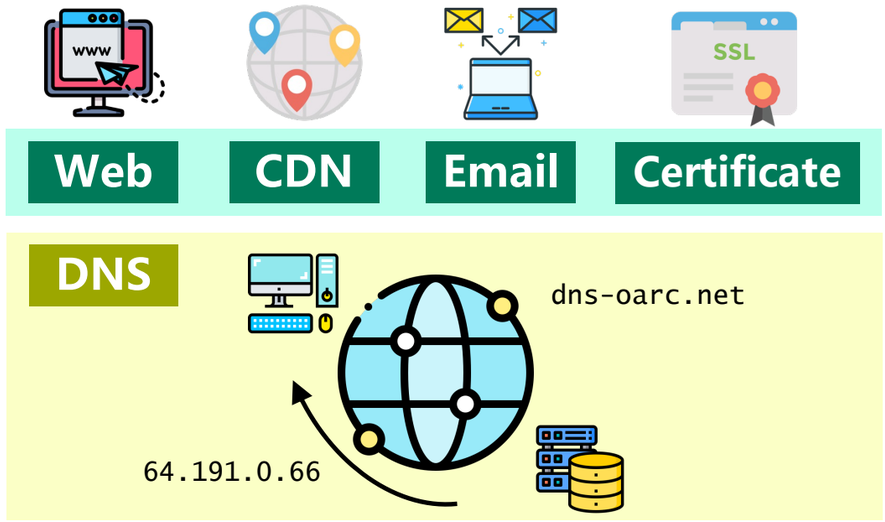
Phoenix Domain Attack: Vulnerable Links in Domain Name Delegation and Revocation

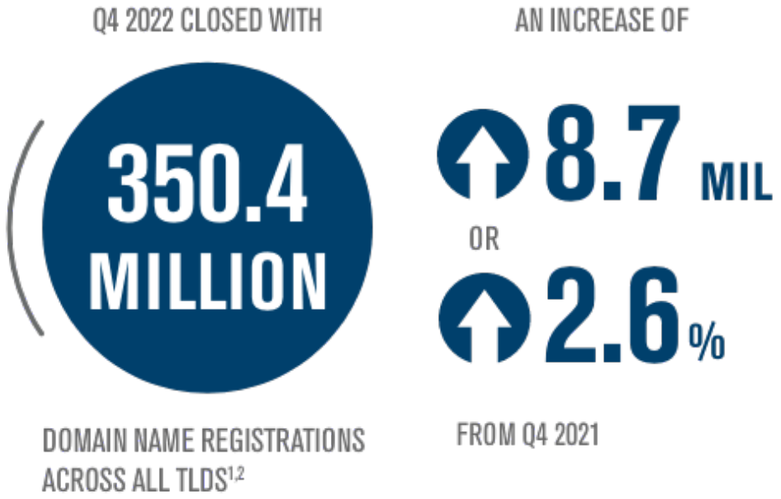
Xiang Li

Tsinghua University

Domain Name

- **Domain name system (DNS)**
  - Entry point of many Internet activities
  - Security guarantee of multiple application services
  - Domain names are widely registered





verisign.com/dnib

Domain Name Abuse

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

bleepingcomputer.com

scmp.com

norton.com

Domain Name Abuse

- **Also abused by criminal activities**
  - Botnet, phishing, malware distribution
- **ICANN Domain abuse activity reporting (DAAR)**
  - In March 2023
  - Check 216,171,933 domain names within 1,154 gTLDs

622,875 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.

theregister.com

intelligentciso.com

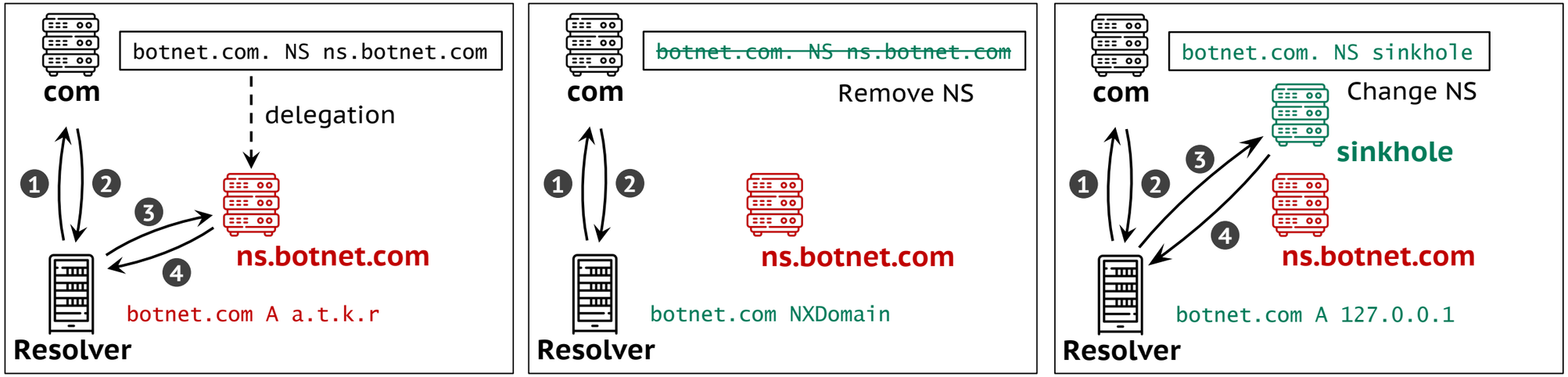
Question

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



Question

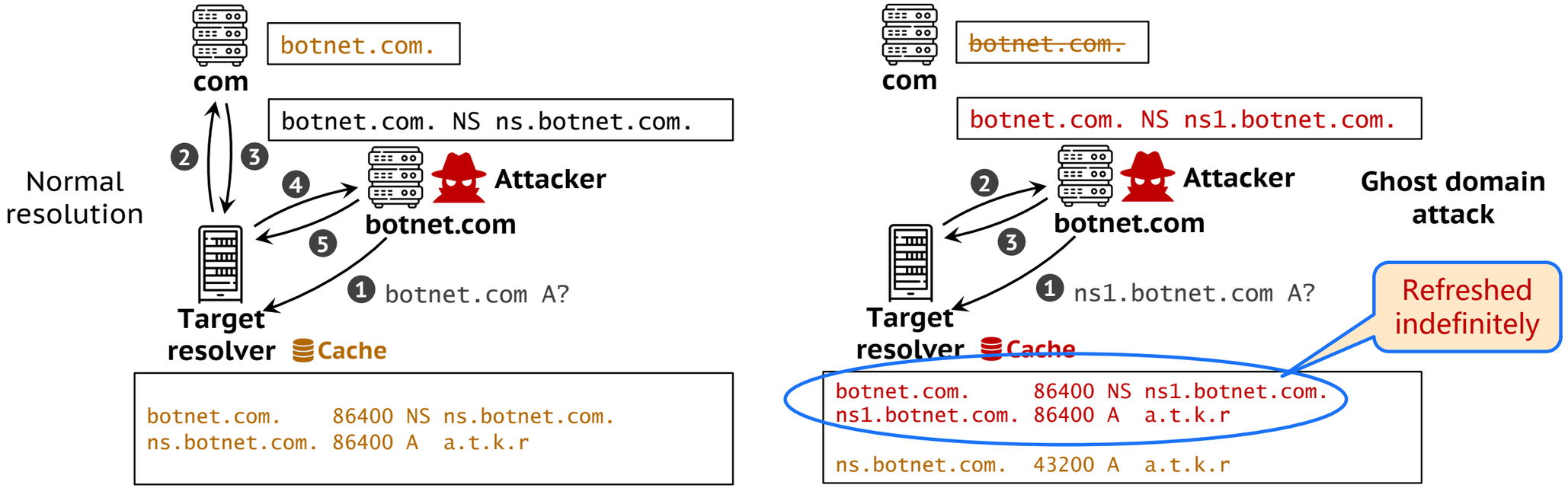
Does domain name revocation function as desired?

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



Takeaway

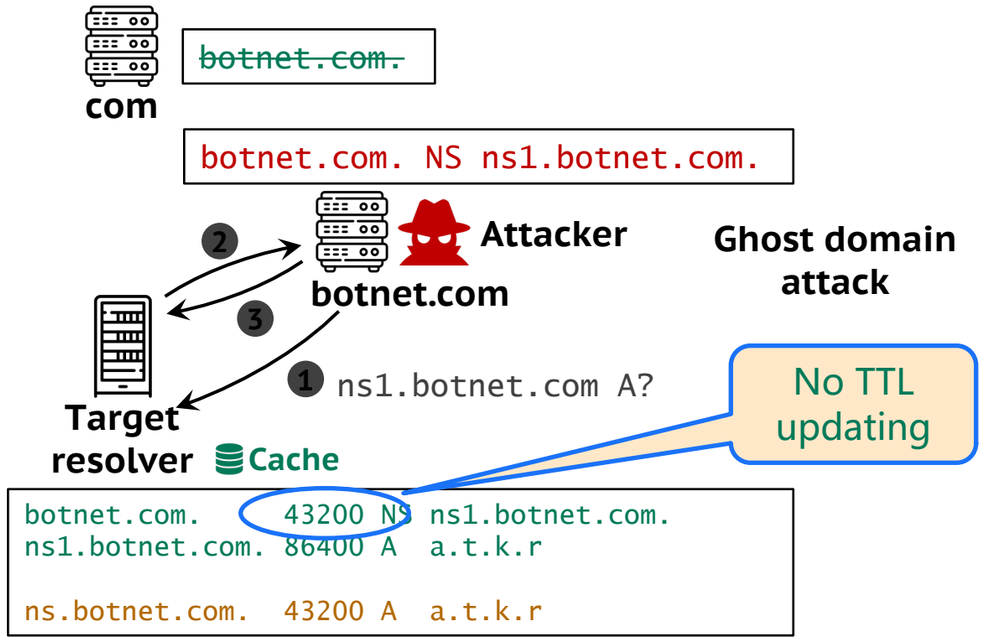
With ghost domain, even after revocation, malicious domains can still be resolvable.

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



Question

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 by our NISL lab too
  - 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

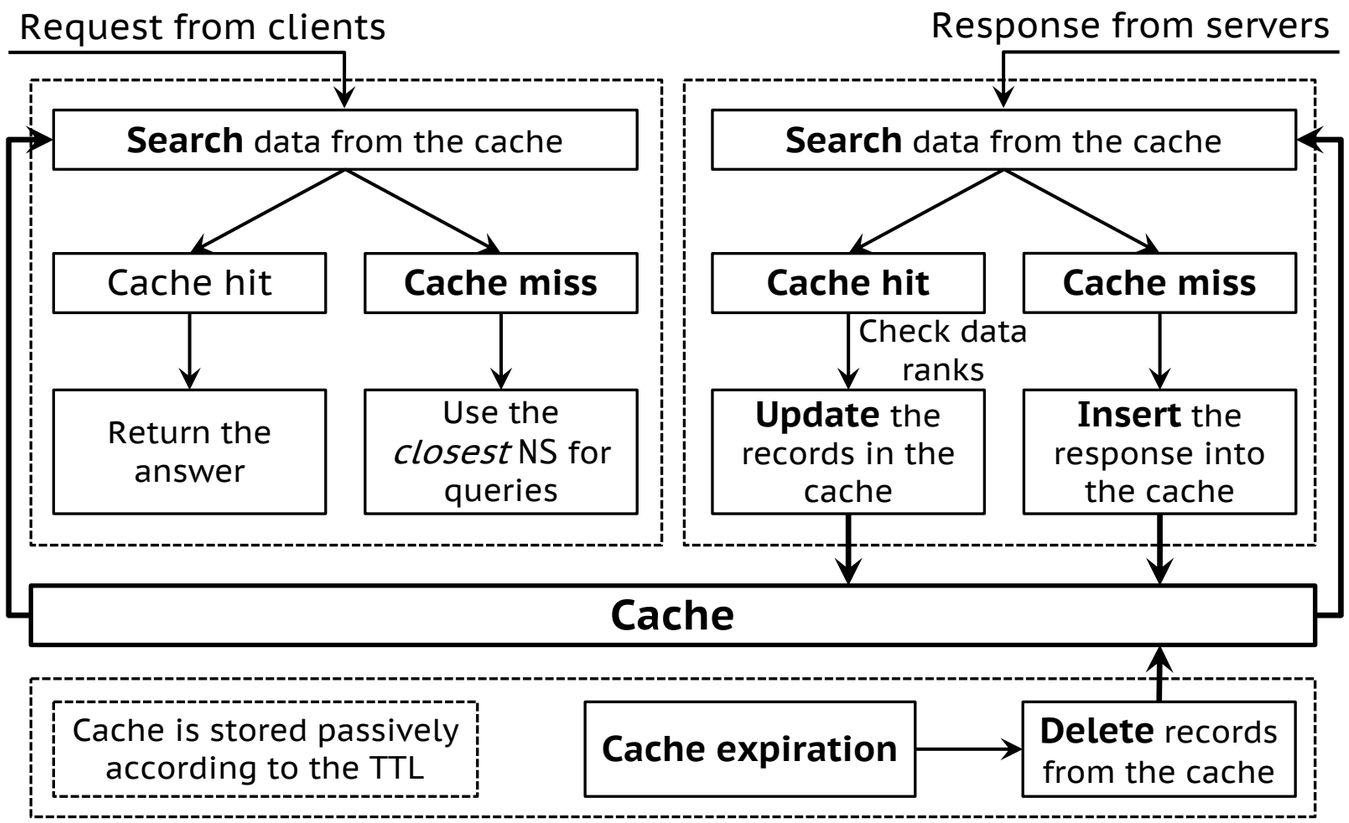
Question

Why is domain name revocation still vulnerable?

We find that the entire attack surface remains unclear now.

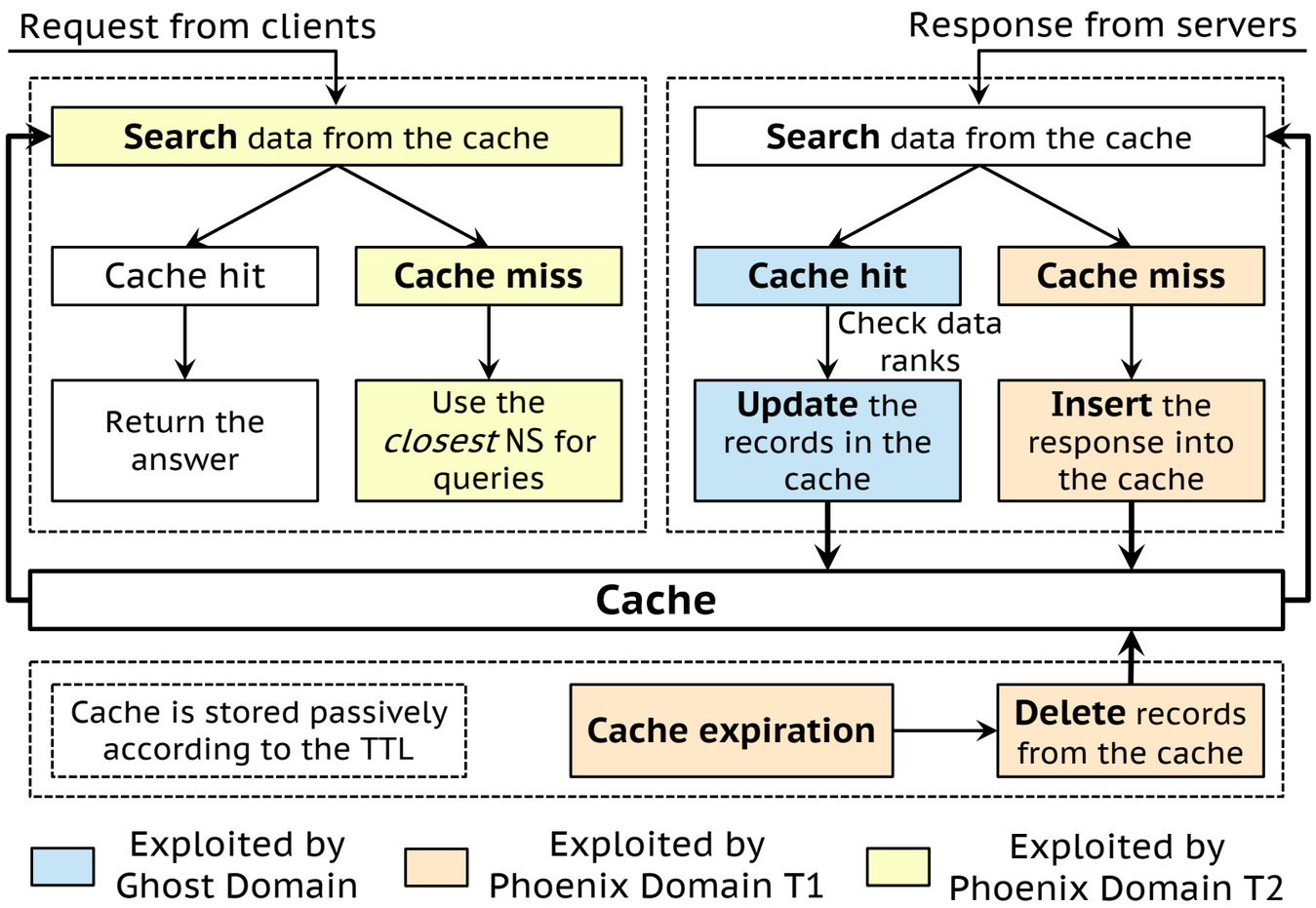
DNS Cache Operations

➢ Summary



DNS Cache Operations

- **Summary**
  - Updating
  - Insertion
  - Searching



Question

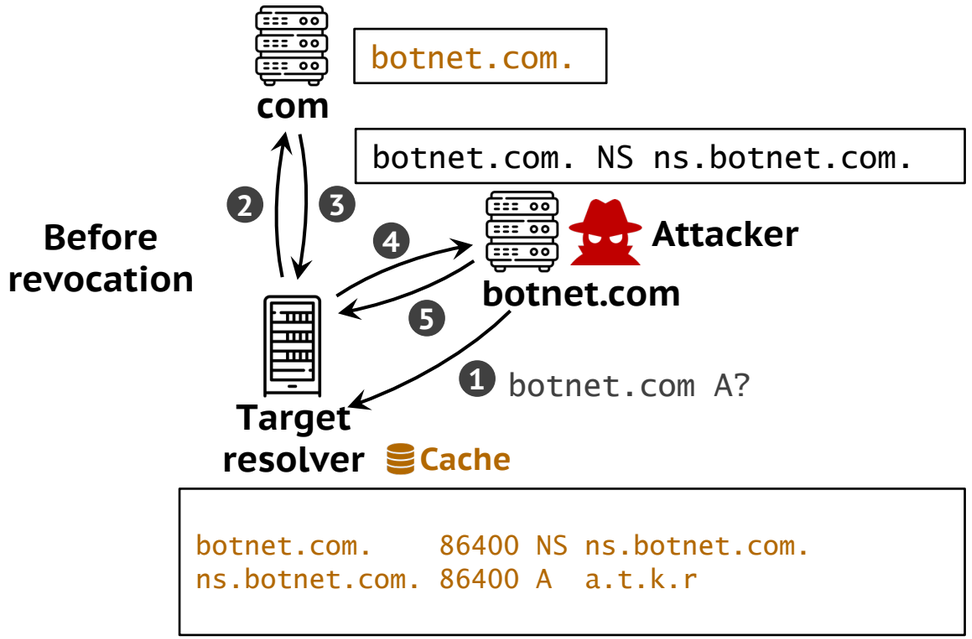
How does Phoenix Domain work?

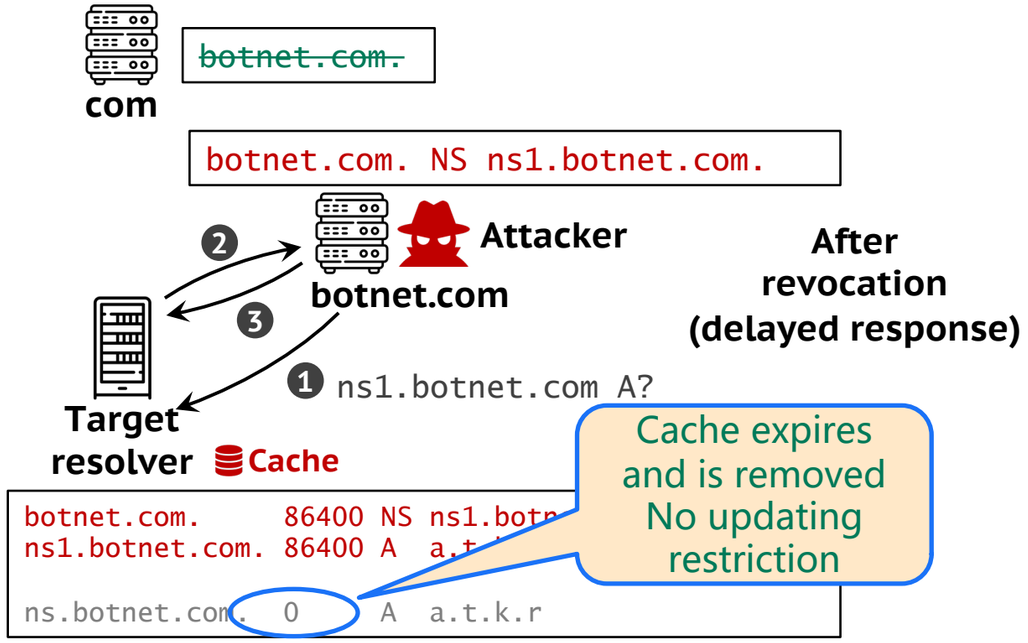
Two variations, two ways.

Phoenix Domain T1

➢ T1 attack

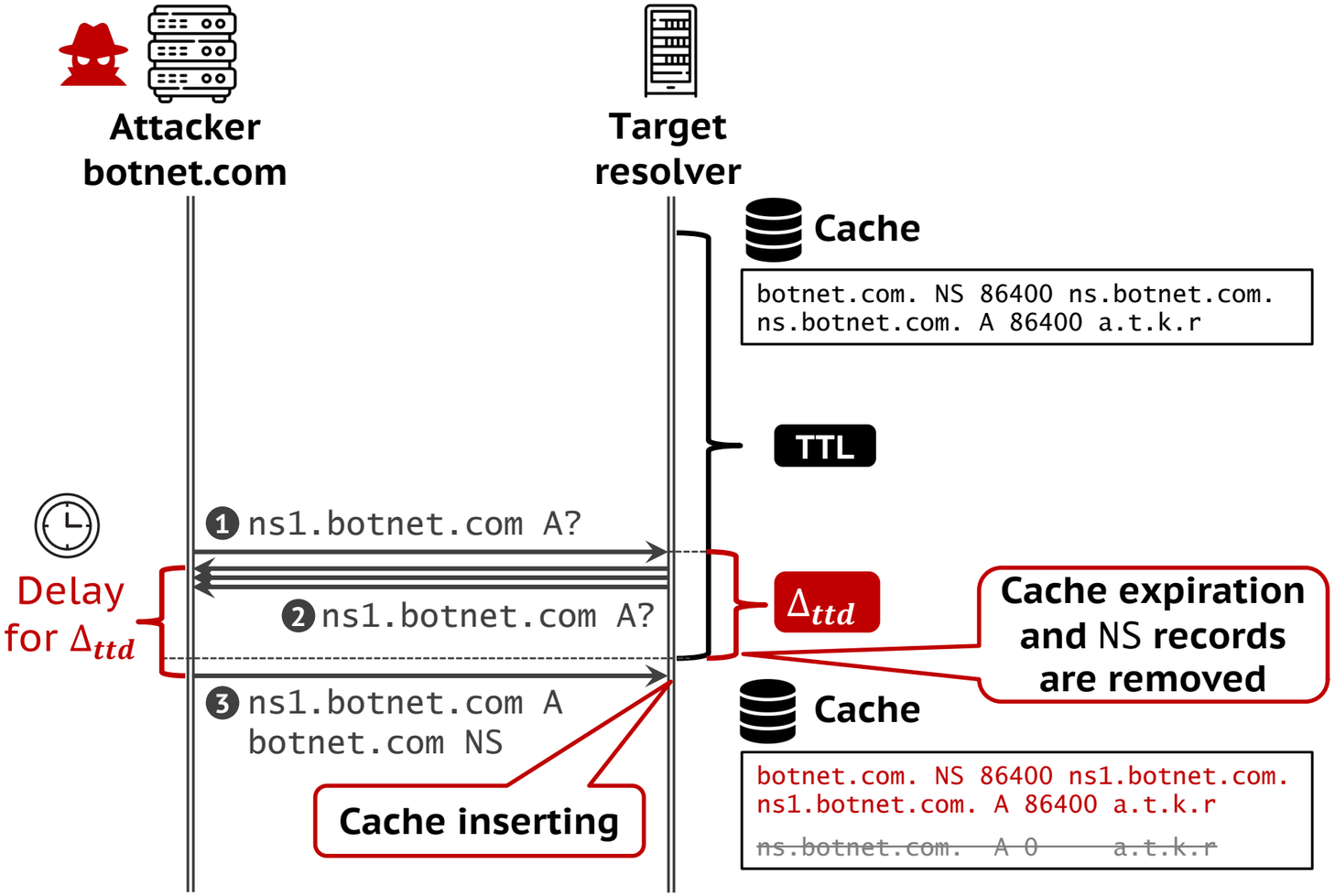
- Exploiting vulnerable cache insertion implementations
- Inserting new NS records when the old is about to expire





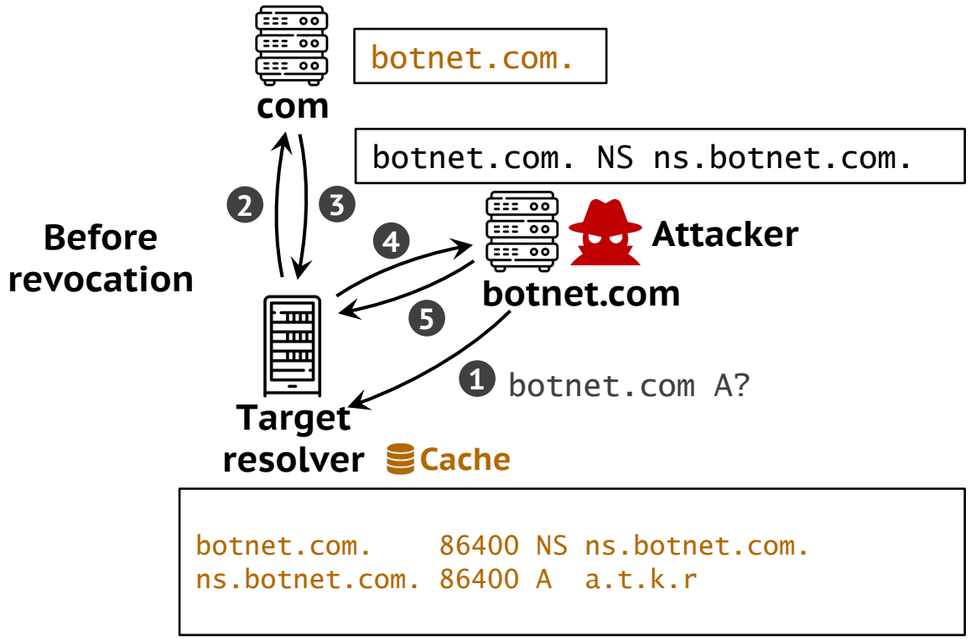
Phoenix Domain T1

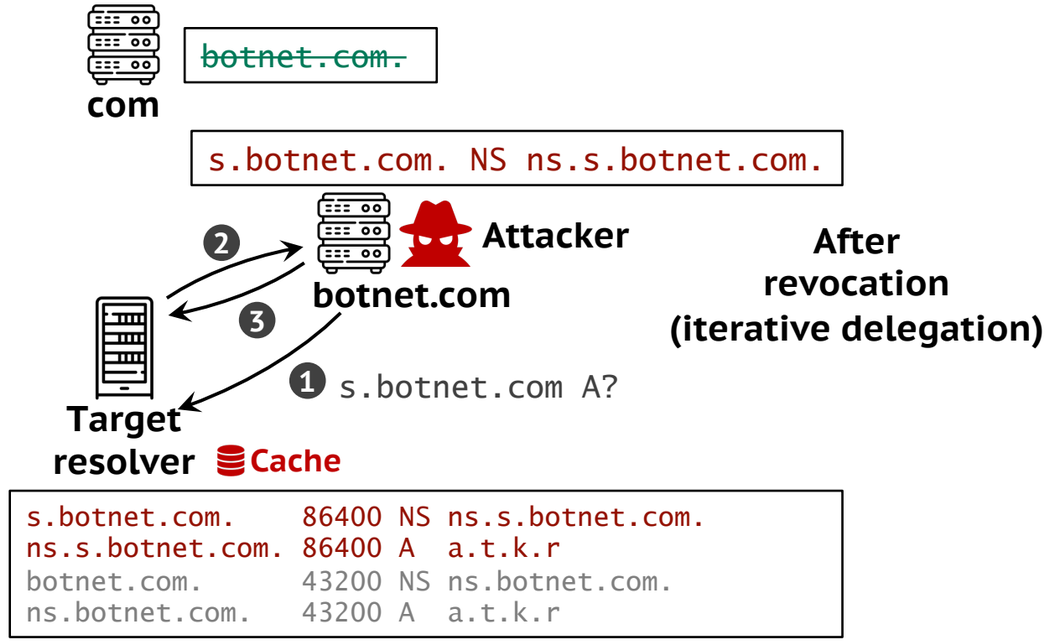
- **T1 attack**
  - Attack steps
  - Cache expiration
  - Cache deletion
  - Cache insertion



Phoenix Domain T2

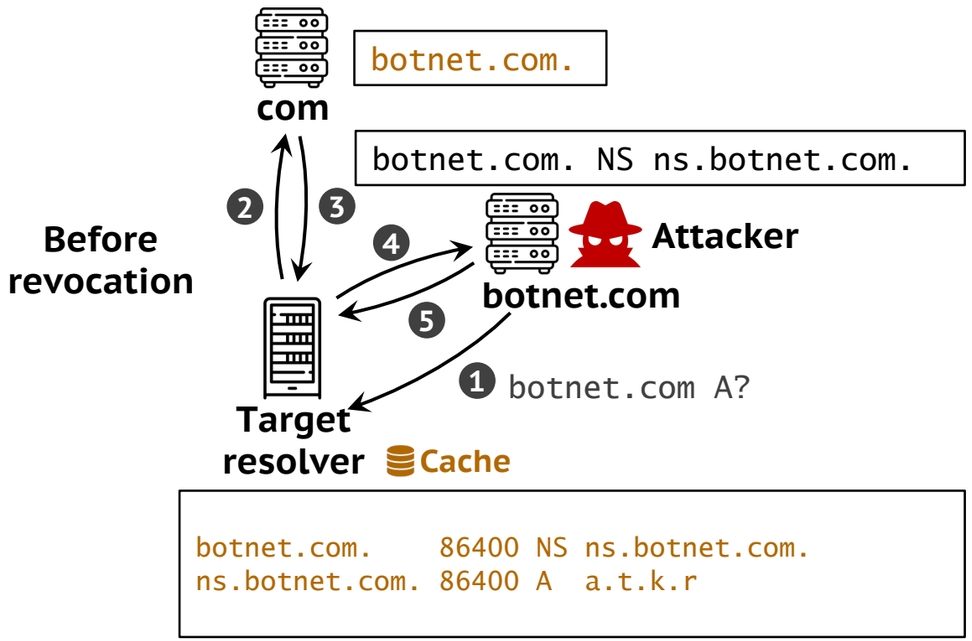
- **T2 attack**
  - Exploiting vulnerable cache searching operations
  - Inserting new NS records of subdomains

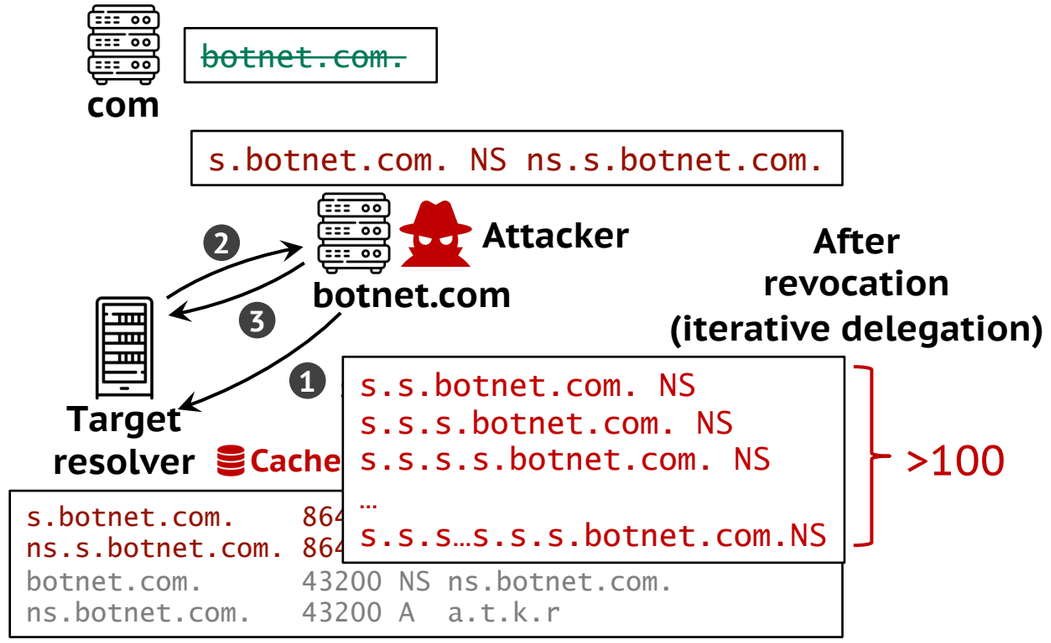




Phoenix Domain T2

- **T2 attack**
  - Exploiting vulnerable cache searching operations
  - Inserting **new NS records of subdomains**





Vulnerable Software

- **Phoenix domain T1**
  - BIND9, Knot, Unbound, and Technitium
- **Phoenix domain T2**
  - All tested 8 software are vulnerable (7 confirmed, 9 CVEs)

BIND 9 | KNOT RESOLVER | unbound | POWERDNS | Microsoft DNS | MaraDNS | Simple DNS Plus | Technitium DNS Server

CVE-2022-30250 CVE-2022-30251
CVE-2022-30252 CVE-2022-30254
CVE-2022-30256 CVE-2022-30257
CVE-2022-30258 CVE-2022-30698
CVE-2022-30699

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. (15 confirmed)

Google Public DNS

1.1.1.1

ADGUARD DNS

quad9

DYN

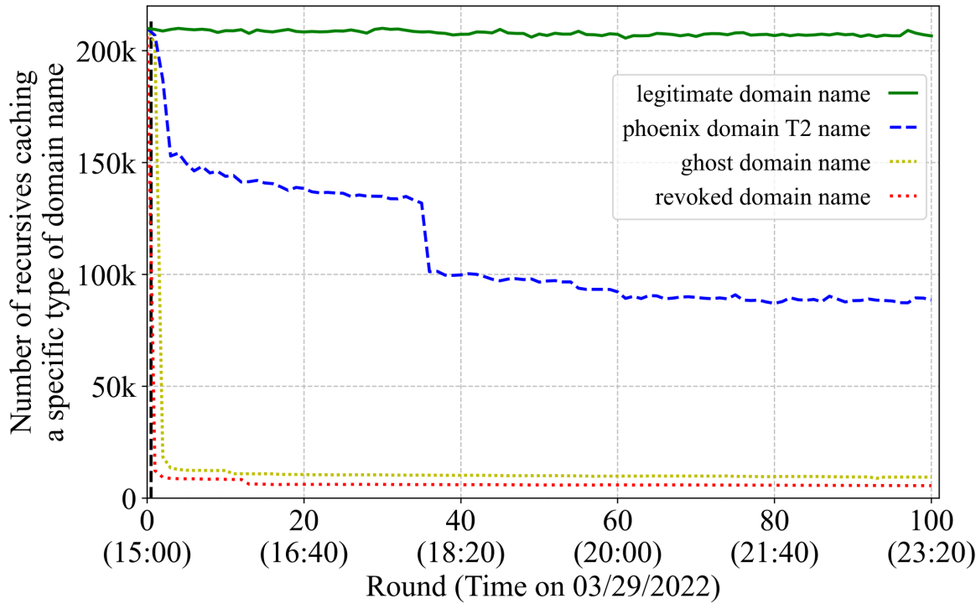
Vulnerable Open Resolvers

- **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**		

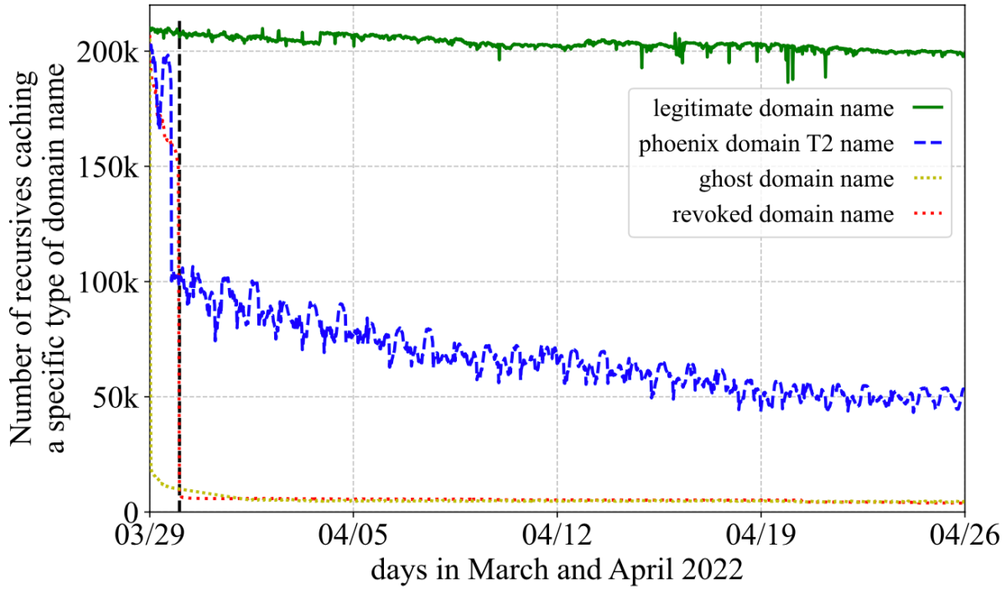
Experiments for T2

- **Short-term experiments**
  - Check how many labels are supported
  - 89% are vulnerable
  - After 100 rounds, 42% are vulnerable



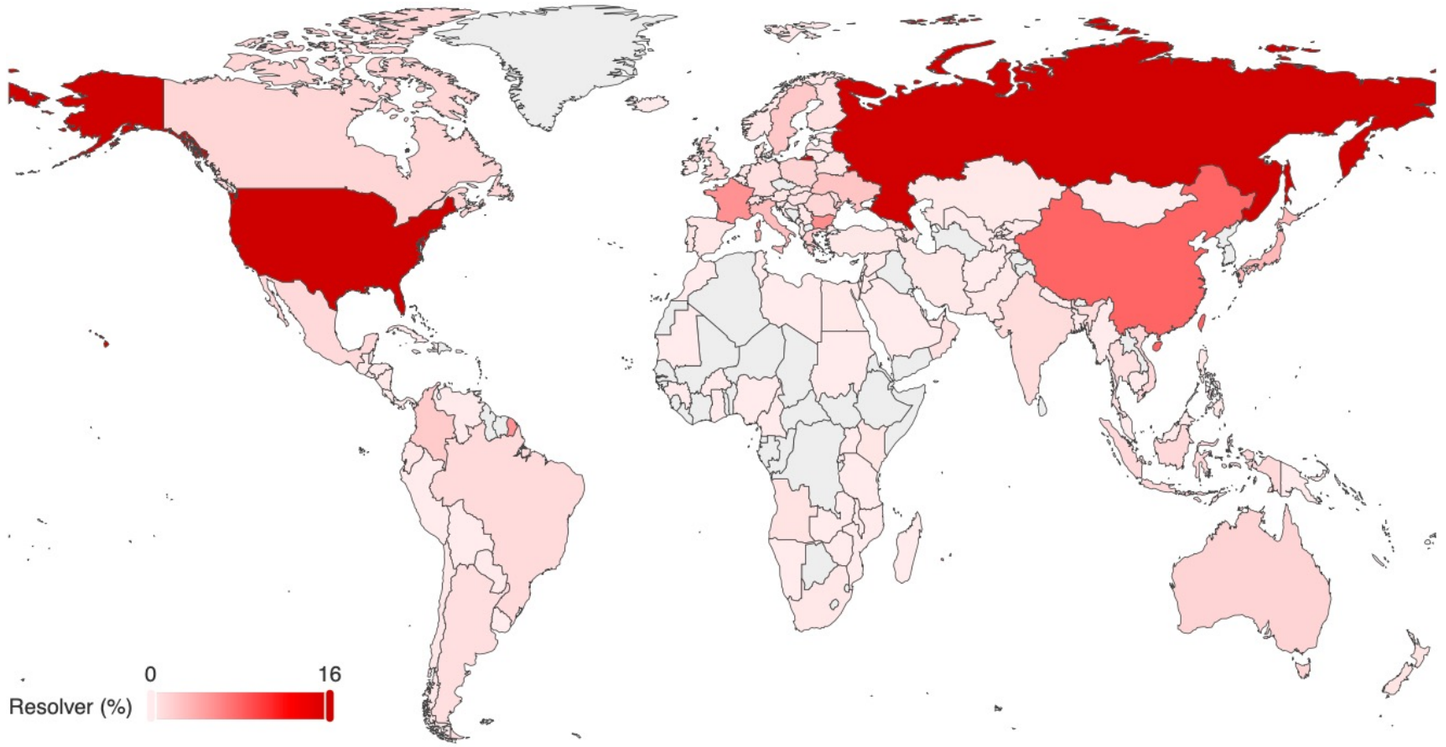
Experiments for T2

- **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



Mitigation

- 6 approaches
- Discussing with RFC editors
- For example,
- **M1:** when NS RRs expire, querying upstream for NS
- **M2:** trust NS from the parent more than the child
- **M3:** use small TTL values

Delegation Revalidation by DNS Resolvers
draft-ietf-dnsop-ns-revalidation-03

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.

Black Hat Sound Bytes

- **The DNS RFCs and specifications are not clear to provide a definitive definition for each operation, hence leaving a large attack window for ambiguous implementations.**
  - We should check the RFC's essential specifications.
- **The DNS implementations are not consistent across software, even for identical client queries.**
  - This inconsistency is likely to conceal possible risks, which should be thoroughly researched and evaluated.
- **The original DNS mechanism is insufficient to defend against several types of attacks.**
  - To improve it, we should propose new patches or redesign some structures.

Question

Thanks for listening!
Any question?

Paper

Tool

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