



DNS-OARC

Domain Name System Operations Analysis and Research Center

Misty Registry: An Empirical Study of Flawed Domain Registry Operation

Mingming Zhang, Yunyi Zhang, Baojun Liu, Haixin Duan, Min Zhang,
Fan Shi, and Chengxi Xu

Yunyi Zhang
Tsinghua University



清華大學
Tsinghua University

Overview

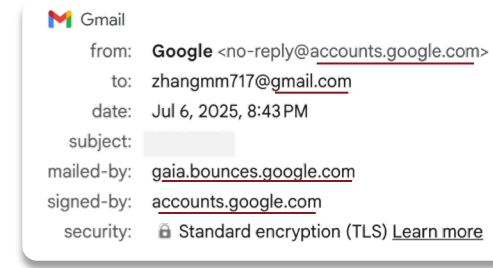
- **A top-down security analysis at the domain registry level**
 - Revealing domain status overlaps and complex operation triggers (e.g., ICANN policies, registrar/registrant settings).
- **Uncovered three flawed operation practices**
 - Redundant domain creation
 - Siloed DNS host management
 - Insufficient domain deletion
- **Impact of these flawed practices**
 - **6** mainstream registry backends and **812** TLDs face security risks
 - More than **1.6M** domain names are at risk of **domain takeover and hijacking**.

Domain Name: The Gateway of Our Digital Life

➤ Domain Names: Vital identifiers for Internet services



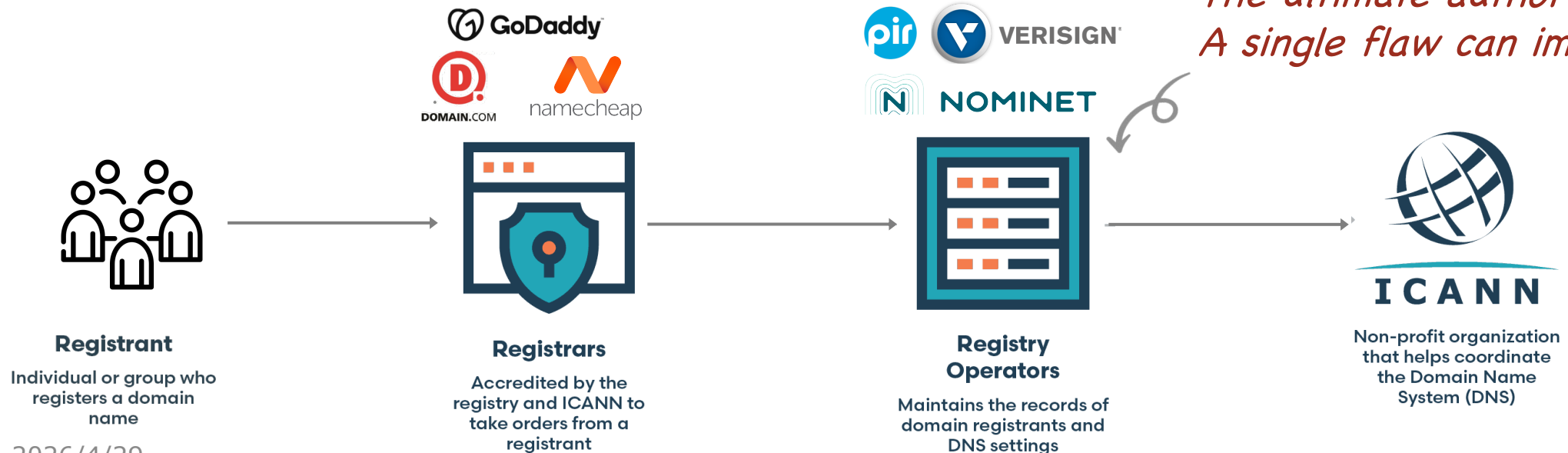
Website Access



Email Communication

➤ Managed by Registrars & Registries

*The ultimate authority for TLDs.
A single flaw can impact millions.*



Unregistered Domain Names in DNS

xn--4gq220j14gckc.top (一谕终见.top)

Registered with Alibaba Cloud

xn--4gqz56iuyholb.top (一諭終見.top)

Unregistered Domain Names in DNS

xn--4gq220j14gckc.top (一谕终见.top)

Registered with Alibaba Cloud

域名 一谕终见.top 的注册信息 

以下信息获取时间: 2023-12-09 23:57:18

[获取最新信息](#)

所有者联系邮箱 Registrant E-mail	如要进行联系, 请在线填写信息 了解更多 委托阿里云购买
注册商 Sponsoring Registrar	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
注册日期 Registration Date(UTC)	2023年11月22日
到期日期 Expiration Date(UTC)	2024年11月22日
域名状态 Domain Status	正常状态 (ok)  https://icann.org/epp#OK
DNS服务器 Name Server	DNS1: dns1.hichina.com DNS2: dns2.hichina.com

domain name registration data

xn--4gqz56iuyholb.top (一谕终见.top)

Unregistered Domain Names in DNS

xn--4gq220j14gckc.top (一谕终见.top)

Registered with Alibaba Cloud



xn--4gqz56iuyholb.top (一諭終見.top)

Unregistered Domain Names in DNS

xn--4gq220j14gckc.top (一谕终见.top)

Registered with Alibaba Cloud



xn--4gqz56iuyholb.top (一谕終見.top)

Unable to find the registration data

Registration data lookup tool

Enter a domain name or an Internet number resource (IP Network or ASN) [Frequently Asked Questions \(FAQ\)](#)

xn--4gqz56iuyholb.top

Lookup

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#) and the [registration data lookup tool Terms of Use](#).

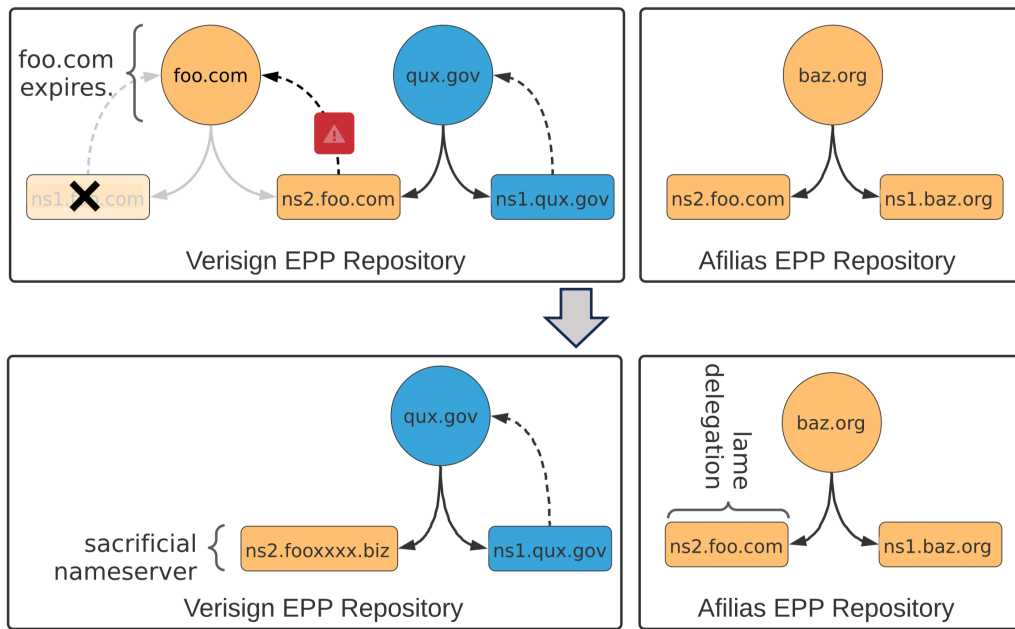
The requested domain was not found in the Registry or Registrar's RDAP server.



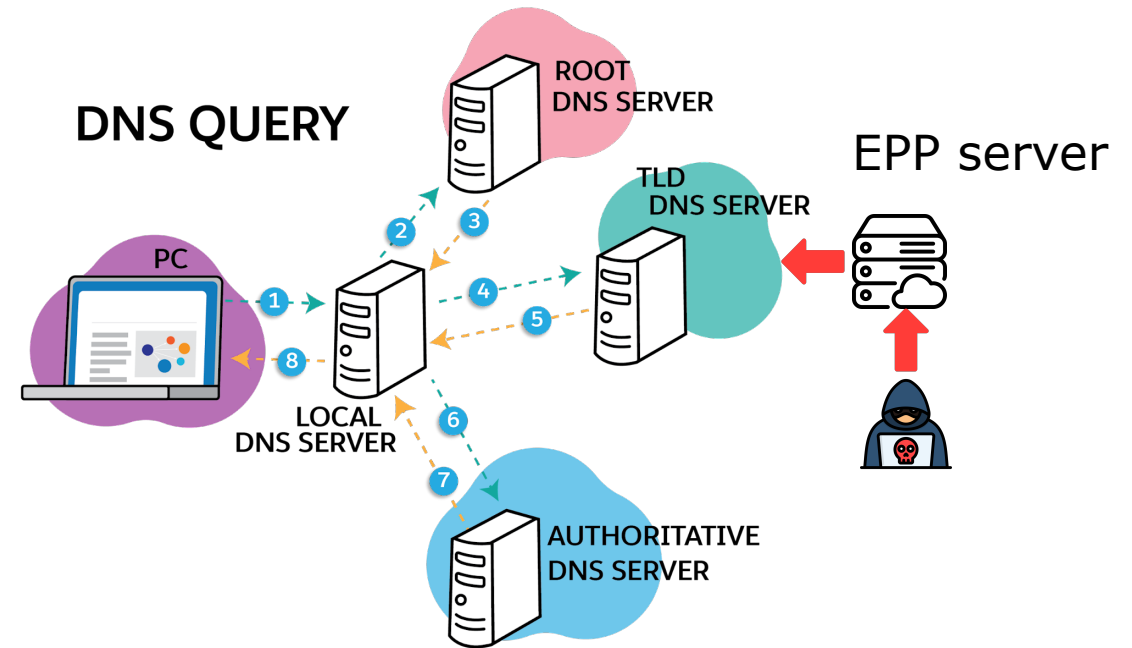
However, it is possible to access its website.

Threats Involving Domain Name Management

- Hijacking domains by sacrificial nameservers [IMC 2021]
- Controlling the TLD by controlling the EPP server [1]



The undocumented registrar practices of the registration bureau pose a risk of domain name hijacking.

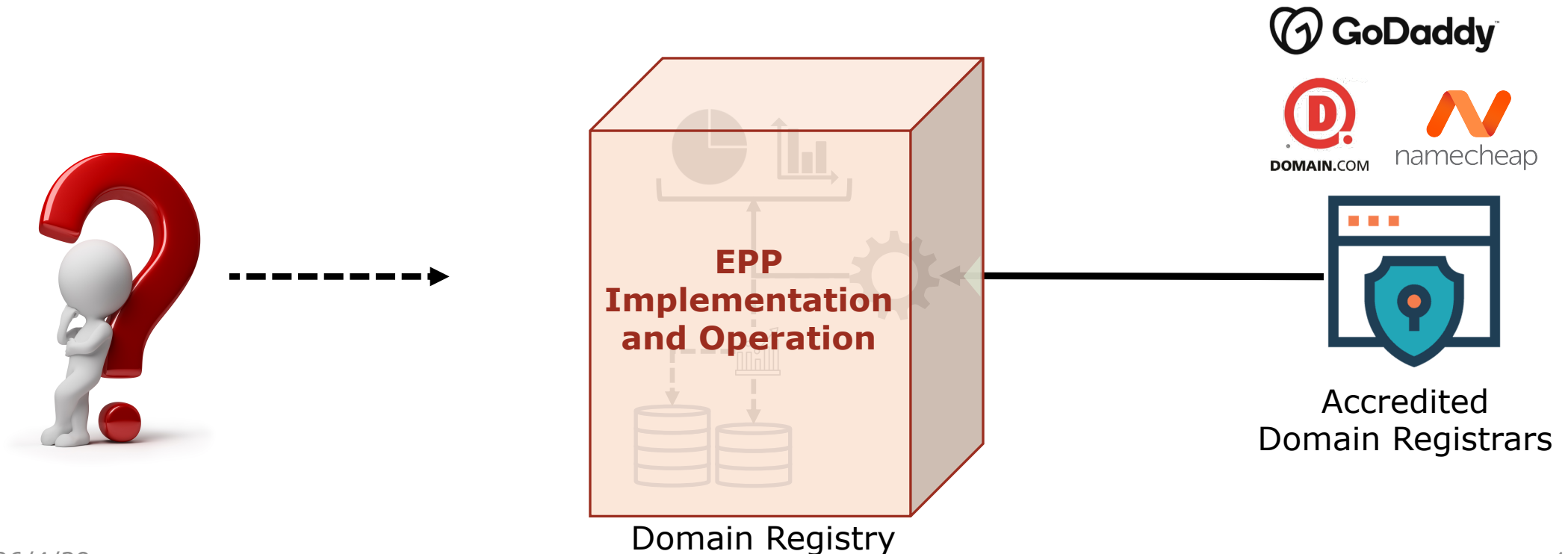


Registry software implementation flaw caused TLDs to be compromised.

However, Registry Security Remains Underexplored

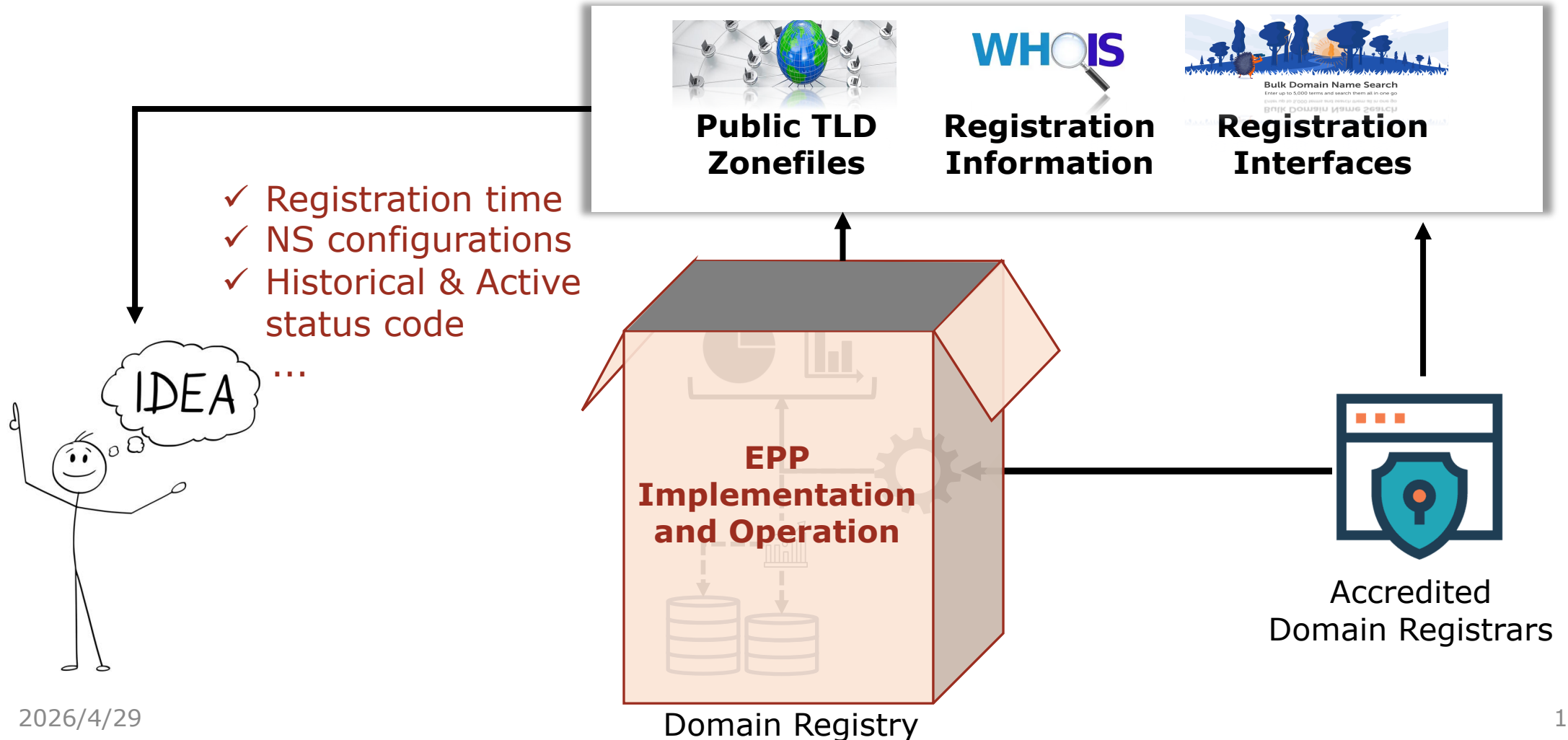
➤ Challenges

1. The EPP implementations are diverse and opaque.
2. Access is restricted to accredited registrars.



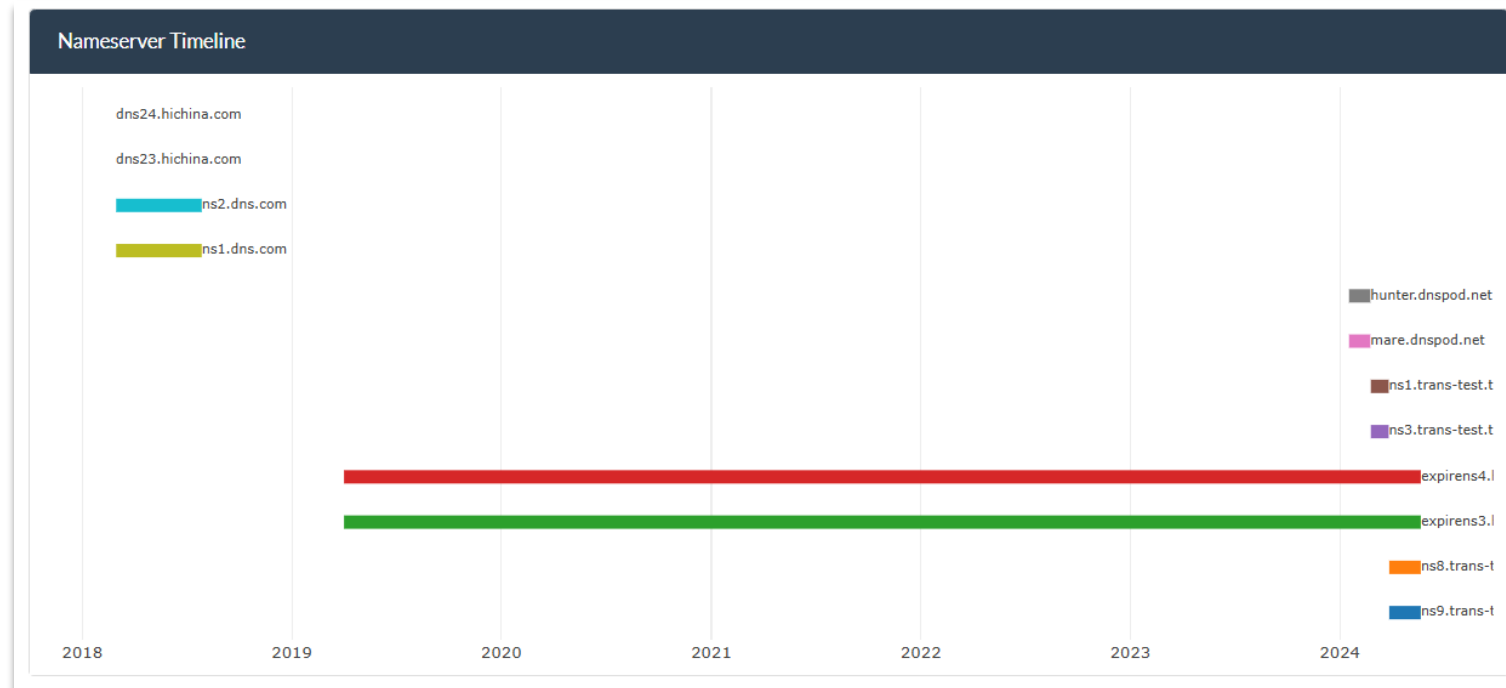
Infer inside operations from an outside view

- Publicly updated domain data enables coarse inference of EPP operations.



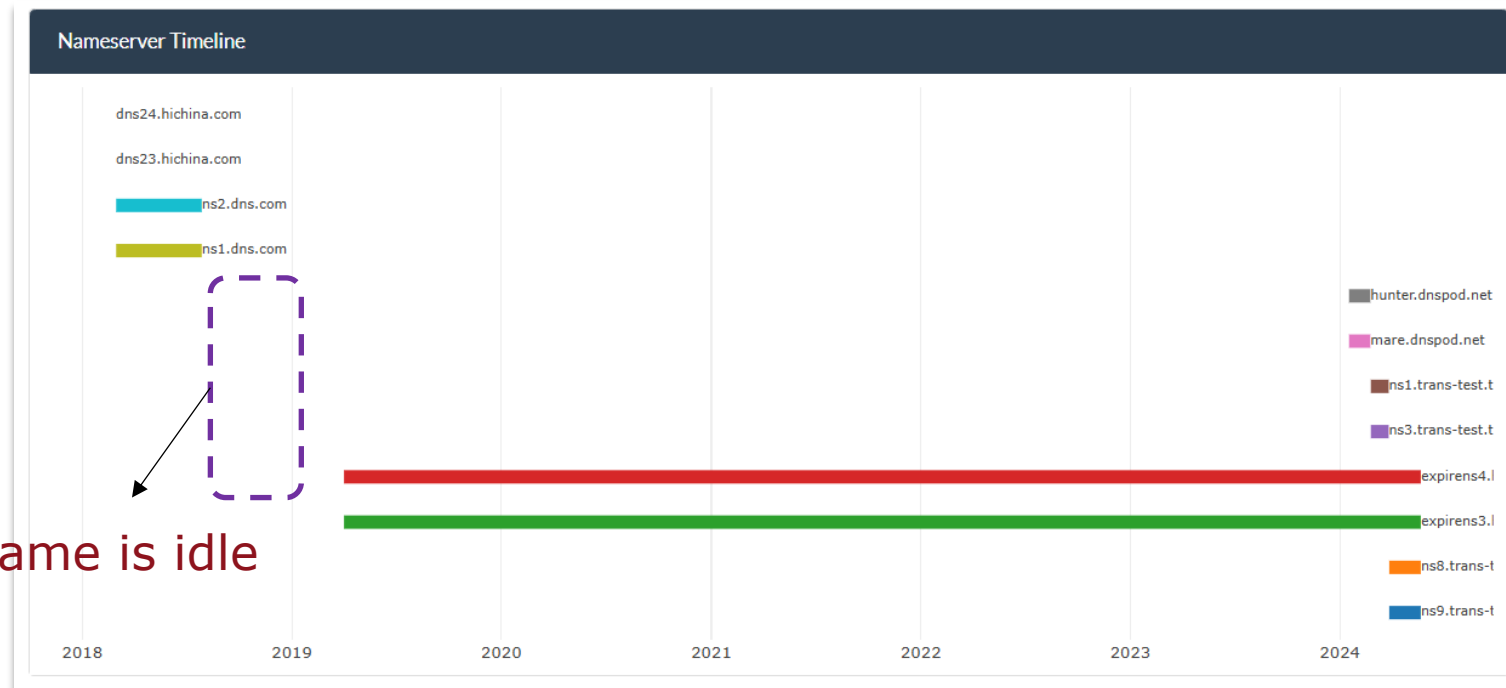
Infer inside operations from an outside view

- All changes to a domain name's delegation records involve the Registry
 - The registrant initiates the changes, and the **Registry** provides assistance.
 - The **Registry** makes changes on its own initiative
- An example



Infer inside operations from an outside view

- All changes to a domain name's delegation records involve the Registry
 - The registrant initiates the changes, and the **Registry** provides assistance.
 - The **Registry** makes changes on its own initiative
- An example

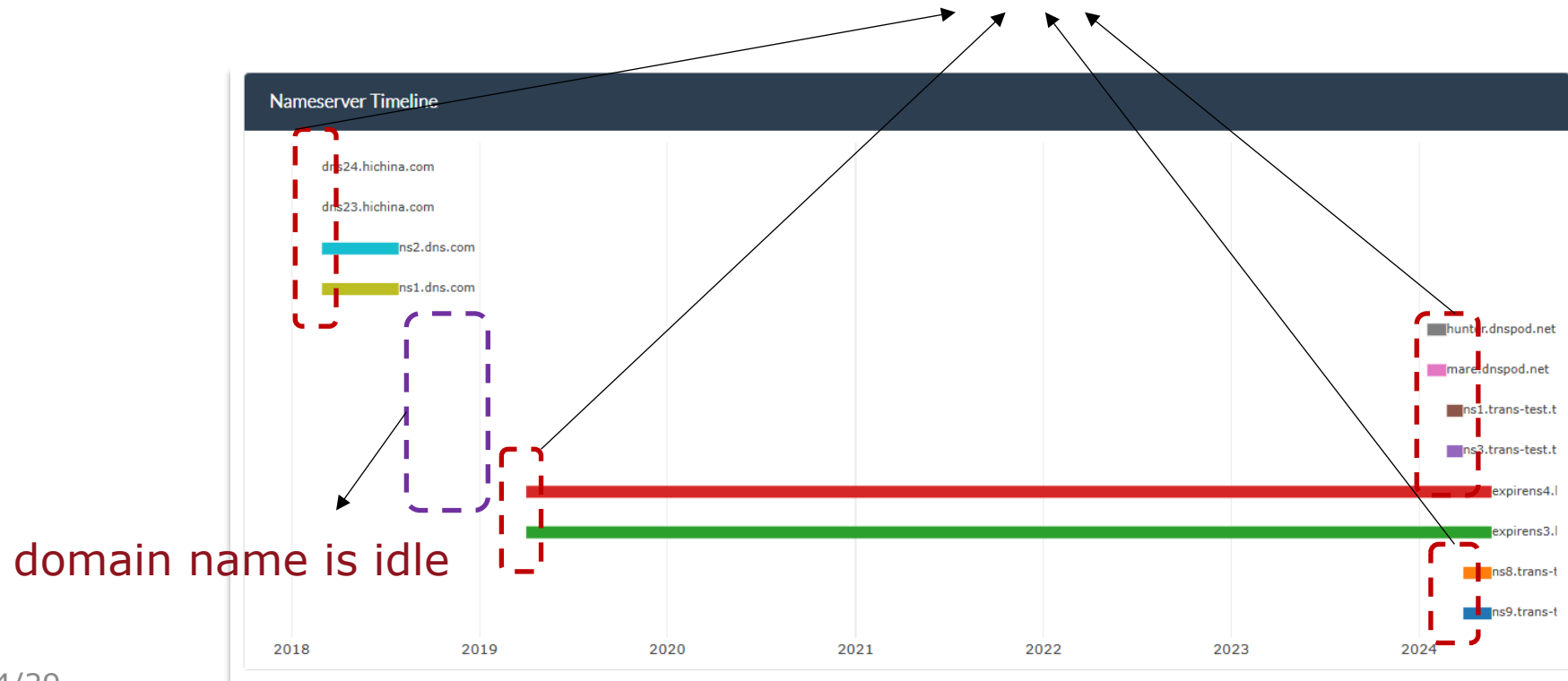


domain name is idle

Infer inside operations from an outside view

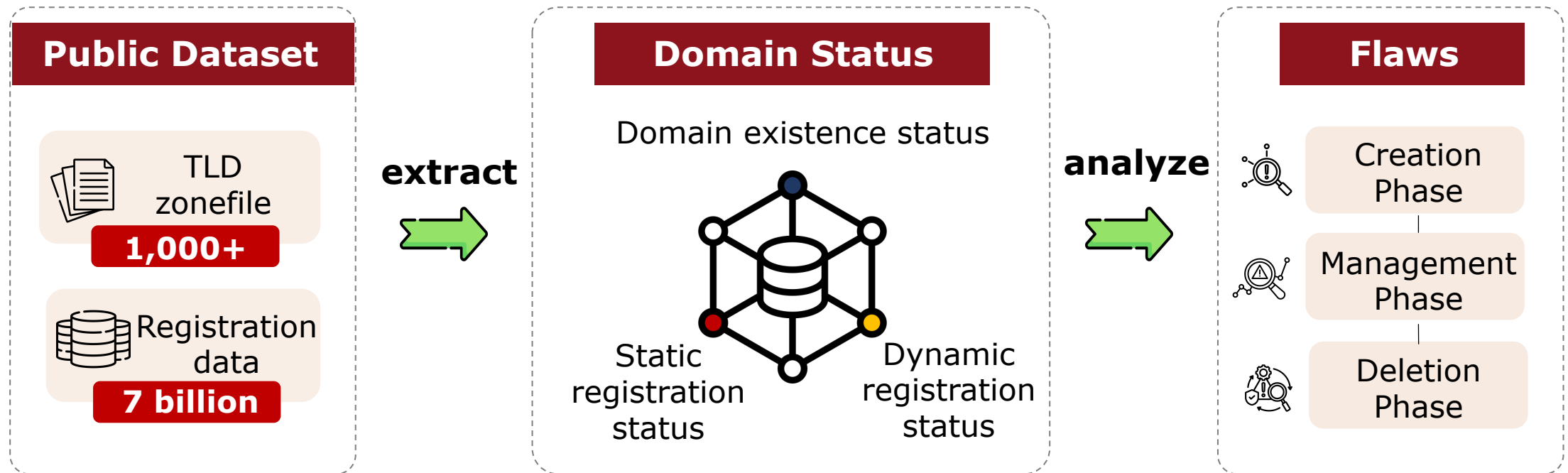
- All changes to a domain name's delegation records involve the Registry
 - The registrant initiates the changes, and the **Registry** provides assistance.
 - The **Registry** makes changes on its own initiative
- An example

Modification of the Domain Name Delegation Records

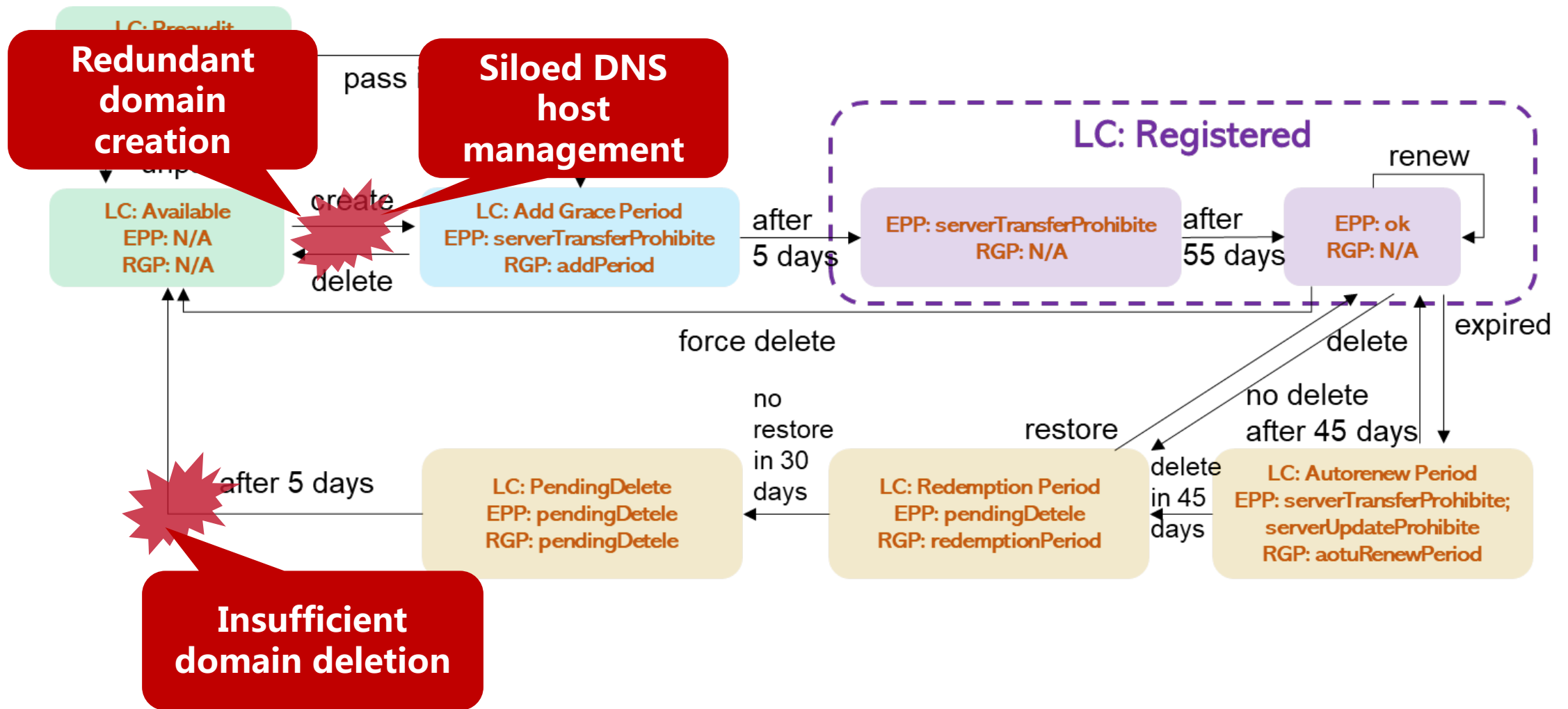


Pipeline

➤ Analyze domain name status using publicly available authorization and registration data



Uncover three registry operation flaws



Creation Phase: The "Twin Domain" Trap

When a registrant registers an internationalized domain name, the registry **automatically** adds the corresponding twin domain **without notifying the registrant**.

IDN Variant

PrimaryDomain:	测试.example,	xn--0zwm56d.example (Punycode)
TwinDomain:	測試.example,	xn--g6w251d.example (Punycode)

→ PrimaryDomain creation
→ TwinDomain creation

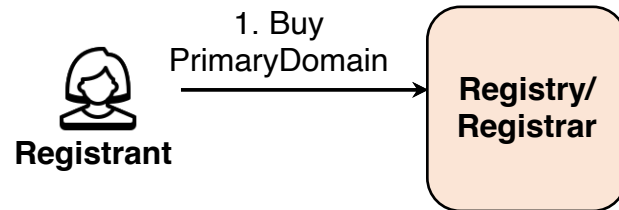
Creation Phase: The "Twin Domain" Trap

When a registrant registers an internationalized domain name, the registry **automatically** adds the corresponding twin domain **without notifying the registrant**.

IDN Variant

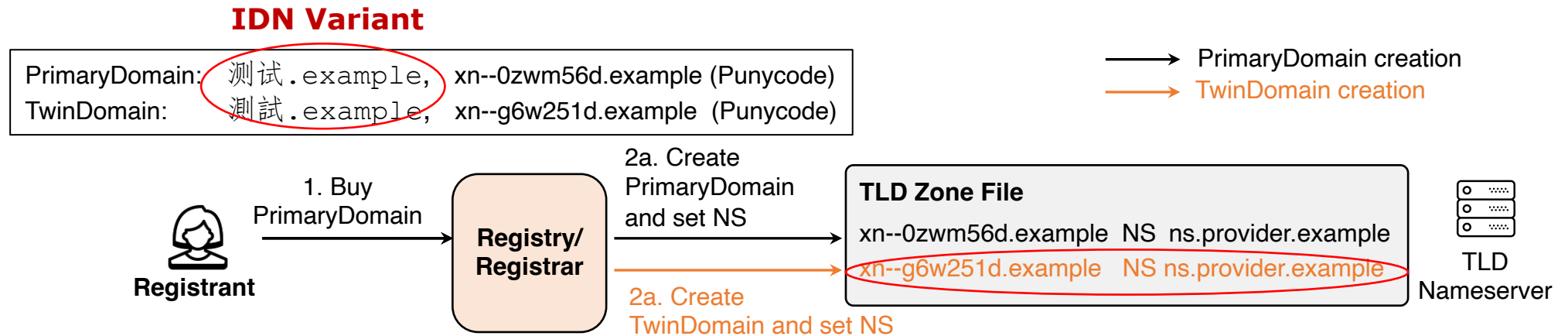
PrimaryDomain:	测试.example,	xn--0zwm56d.example (Punycode)
TwinDomain:	測試.example,	xn--g6w251d.example (Punycode)

→ PrimaryDomain creation
→ TwinDomain creation



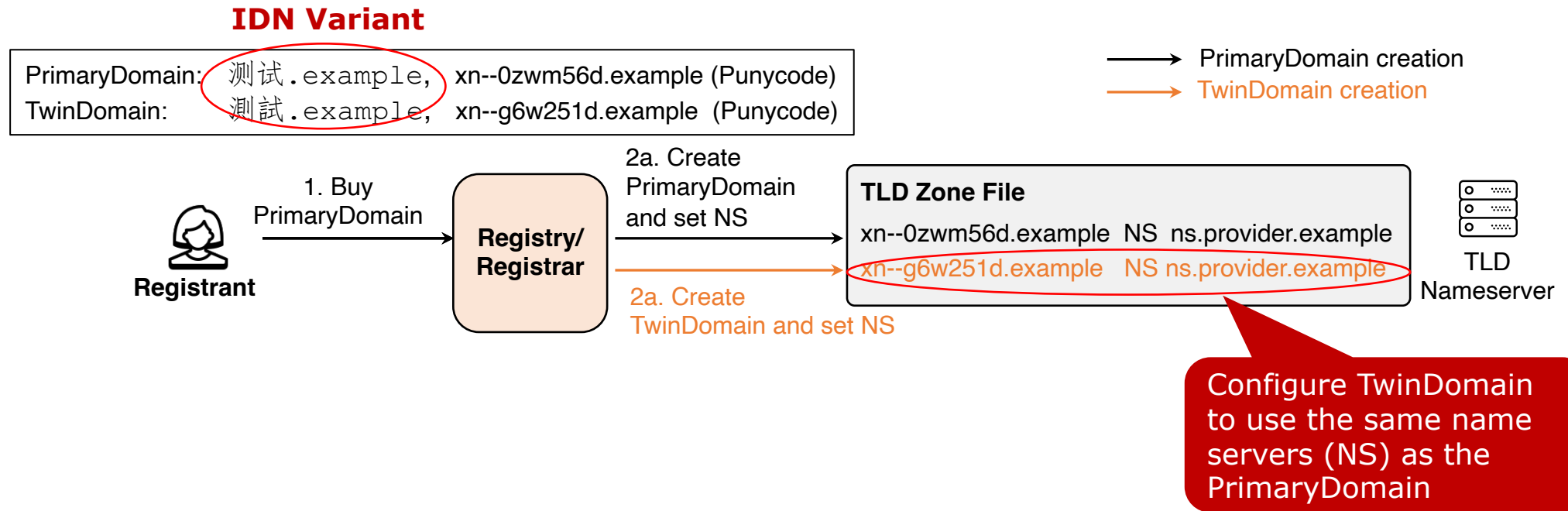
Creation Phase: The "Twin Domain" Trap

When a registrant registers an internationalized domain name, the registry **automatically** adds the corresponding twin domain **without notifying the registrant**.



Creation Phase: The "Twin Domain" Trap

When a registrant registers an internationalized domain name, the registry **automatically** adds the corresponding twin domain **without notifying the registrant**.

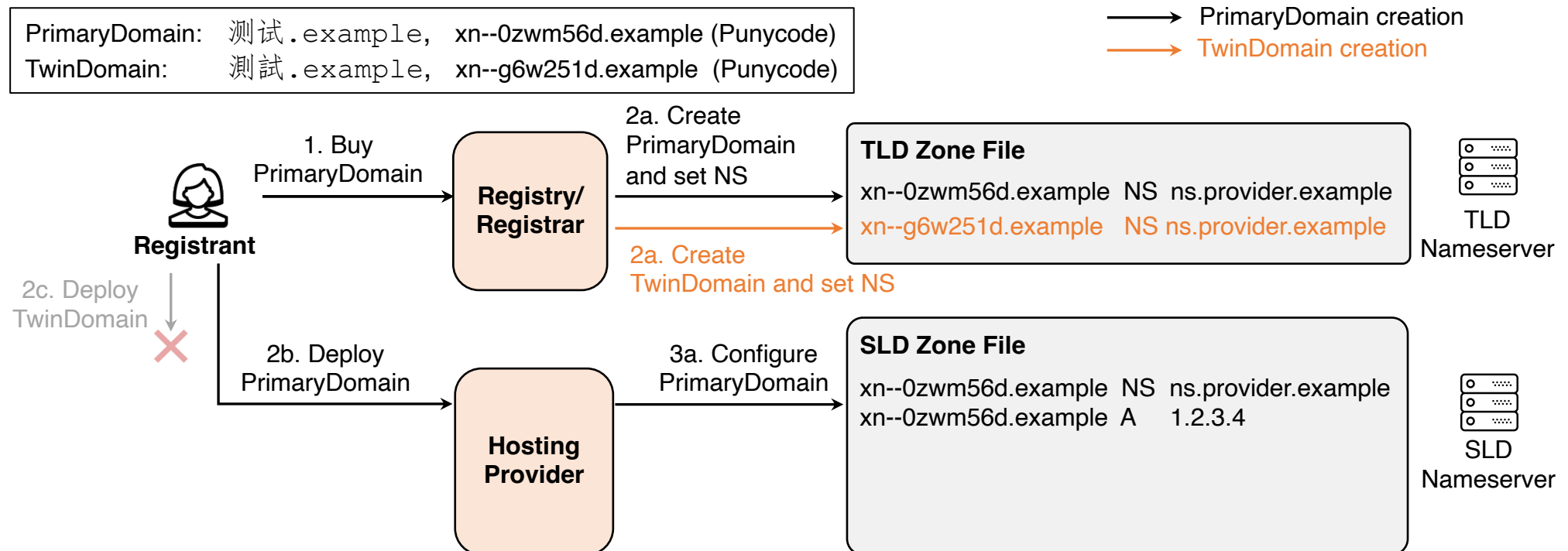


Creation Phase: The "Twin Domain" Trap

Attackers exploit **twin domains** to carry out abuse activities at zero cost.

Threat Model

1. The registrant deploys only **测试.example** on the hosting provider and does not deploy **測試.example**, as they are unaware of its existence.
2. The attacker unauthorizedly hosts the domain **測試.example** on the hosting provider and gains control over it.

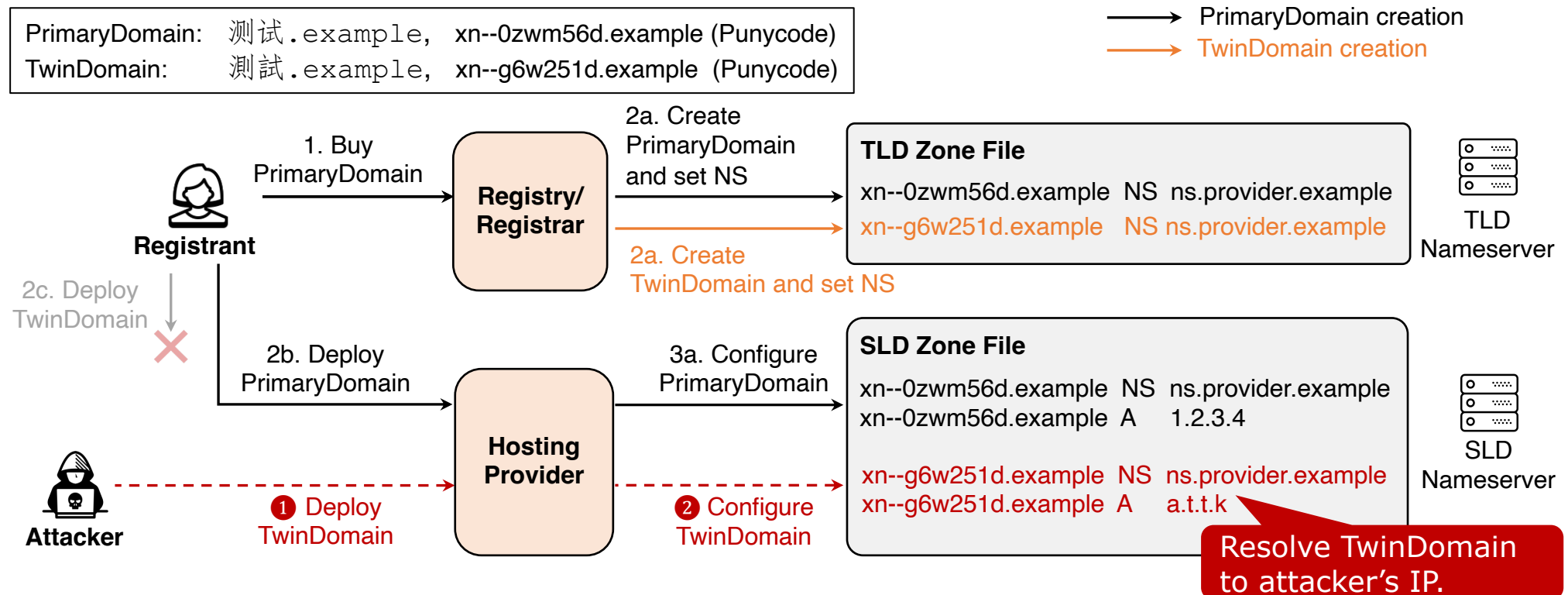


Creation Phase: The "Twin Domain" Trap

Attackers exploit **twin domains** to carry out abuse activities at zero cost.

Threat Model

1. The registrant deploys only **测试.example** on the hosting provider and does not deploy **測試.example**, as they are unaware of its existence.
2. The attacker unauthorizedly hosts the domain **測試.example** on the hosting provider and gains control over it.



Creation Phase: The "Twin Domain" Trap

Impact

- We identified 8,866 sets of twin domains, include domains under .top, .商城, .wang, .我爱你, and .com.
- Among them, **6,017** are vulnerable to potential **domain takeover**, and some have already been exploited.

xn--4gqz56iuyholb.top (一諭終見.top)



25 About - 裸聊直播 #Near me Visnagar [283](#) 928753416 43 42 4187635 93
14 52

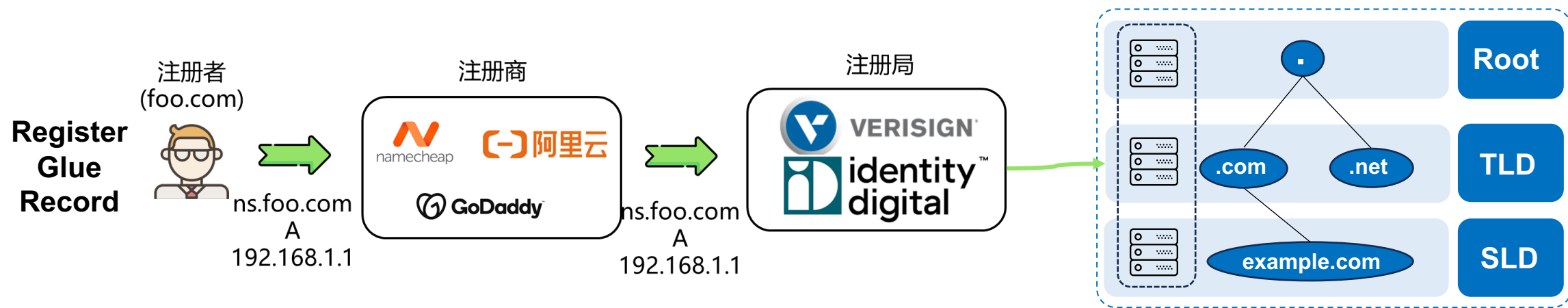


A twin domain was used for multiple fraudulent activities within a month

Twin domains are actively being abused

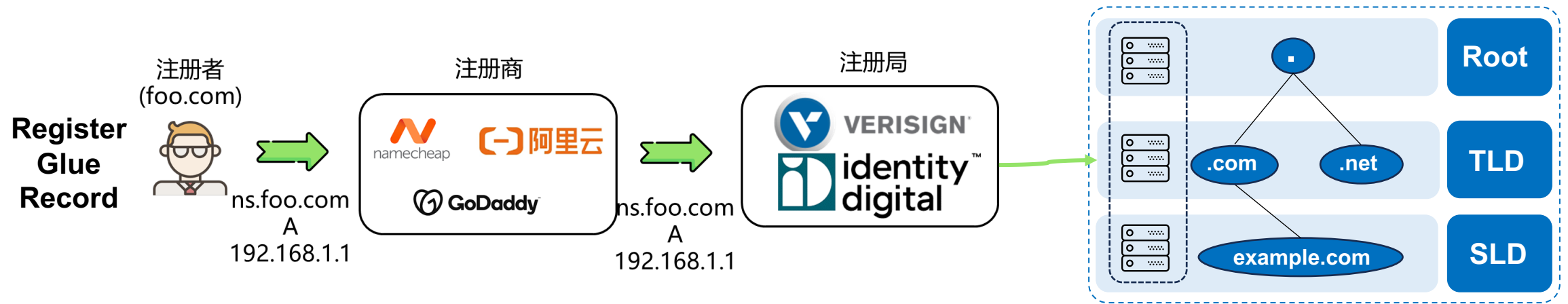
Management Phase: Unchecked Host Objects

Some registries often add all registrant-configured host objects to zone files without proper checks or purging.



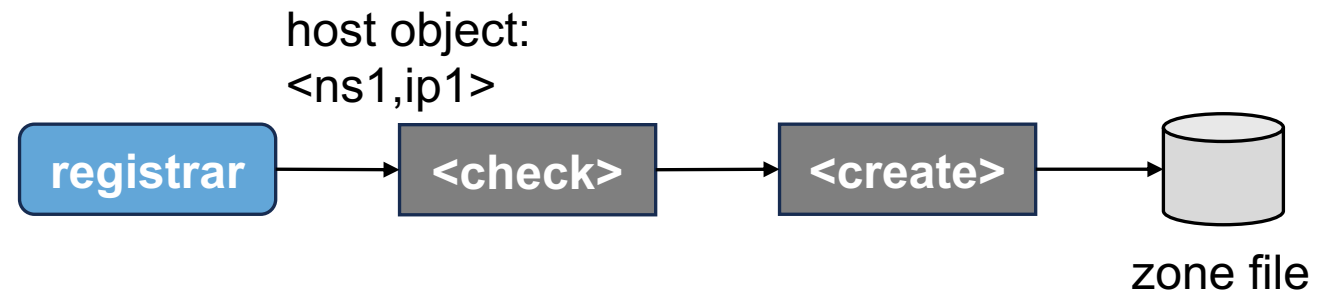
Management Phase: Unchecked Host Objects

Some registries often add all registrant-configured host objects to zone files without proper checks or purging.



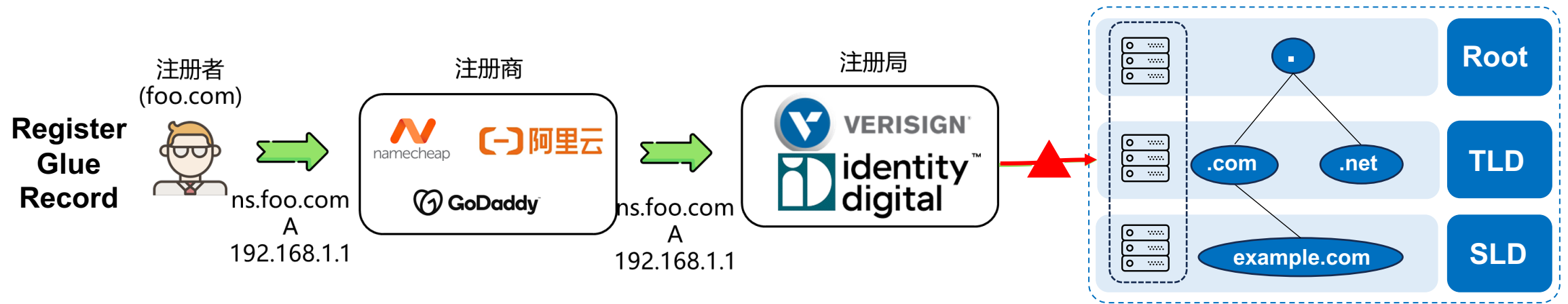
Mode 1

Write to zone file whenever you register the hosts objects:
top, com



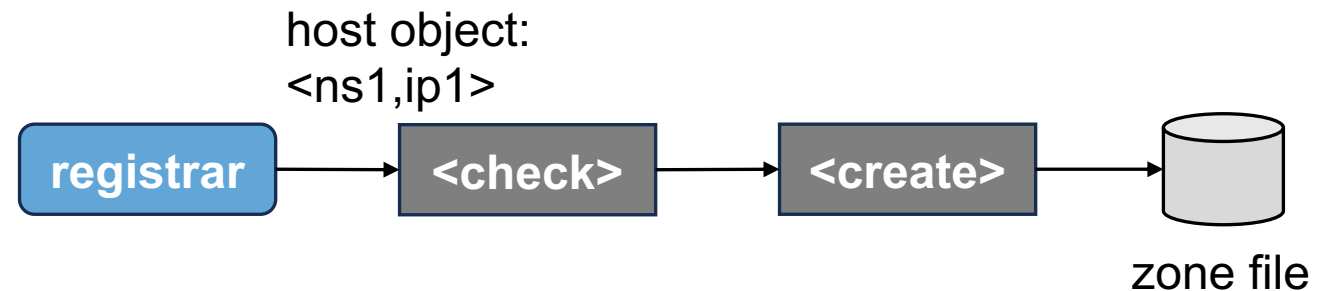
Management Phase: Unchecked Host Objects

Some registries often add all registrant-configured host objects to zone files without proper checks or purging.



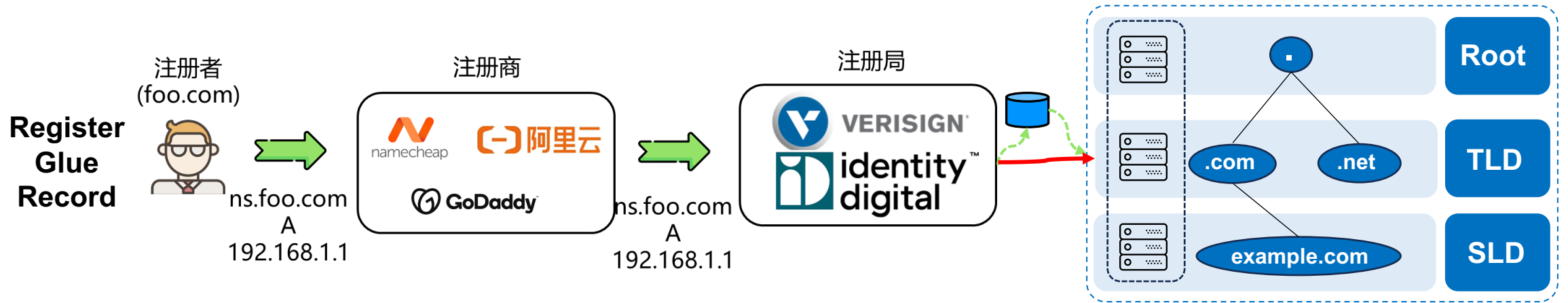
Mode 1

Write to zone file whenever you register the hosts objects:
top, com



Management Phase: Unchecked Host Objects

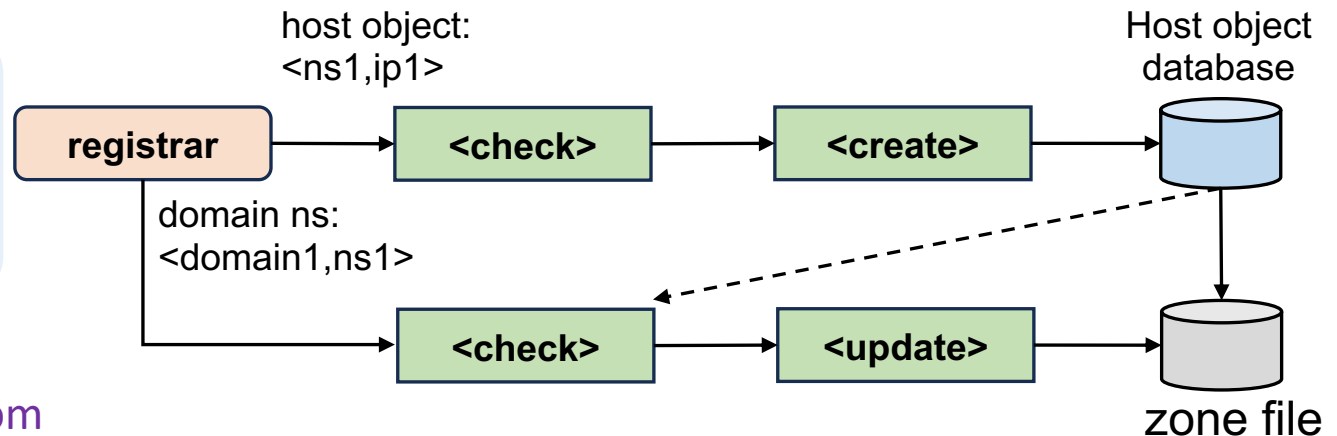
Some registries often add all registrant-configured host objects to zone files without proper checks or purging.



Mode2

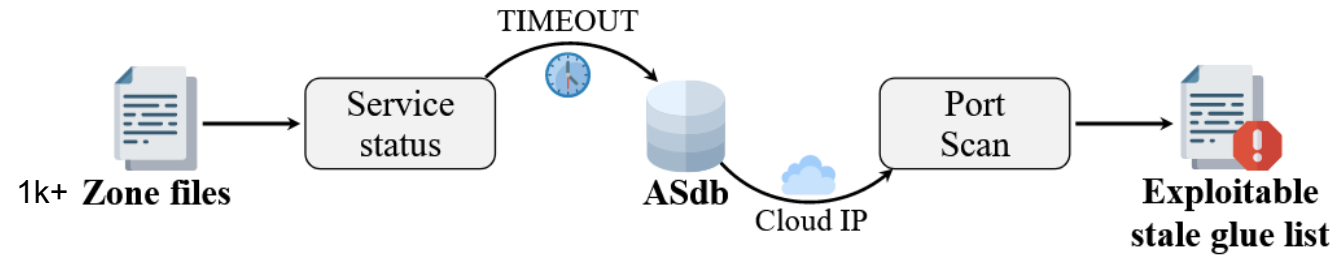
Write to zone file only when used by in-domain delegations, such as `.xyz`, `.site`

In-domain delegation :
`google.com NS ns1.google.com`



Management Phase: Unchecked Host Objects

Identifying stale glue records [1]



Impact

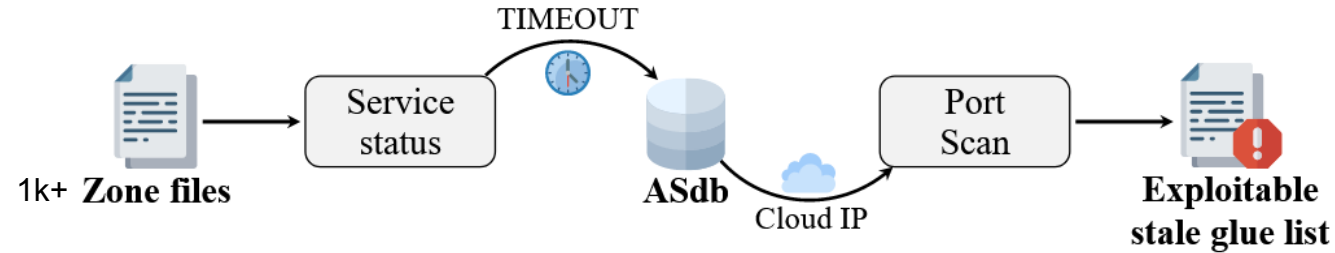
80,251 stale glue records that can be exploited, affecting **1,600,253** domain, including .com, .org, .net

All Glue Records	2,303,951 (100%)
→ Abandoned	532,363 (23.11%)
→ Active Glue Records	1,771,588 (76.89%)
→ Lack in-domain delegation	963,182 (54.37%)
→ Exploitable stale glue records	80,251 (8,33%)

TLD	# glue record	ratio
.com	47,593	13.34%
.org	18,926	6.58%
.info	4,157	4.31%
.net	3,707	7.84%
.top	1,645	12.11%

Management Phase: Unchecked Host Objects

Identifying stale glue records [1]



Impact

80,251 stale glue records that can be exploited, affecting **1,600,253** domain, including .com, .org, .net

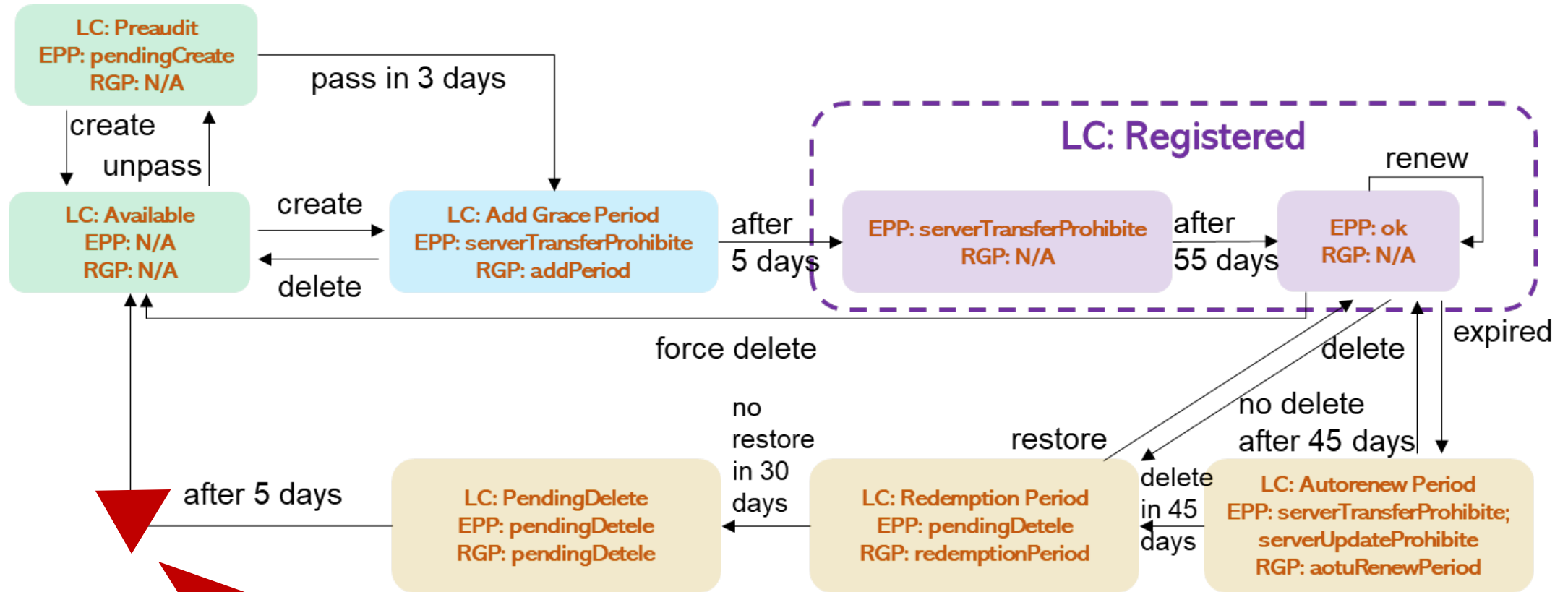
All Glue Records	2,303,951 (100%)
→ Abandoned	532,363 (23.11%)
→ Active Glue Records	1,771,588 (76.89%)
→ Lack in-domain delegation	963,182 (54.37%)
→ Exploitable stale glue records	80,251 (8,33%)

TLD	# glue record	ratio
.com	47,593	13.34%
.org	18,926	6.58%
.info	4,157	4.31%
.net	3,707	7.84%
.top	1,645	12.11%

We confirmed that the registry's glue record management strategy is the key factor leading to a large number of stale glue records

2026/4/29

Deletion Phase: Relic Domains and Hijacking Risks



When a domain name expires, the registry needs to clean up all resource records related to the domain name.

Deletion Phase: Relic Domains and Hijacking Risks

After a domain name expires, some of its delegation records remain uncleared.

untapped relic domains

The domain's delegation record has lost its administrator, so it remains in the zone file.

No WHOIS, but the NS record exists



resurrected relic domains

The new registrar/registrant does not have authority over the old delegation records. It can add new records but cannot delete zombie records.

The NS records in WHOIS are inconsistent with the NS records in the zone file.

Inconsistent NS records

	NS (zone)	NS (WHOIS)	Expiry Date	Static Registration Status	Dynamic Registration Status
exa.com	ns.foo.com	ns.exa.com	2025-04-08	registered	registered
exa.com	ns.exa.com				
bar.com	ns.bar.com	/	2023-03-08	unregistered	unregistered

domain not registered

Deletion Phase: Relic Domains and Hijacking Risks

Impact in the wild

Untapped relic domains

3,425 domains confirmed, covering **11** TLDs, including top , app , vip, 我爱你.
Registrie backends: GoDaddy、Nominet、Google、ZDNS 和 Beijing Tele-infoNetwork

Resurrected relic domains

19 domains confirmed, covering **13** TLDs, including top , ren, courses , biz , cymru
Registrie backends : Identity Digital、GoDaddy、Nominet 和 ZDNS

Registry ¹	#TLD ²	Resurrected relic domain		Untapped relic domain	
		TLD	#Domain	TLD	#Domain
Identity Digital [3]	447	zone	1	-	-
GoDaddy [24]	216	courses, design, party, club, wiki, rugby	8	vip	1
Nominet [45]	73	cymru, bot, wales	3	cymru	4
Google [25]	46	-	-	app, page, dev, みんな	47
ZDNS [8]	20	top, ren	5	top, wang, ren, 我爱你	3,374
Beijing Tele-info [6]	10	-	-	信息	1
Total	812	-	17	-	3,425

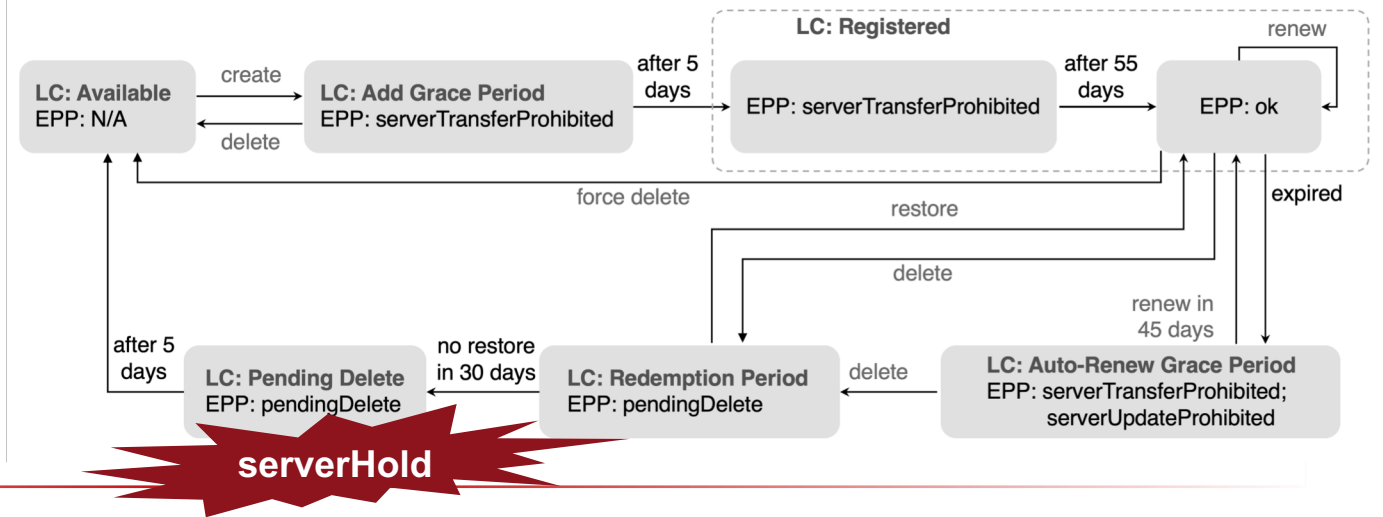
¹: The relationship between new gTLDs and their registry backends is derived from the project nTLDStats [26].

²: The number of new gTLDs supported by the registry backend.

Deletion Phase: Relic Domains and Hijacking Risks

Root Cause Analysis

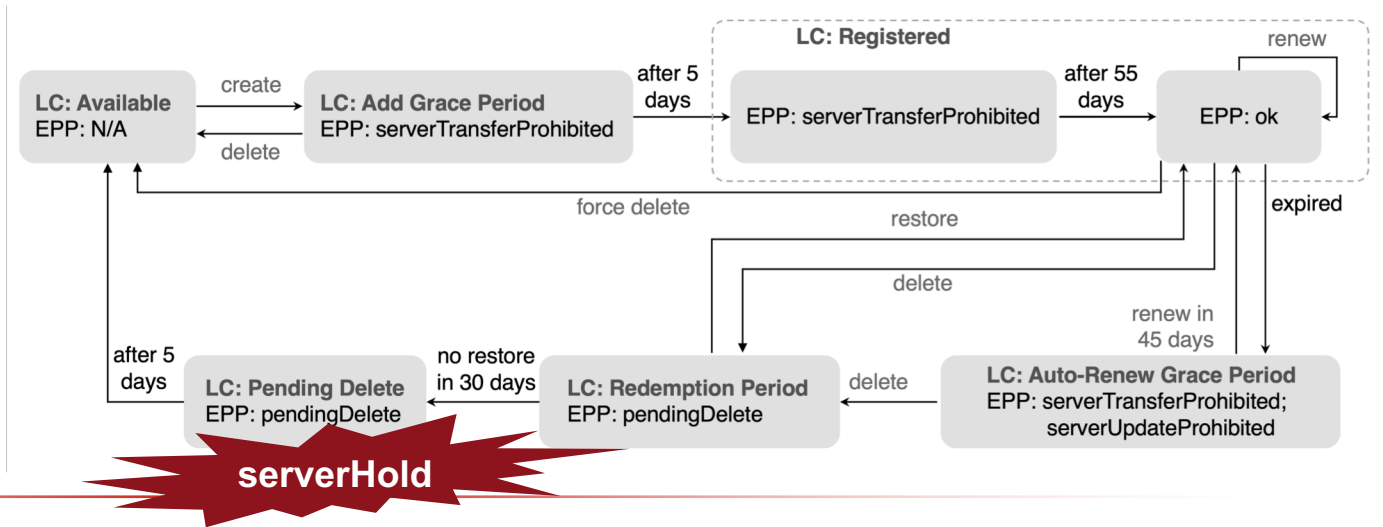
The **pendingDelete** status and the **serverHold** status of the domain overlap, causing the software to be unable to clean up the delegation records normally.



Deletion Phase: Relic Domains and Hijacking Risks

Root Cause Analysis

The **pendingDelete** status and the **serverHold** status of the domain overlap, causing the software to be unable to clean up the delegation records normally.



Disclosure

Google and ZDNS have confirmed the issue and have completed the fix



Lai Jiang <jianglai@msn.com>

收件人: Jingkai Yu

抄送: 你

Hi Jingkai,

Thank you for reaching out prior to publication. We appreciate it. I checked our bug tracking system and it appears to be fixed. I am double checking with the person responsible to make sure that is indeed the case and will get back to you shortly.

Best,
Lai

...



周二 2025/1/21 20:58

Stale and Dangling records are harmful, But ...

- **Dangling record risk was first identified in 2016**
- **Zombie awakening attack (2020)**
- **XDAuth attack (2024)**
- **Sitting Ducks attack (2024)**

Dangling resource records are being widely abused.

We can do it ...

EXAMPLE

Route 53 protects `child.example.com` from dangling delegation records risk by preventing `<ns1>`, `<ns2>`, `<ns3>`, and `<ns4>` from being assigned to newly created hosted zones with the same domain name.

The screenshot shows the AWS documentation page for "Protection from dangling delegation records in Route 53". The page is part of the "Developer Guide" under "Amazon Route 53". The main content area contains the following text:

With Route 53, a customer can create a hosted zone, such as `example.com`, to host their DNS records. Each hosted zone comes with a "delegation set", which is a set of four name servers that a customer can use to configure NS records in the parent domain. These NS records can be called "delegation NS records", or "delegation records".

In order for the `example.com` Route 53 hosted zone to become authoritative, the rightful owner of the `example.com` domain needs to configure delegation records in their ".com" parent domain through the domain registrar. In cases where a customer loses access to the four name servers configured in the parent domain, for example because the associated hosted zone is deleted, it can create a risk that an attacker can exploit. This is referred to as a "dangling delegation records" risk.

Route 53 protects against the dangling delegation record risk in the case where a hosted zone is deleted. After deletion, if a new hosted zone is being created with the same domain name, Route 53 will check if the delegation records pointing to the deleted hosted zone are still present in the parent domain. If they are, Route 53 will prevent any overlapping name servers from being assigned. This is scenario 1 in the following examples.

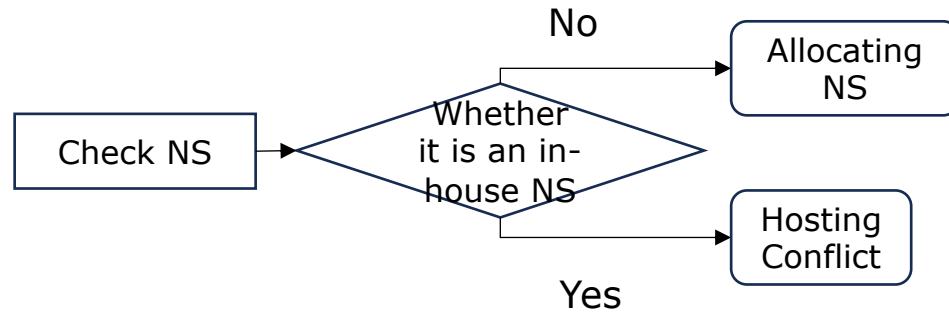
However, there are other dangling delegation record risks, which Route 53 can't protect against, as

The page also features a sidebar with a navigation menu, a search bar, and a "Create an AWS Account" button. The sidebar menu includes sections like "Resolver", "Security", "Data protection", "Identity and access management", "Logging and monitoring", "Compliance validation", "Resilience", "Infrastructure security", "Sending findings to Security Hub CSPM", "Monitoring", "Troubleshooting", "IP address ranges", "Tagging resources", "Tutorials", and "Best practices". The "Data protection" section is expanded, showing "Protection from dangling delegation records" as the selected item.

How to do it ...

Double Clear

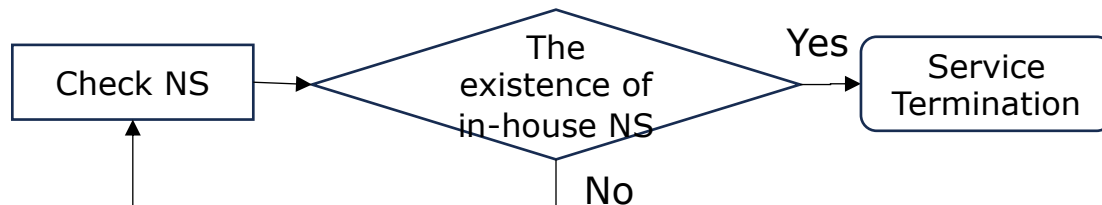
FIRST: When a user intends to host a domain



When domain hosting providers assign specific Name Servers (NS) to a user, they first perform an **NS check** to verify if any **stale or legacy NS records** exist.

GOAL: prevent vulnerable domains from being exploited by malicious actors

SECOND: When a user terminates the hosting service



The provider enforces the removal of the domain's NS records through an active verification mechanism.

2026/4/29 **GOAL: inhibit the creation of additional dangling records at the source**



DNS-OARC

Domain Name System Operations Analysis and Research Center

Thank You & Get in Touch!

Yunyi Zhang

Emails:

yunyizhang@mail.tsinghua.edu.cn



清華大學
Tsinghua University