% are vulnerable
  - After one month, 25% are vulnerable



Experiments for T2

- **Geolocation of vulnerable resolvers**
  - USA, Russia, and China



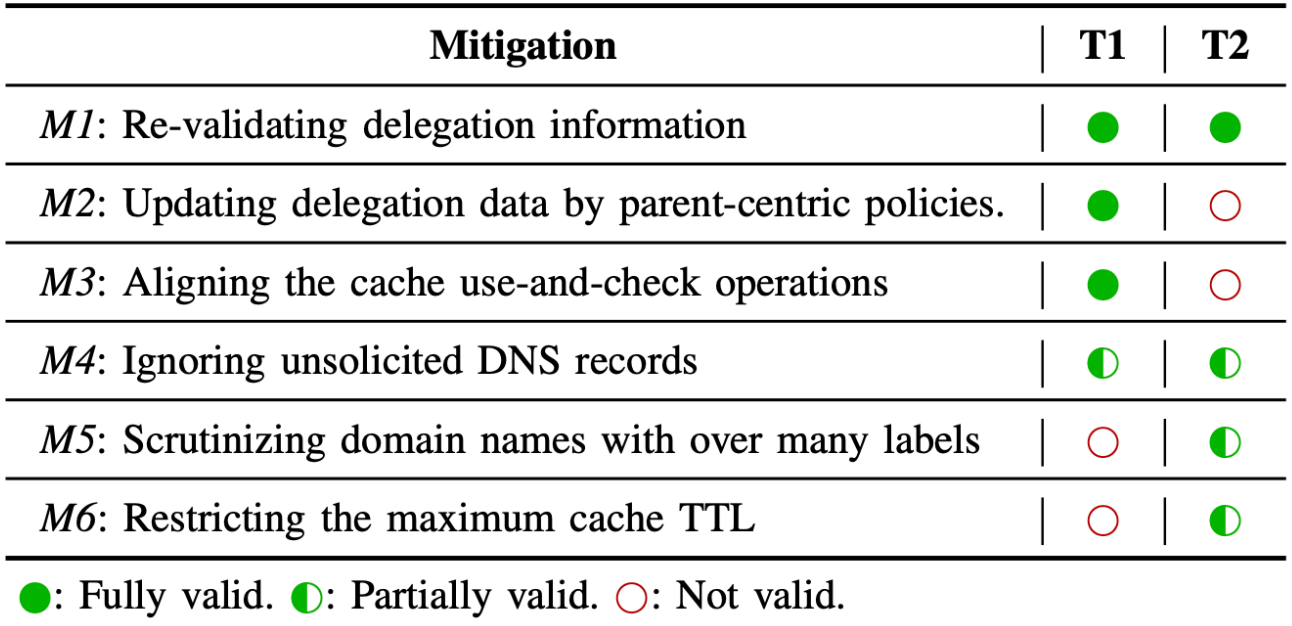
Disclosure & Mitigation

Disclosure feedback

- 7 software and 15 resolver vendors confirmed
- 9 CVE-ids are assigned

Mitigation

- 6 approaches
- Discussing with
- RFC editors



Mitigation	T1	T2
M1: Re-validating delegation information	●	●
M2: Updating delegation data by parent-centric policies.	●	○
M3: Aligning the cache use-and-check operations	●	○
M4: Ignoring unsolicited DNS records	◐	◐
M5: Scrutinizing domain names with over many labels	○	◐
M6: Restricting the maximum cache TTL	○	◐

●: Fully valid. ◐: Partially valid. ○: Not valid.

Conclusion

- **New phoenix domain attacks**
  - Systematic analysis of cache operations
- **Two novel vulnerabilities**
  - T1 resulting from poor implementations
  - T2 resulting from de facto protocol standards
- **Comprehensive influence**
  - Many many resolvers are vulnerable and exploitable
- **Detailed mitigation approaches**

Thanks for listening!

Any question?

Xiang Li, Tsinghua University
x-l19@mails.tsinghua.edu.cn

TSINGHUA UNIVERSITY 1911

UCI Samueli
School of Engineering
University of California, Irvine

奇安信
QI-ANXIN