DareShark: Detecting and Measuring Security Risks of Hosting-Based Dangling Domains

Mingming Zhang, **Xiang Li**, Baojun Liu, Jianyu Lu, Yiming Zhang,
Jianjun Chen, Haixin Duan, Shuang Hao, and Xiaofeng Zheng

(Accepted by [ACM SIGMETRICS 2023])

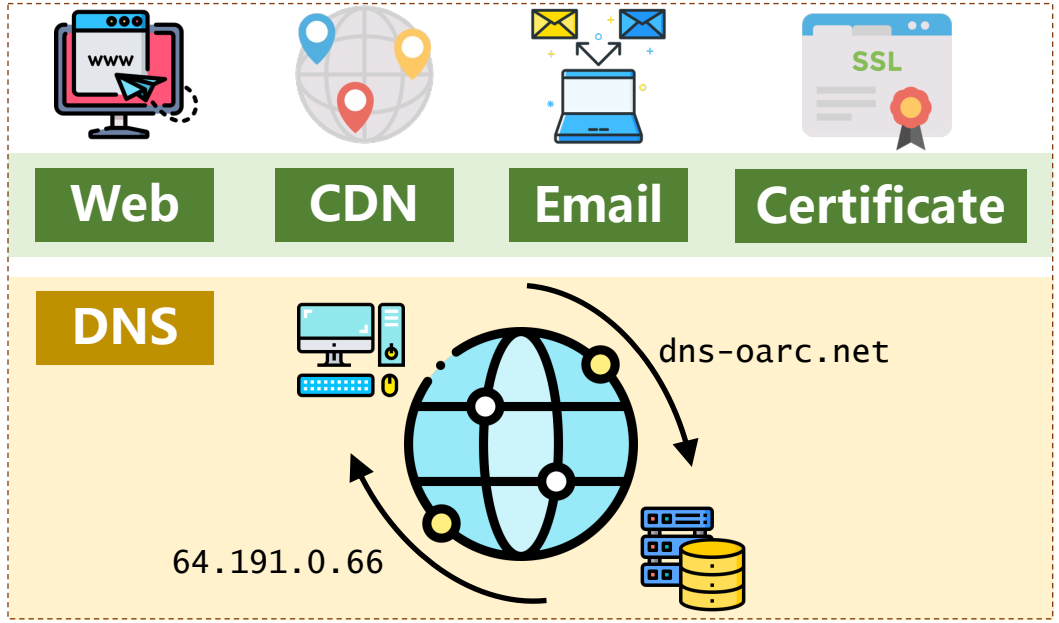
Presenter: Xiang Li, Tsinghua University

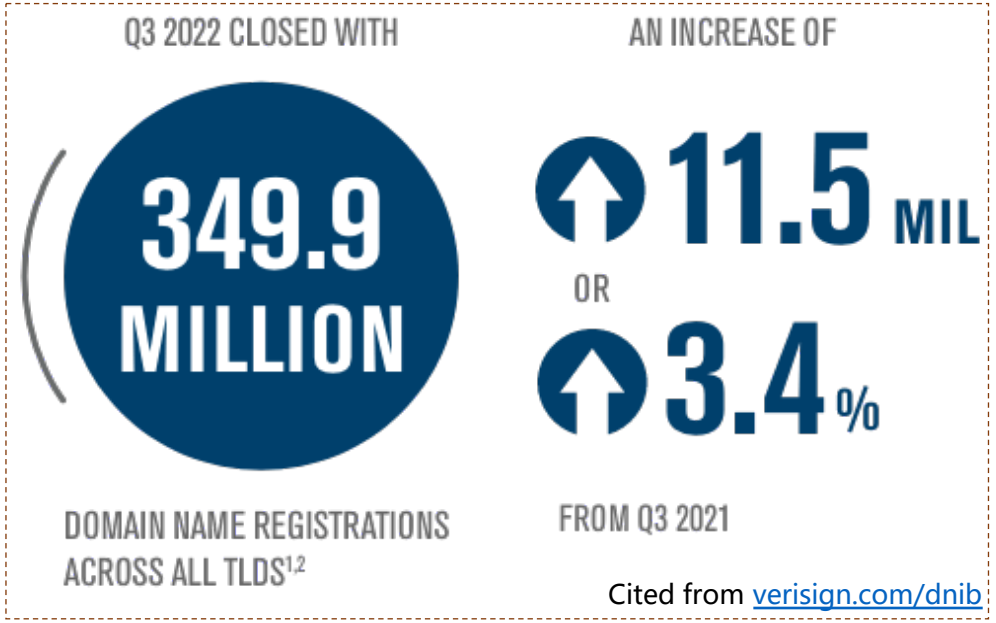
February 16th, 2023

Domain Name

➢Domain name system (DNS)

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





Cited from verisign.com/dnib

Domain Name Abuse

- **Adversaries could exploit the domains outside of their authority for malicious activities**
  - Botnet, phishing, malware distribution, etc.

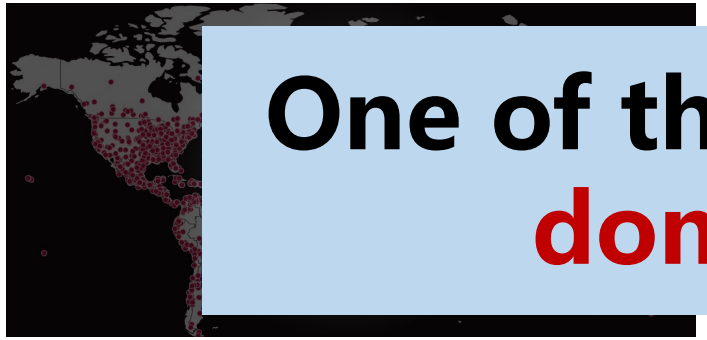
Cited from bleepingcomputer.com

Cited from scmp.com

Cited from norton.com

Domain Name Abuse

- **Adversaries could exploit the domains outside of their authority for malicious activities**
  - Botnet, phishing, malware distribution, etc.



One of the powerful ways is domain takeover

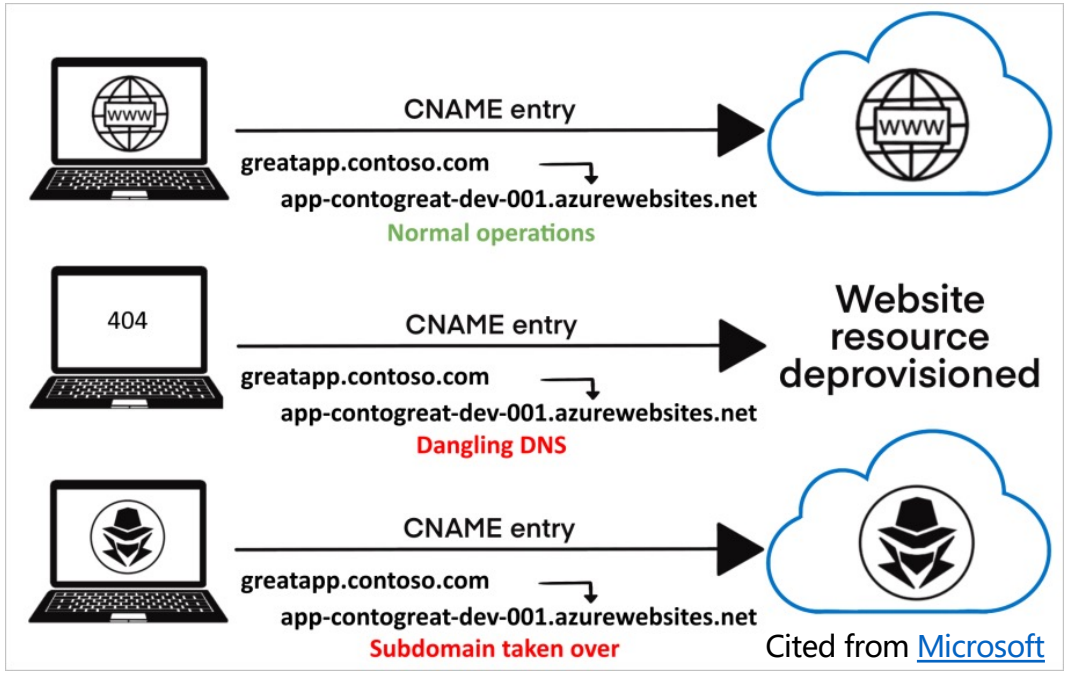
Cited from bleepingcomputer.com

Cited from scmp.com

Cited from norton.com

Domain Name Takeover

- **DNS Resource Records (RRs) → Use-After-Free**

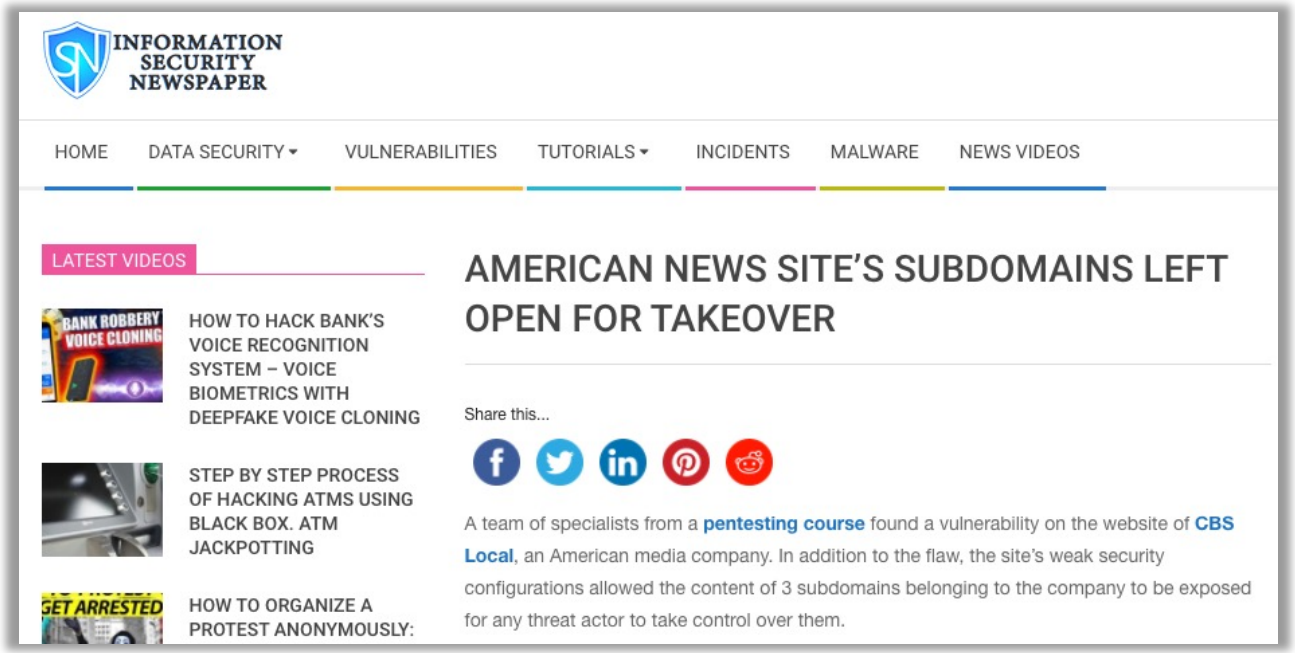


- **Security-sensitive Dangling DNS Records (Dares) → Domain Takeover**
  - A, CNAME, NS

All Your DNS Records Point to Us [CCS '16]

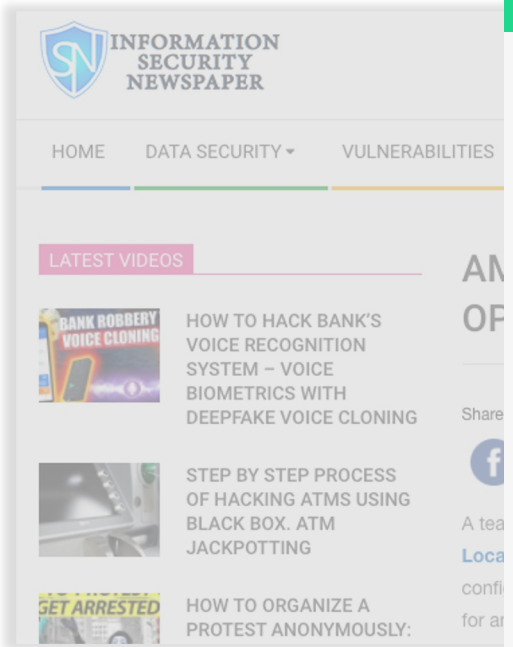
Domain Name Takeover

- Many domain-takeover incidents occur in recent years



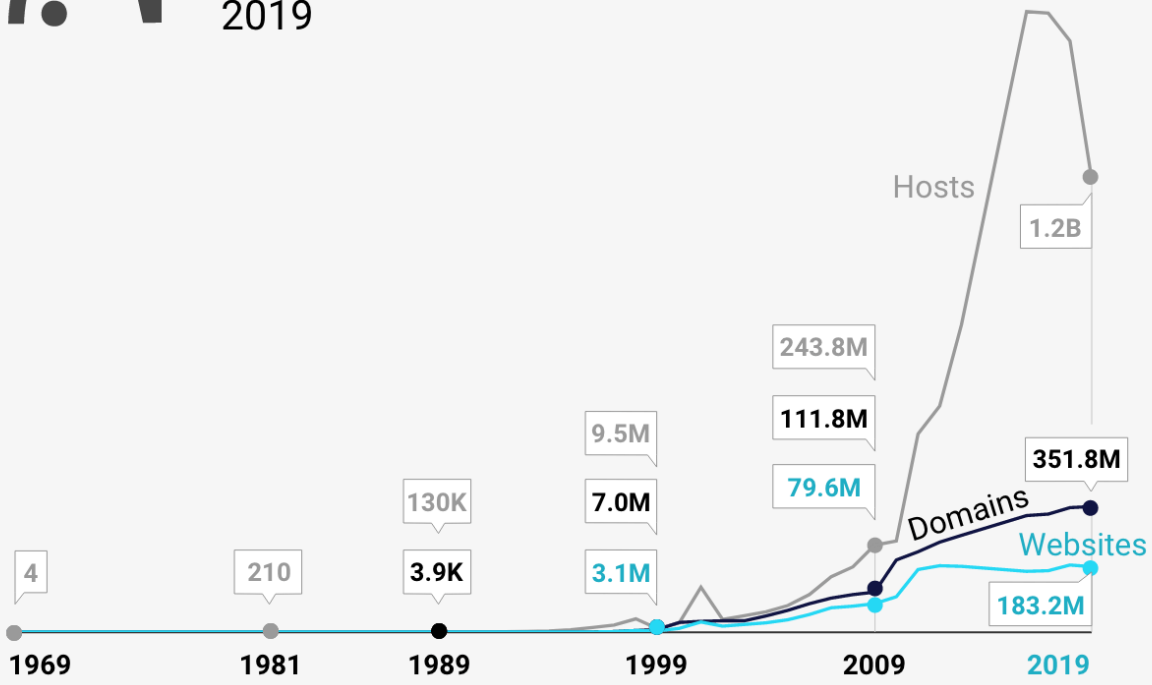
Domain Name Takeover

- Many dor ecent years



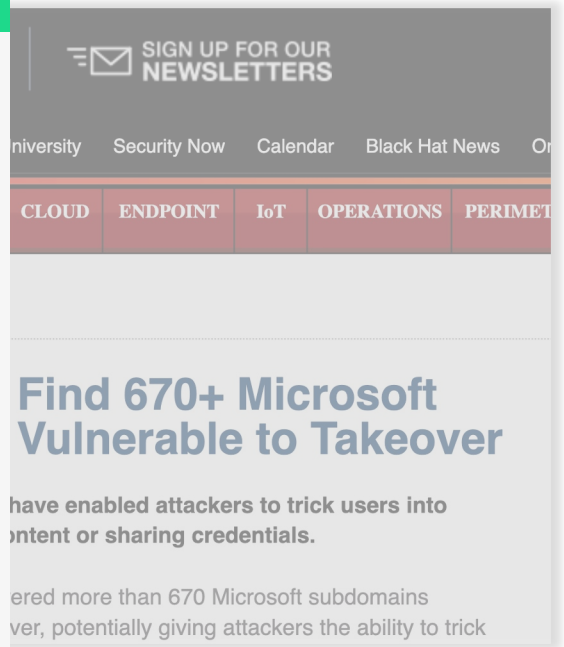
Web Hosting Statistics 2023: State of The Website Hosting Industry

The growth chart with number of web hosts, domain names, and websites from 1969 to 2019



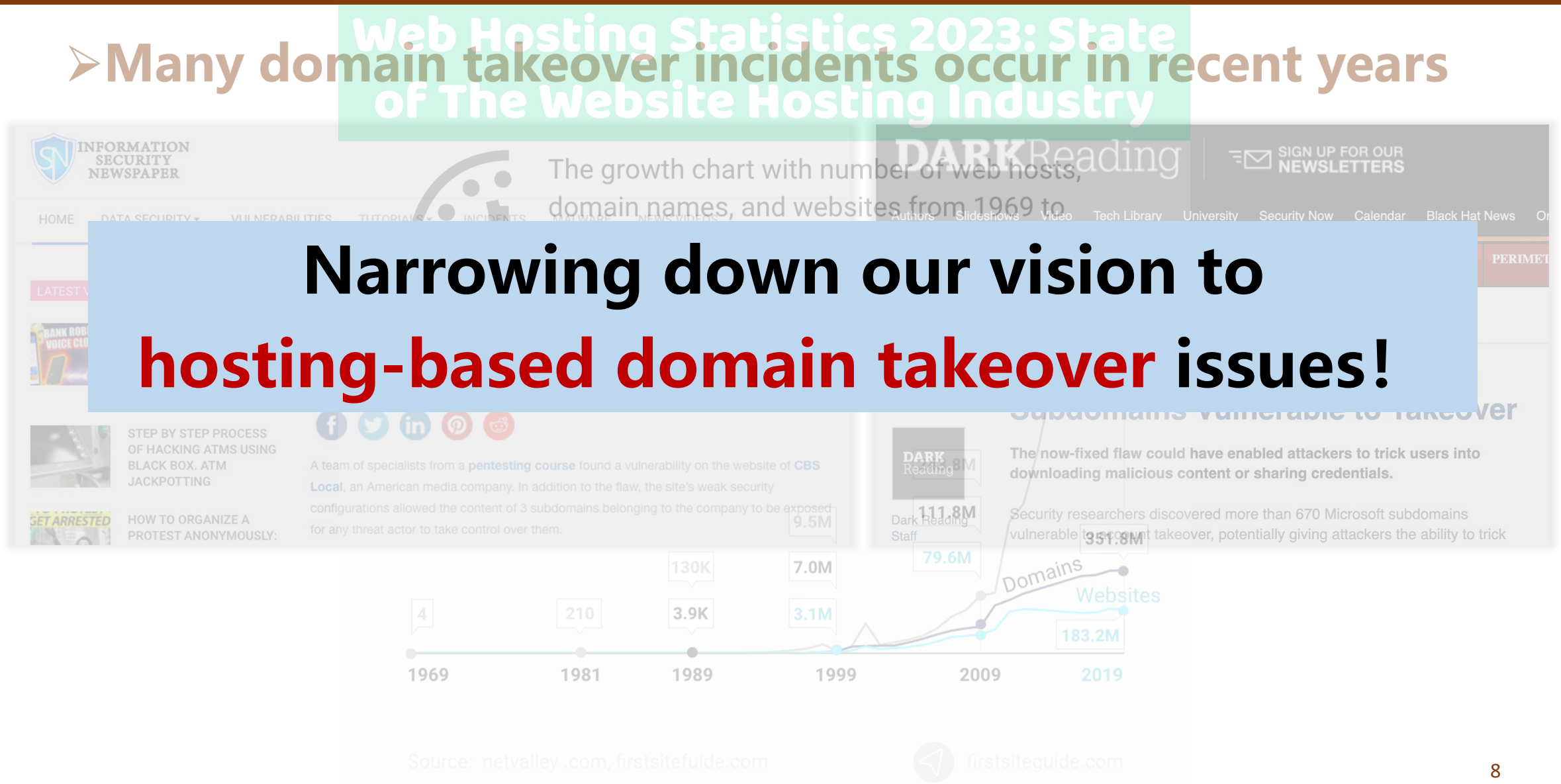
Source: netvalley .com, firstsitefuide.com

firstsiteguide.com



Domain Name Takeover

- Many domain takeover incidents occur in recent years

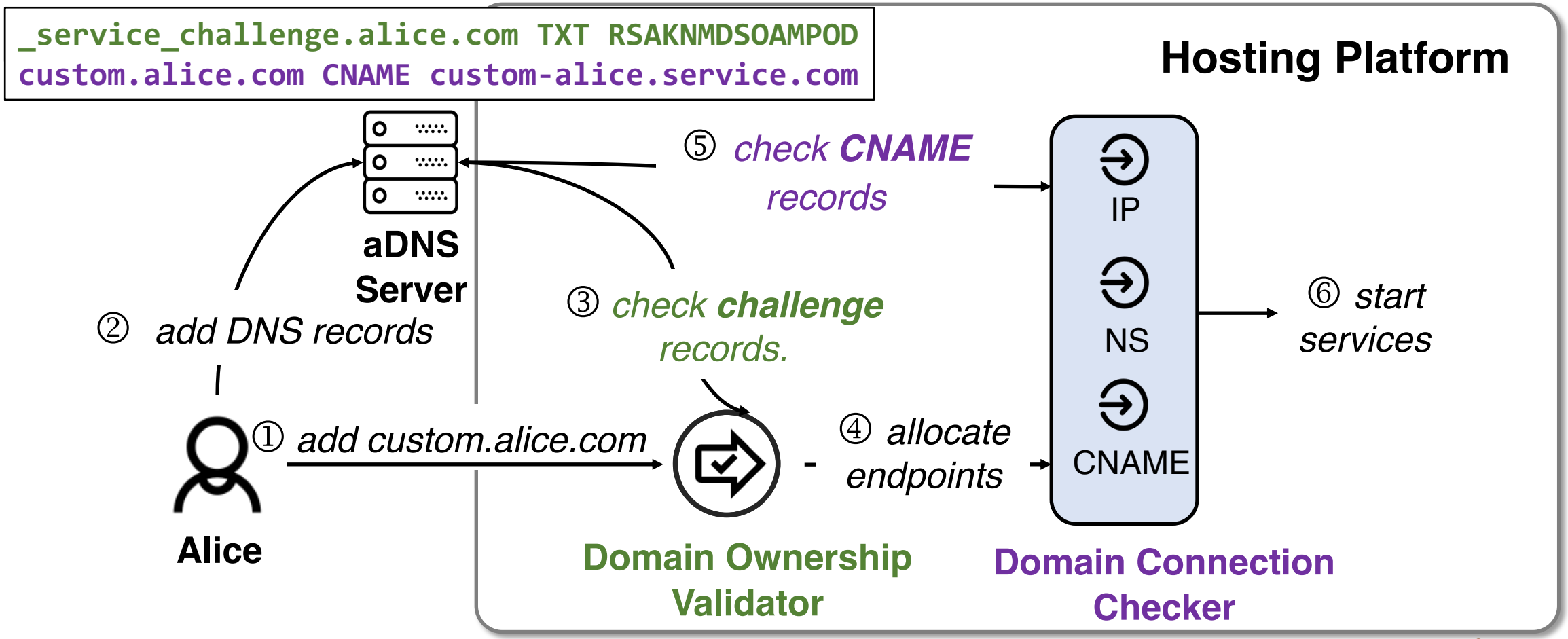


Narrowing down our vision to hosting-based domain takeover issues!

What is hosting-based domain takeover?

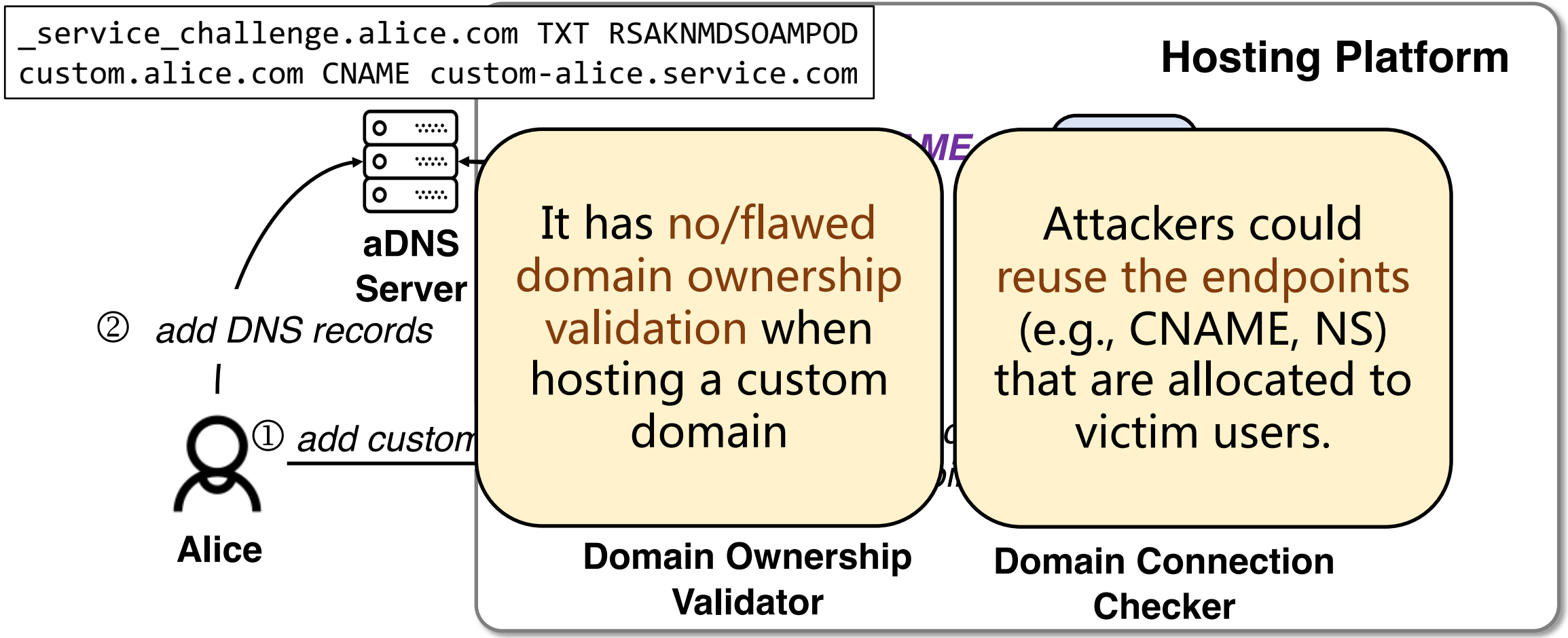
Public Hosting Service

➢Domain hosting procedures



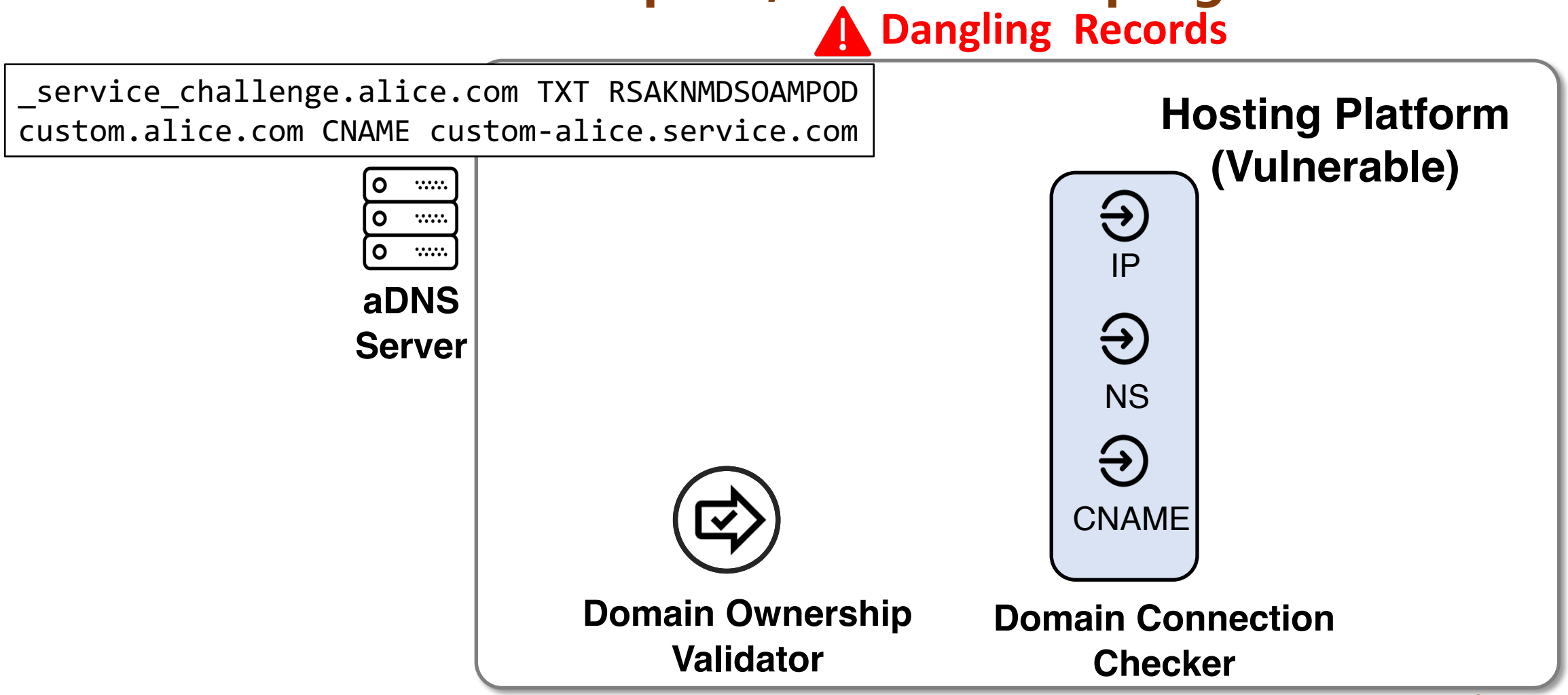
Vulnerable Hosting Service

➢ **However, a hosting service might be vulnerable if:**



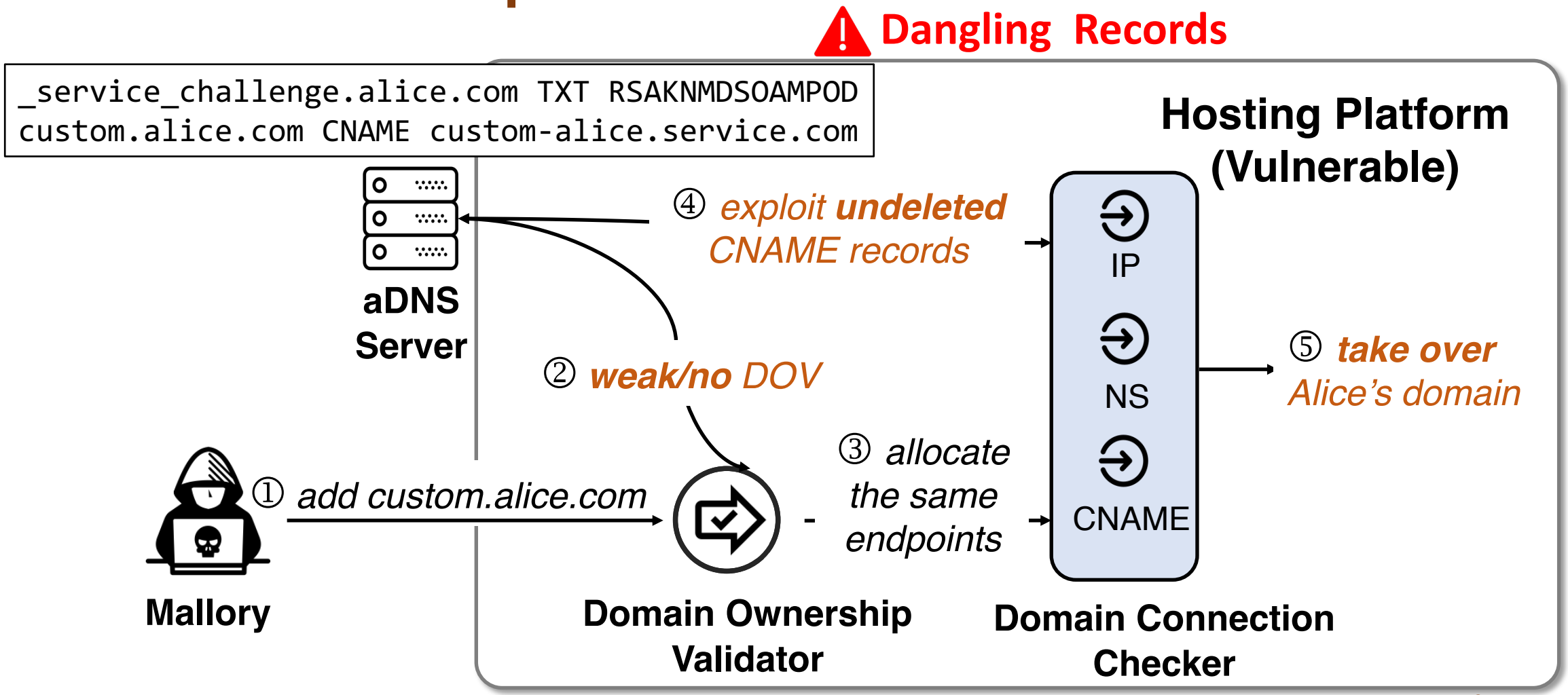
Hosting-based Domain Takeover

- When Alice's service expires, she doesn't purge RRs

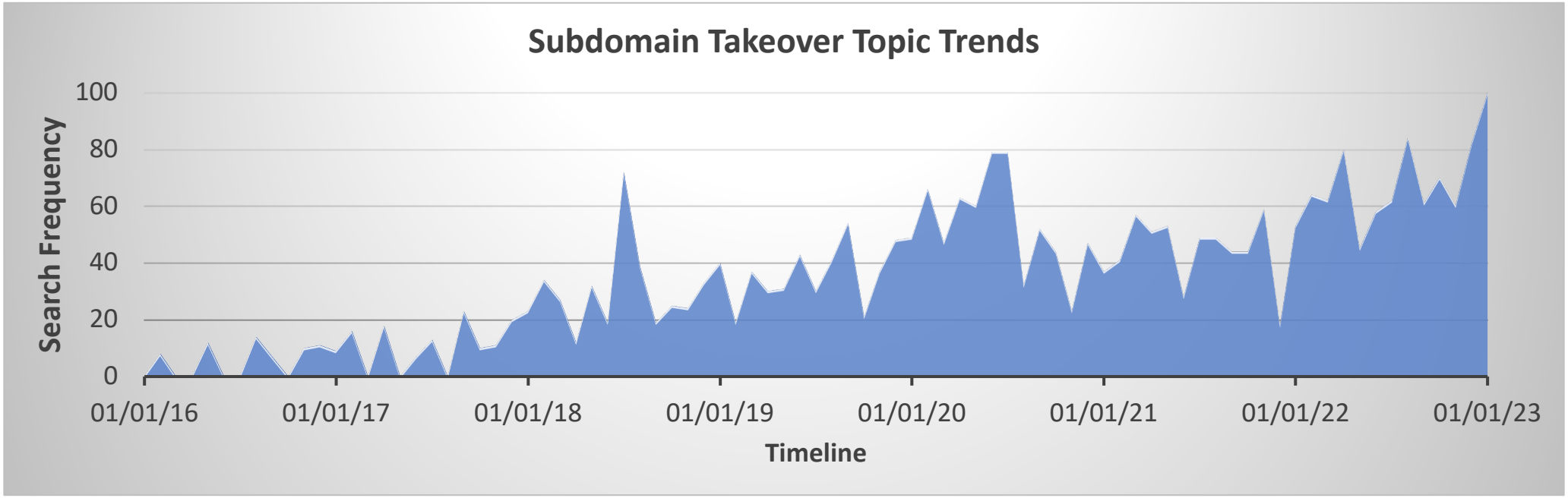


Hosting-based Domain Takeover

➢Domain takeover procedures



Why domain takeover occurs ceaselessly?



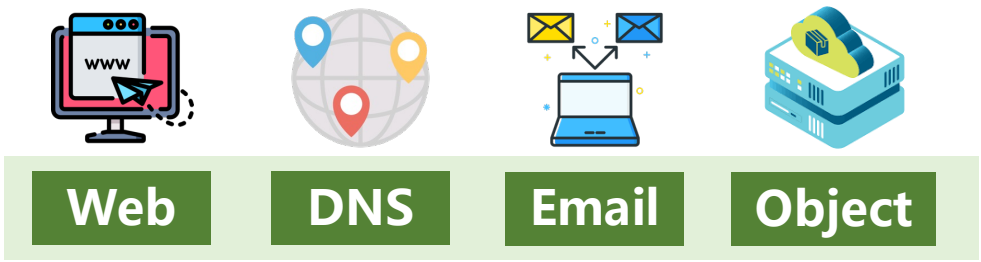
"Domain takeover incidents are still on the rise, increasing by 25% from 2020 to 2021."[1]

[1]https://blog.detectify.com/ 2022/03/22/subdomain-takeover-on-the-rise-detectify-research/.

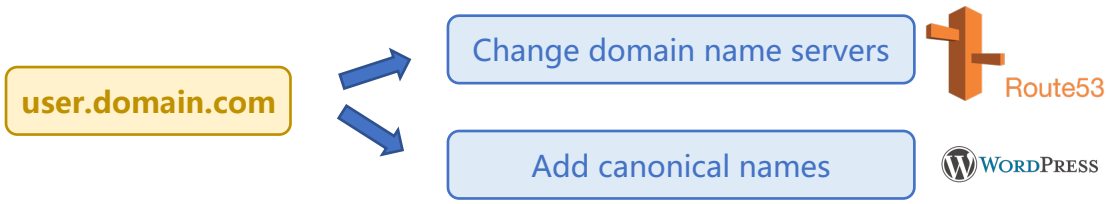
Motivation

1. A generic method for discovering third-party hosting services is needed

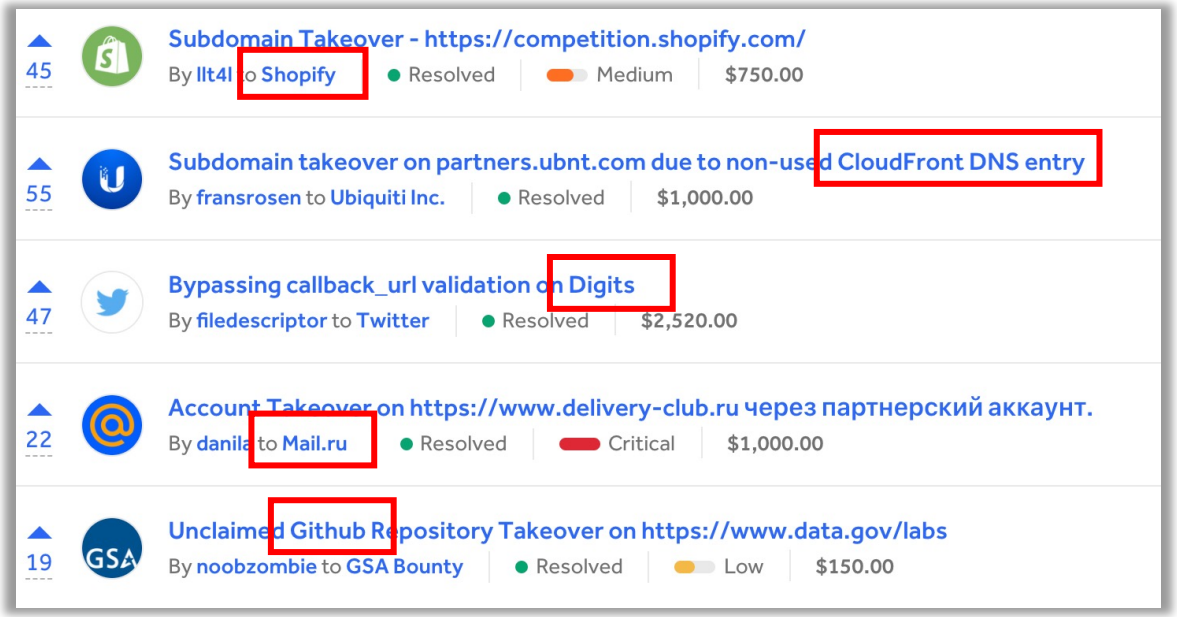
➢ **Various hosting service types**



➢ **Various domain hosting strategies**



➢ **Ad-hoc hacktivity reports on HackerOne**



Motivation

2. An efficient detection system is absent for quickly digging out vulnerable domains in the wild

- **Large companies have thousands of subdomains, with DNS chains changing frequently**

Subdomain	IP Address
enterpriseenrollment.microsoft.com	13.69.233.144
cdn.microsoft.com	23.52.255.32
sample.microsoft.com	65.55.69.140
enterpriseregistration.microsoft.com	20.190.137.40
event.microsoft.com	23.36.163.119
security.microsoft.com	52.109.88.132
mcp.microsoft.com	168.61.188.172
family.microsoft.com	23.196.249.123
signup.microsoft.com	13.107.237.45
jobs.microsoft.com	52.207.139.125
events.microsoft.com	20.49.104.24

How to timely detect vulnerable domains among them?

Previous work: active DNS resolution
[Daiping 2016, Eihal 2020 , Marco 2021]

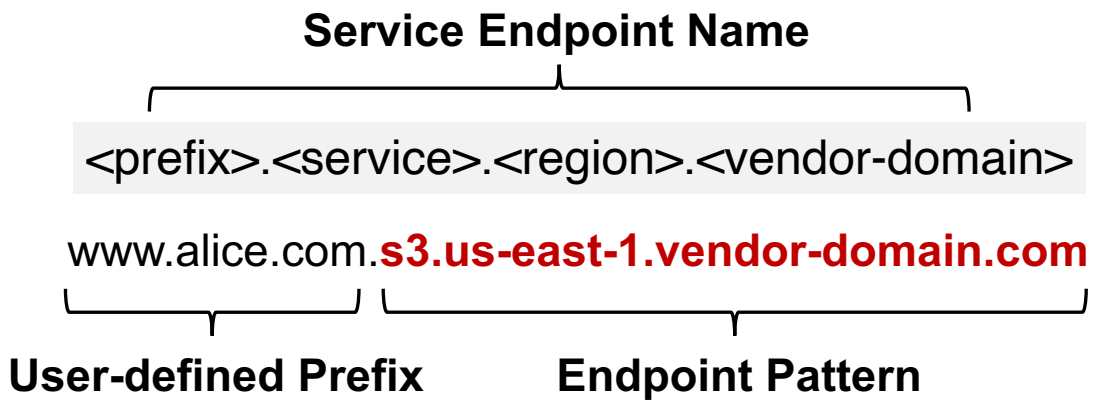
Can we discover more hosting services and detect vulnerable domains timely?

The domain characteristics of hosting services and the DNS chains of domains are logged in DNS traffic.

Empirical Observations

O1. Similar endpoint naming conventions

➢ Service Endpoint Patterns



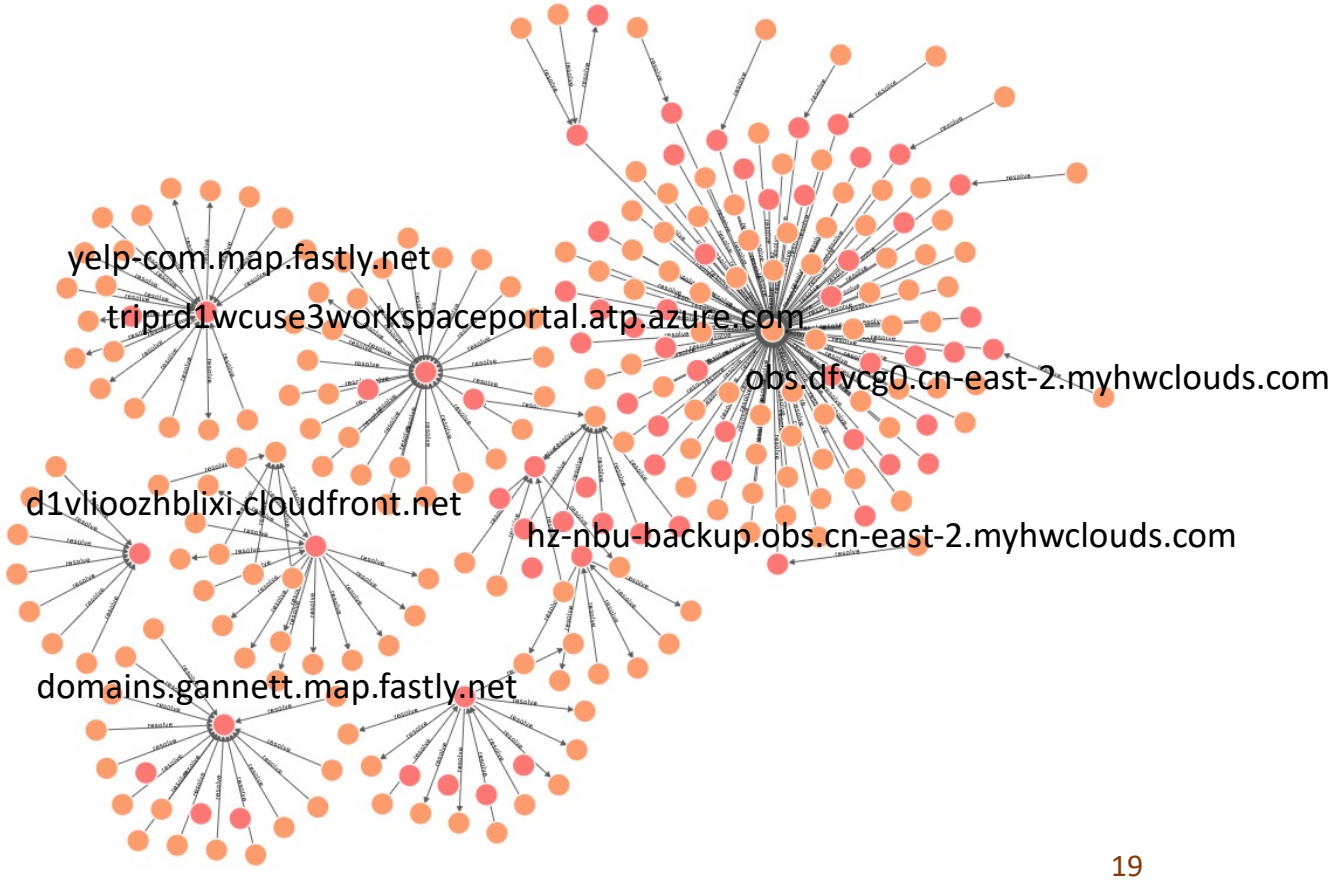
Empirical Observations

O2. High domain dependency number

- **One service apex domain may serve thousands of customers' domains**

```
custom1.com   CNAME   prefix1.service.com
custom2.com   CNAME   prefix2.service.com
                ...
customN.com   CNAME   prefixN.service.com
```

$$DN(\text{“}service.com\text{”}) = N$$



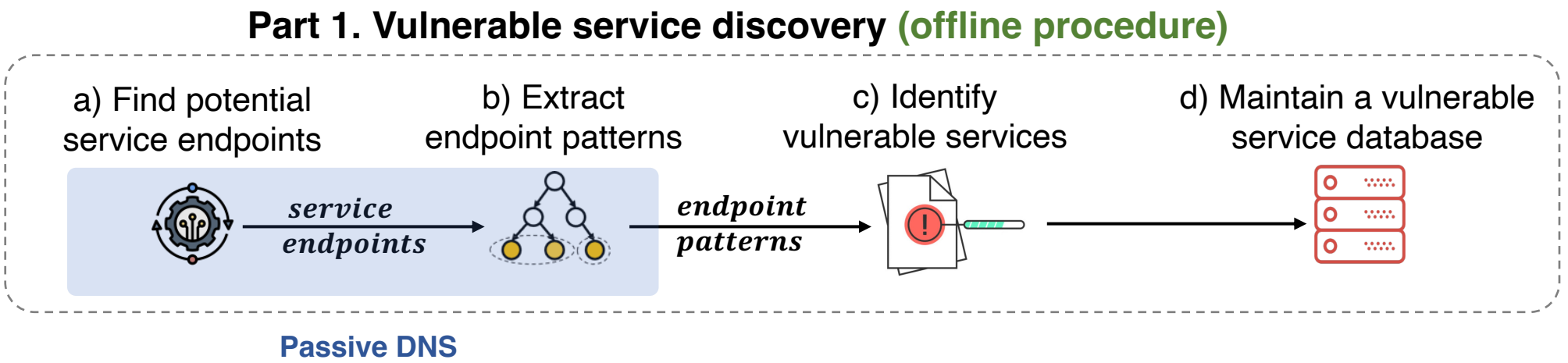
Our solution

Automate the approach to discovering services and vulnerable domains using passive DNS traffic.

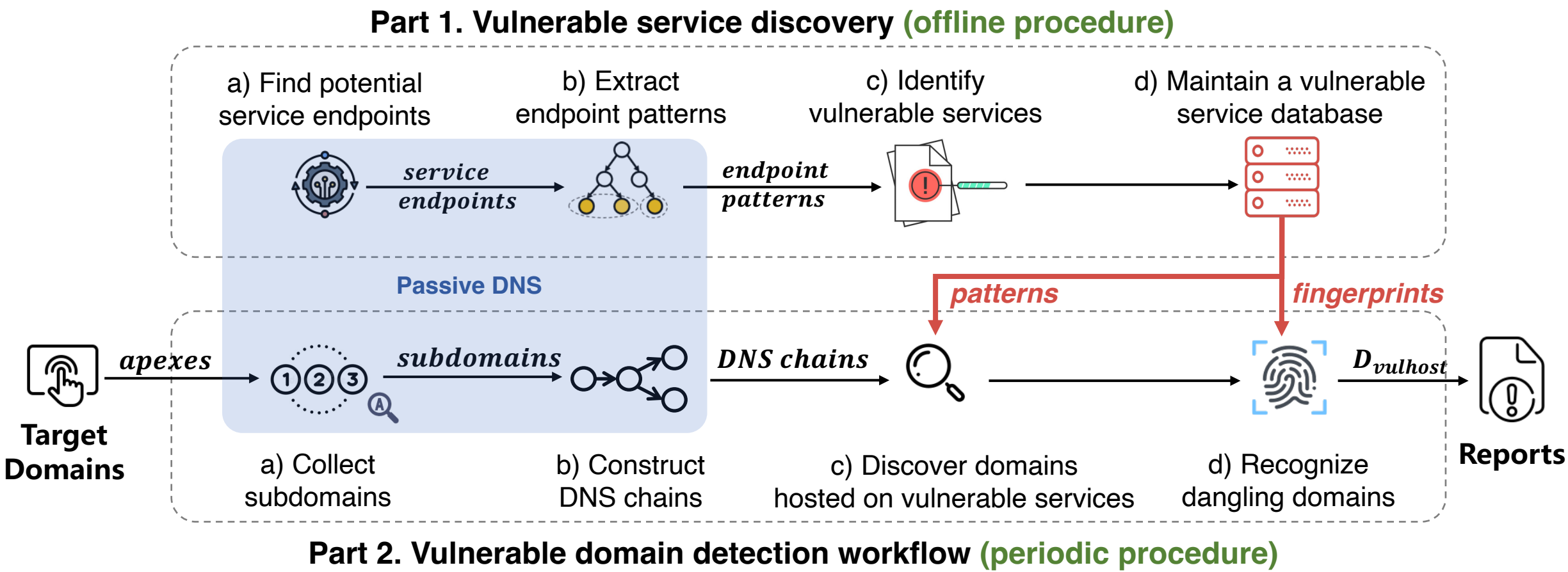
Our Tool: DareShark

- **A novel framework that can assist in:**
  - **Discovering vulnerable hosting services**
    - ↳ **Expand the detection scope**
  - **Detecting hosting-based vulnerable domains efficiently**
    - ↳ **Prevent potential security threats**

DareShark Workflow

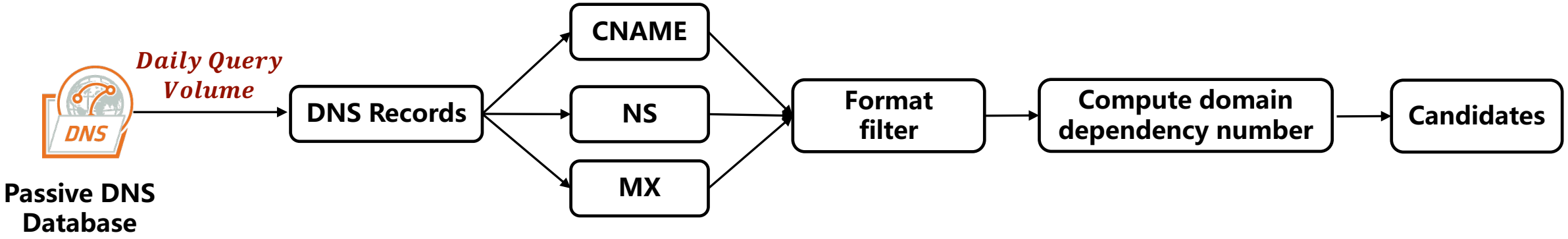


DareShark Workflow



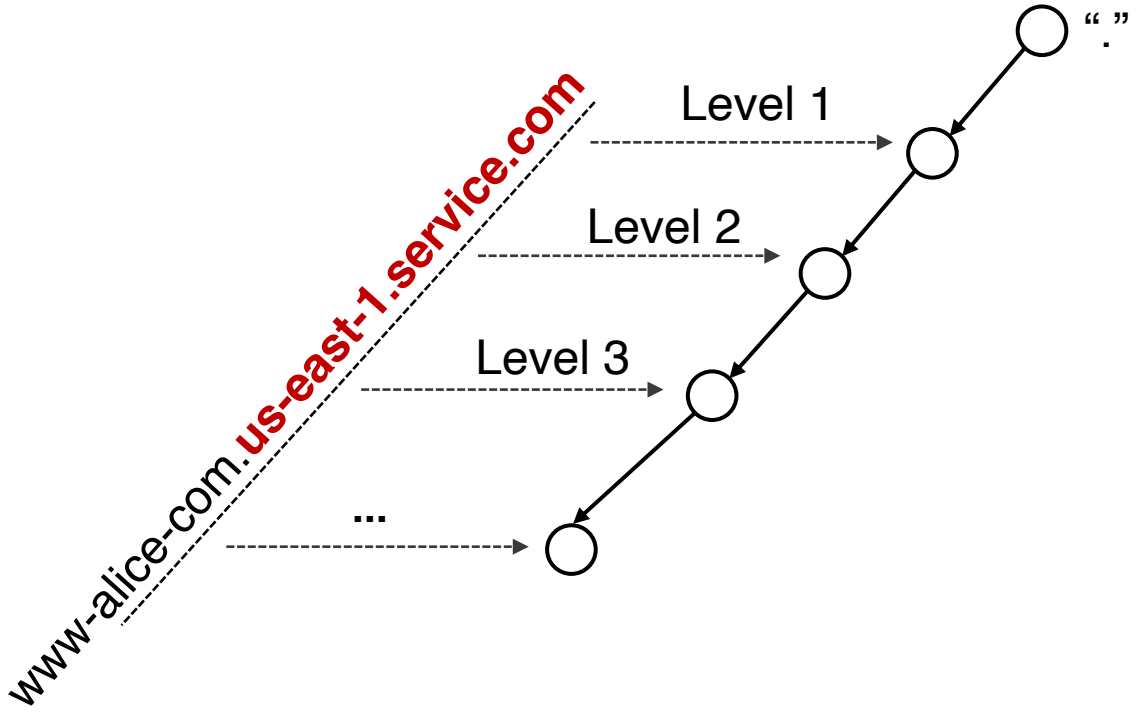
Part I: Discovering Vul. Services

- **Step 1: Finding service endpoint candidates**
  - Filtering endpoint domains by DNS resolution popularity and domain dependency.



Part I: Discovering Vul. Services

➢ **Step 2: Extracting endpoint patterns via a Domain Suffix Tree**



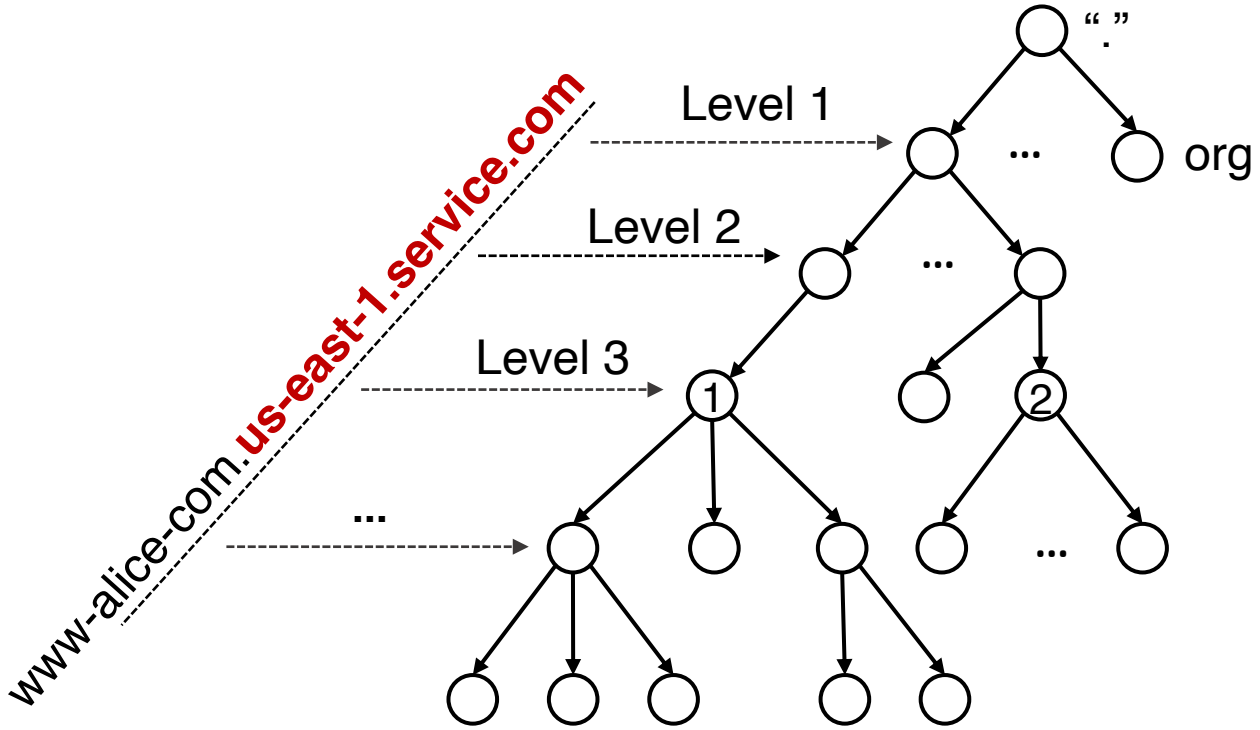
Domain Tree

Domain Tree Construction:

- The root is “.” , and children nodes are eTLDs, apex domains, apex+1, apex+2, and so on

Part I: Discovering Vul. Services

➢ Step 2: Extracting endpoint patterns via a Domain Suffix Tree



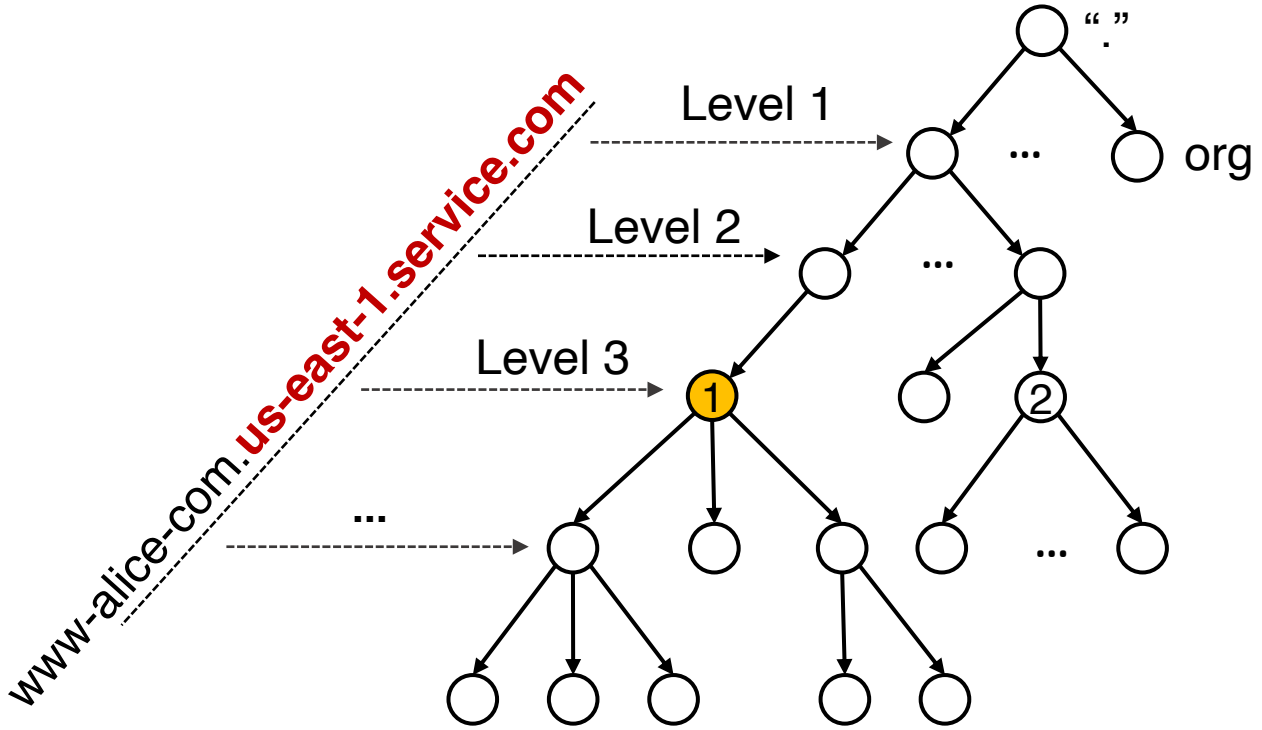
Domain Tree

Domain Tree Construction:

- The root is "." , and children nodes are eTLDs, apex domains, apex+1, apex+2, and so on

Part I: Discovering Vul. Services

➢ **Step 2: Extracting endpoint patterns via a Domain Suffix Tree**



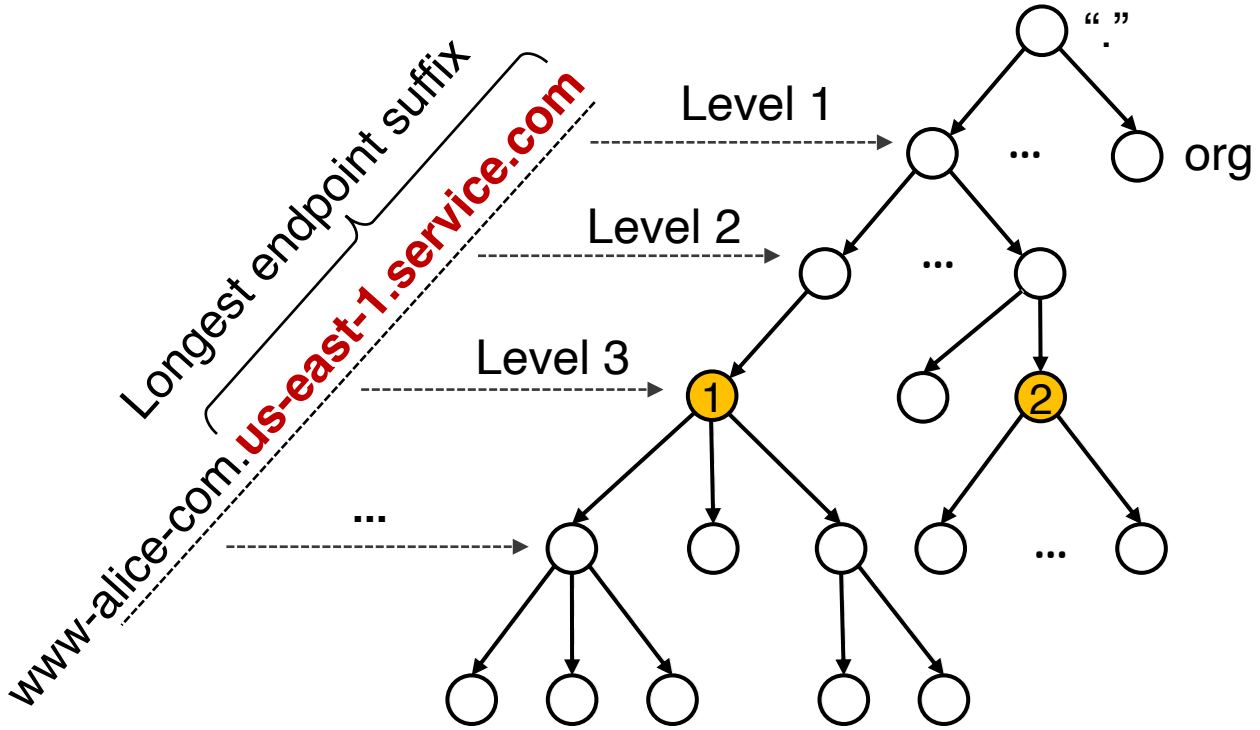
Domain Tree

Tree node attributes (Example of Node 1)

```
{
  "name"        : "us-east-1.service.com",
  "suffixLevel": 3,
  "DN"          : Dependency Number,
  "subCount"    : 3,
  "subList"     : ['a', 'b', 'c'],
  "subEntropy"  : Shannon entropy of subList
}
```

Part I: Discovering Vul. Services

➢ Step 2: Extracting endpoint patterns via a Domain Suffix Tree



Domain Suffix Tree (DST)

Domain Tree Pruning

- Prune the tree from the bottom up, by limiting number of hosted FQDNs, subCount, and subEntropy of each node

Part I: Discovering Vul. Services

- **Step 2: Extracting endpoint patterns via a Domain Suffix Tree**

  - **Service Endpoint Examples**

Services	Endpoint Names (endpoint patterns)
Aliyun OSS	alice.storage.com.oss-cn-hongkong.aliyuncs.com
Amazon S3	a.b.c.d.s3.us-east-1.amazonaws.com ab-cd.s3.dualstack.us-gov-west-1.amazonaws.com
GitHub	abcd.github.io

Part I: Discovering Vul. Services

- **Step 3: Identifying services and checking service vulnerabilities**
  - **Narrow down the candidate list of endpoint patterns**

    e.g., remove highly randomized endpoint domains

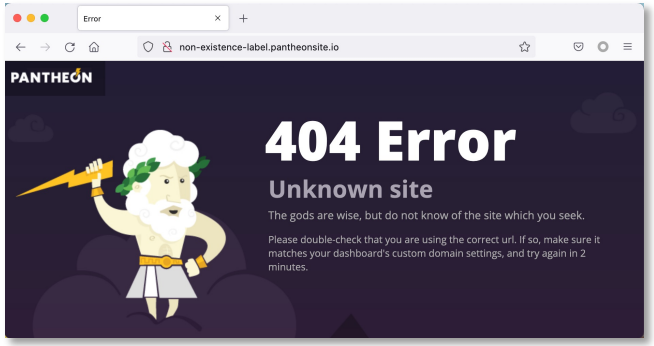
  - **Map endpoint patterns to services**

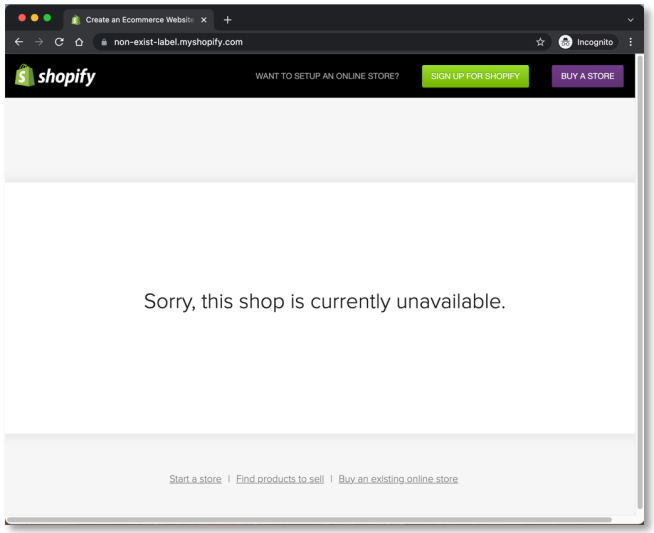
    e.g., access homepages, dig through search engines

  - **Check vulnerabilities in domain connection and domain ownership validation**

Part I: Discovering Vul. Services

➢ Step 4: Maintaining a database for vulnerable services





Vulnerable Service Fingerprints

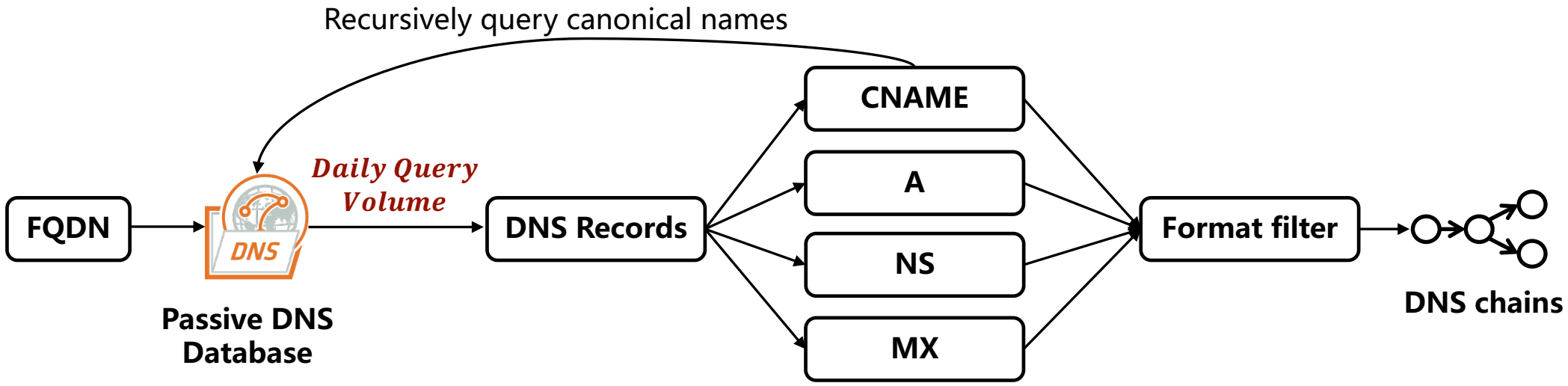
Type	Response Example	# Banner	# Service	# Vendor
HTTP Response		**106**	**59**	**48**
Header	`"404 Unknown site"`	14	13	10
Body	`"NoSuchBucket"`	92	52	47
DNS Answer		**4**	**13**	**9**
NX-CNAME[1]	`status:NXDOMAIN`	1	11	7
Default Rdata[2]	`127.0.0.1` `nx.aicdn.com`	3	2	2
Total		**110**	**64**	**51**

Part II: Detecting Hosting-based Dares

➢ Collecting subdomain names from passive DNS logs

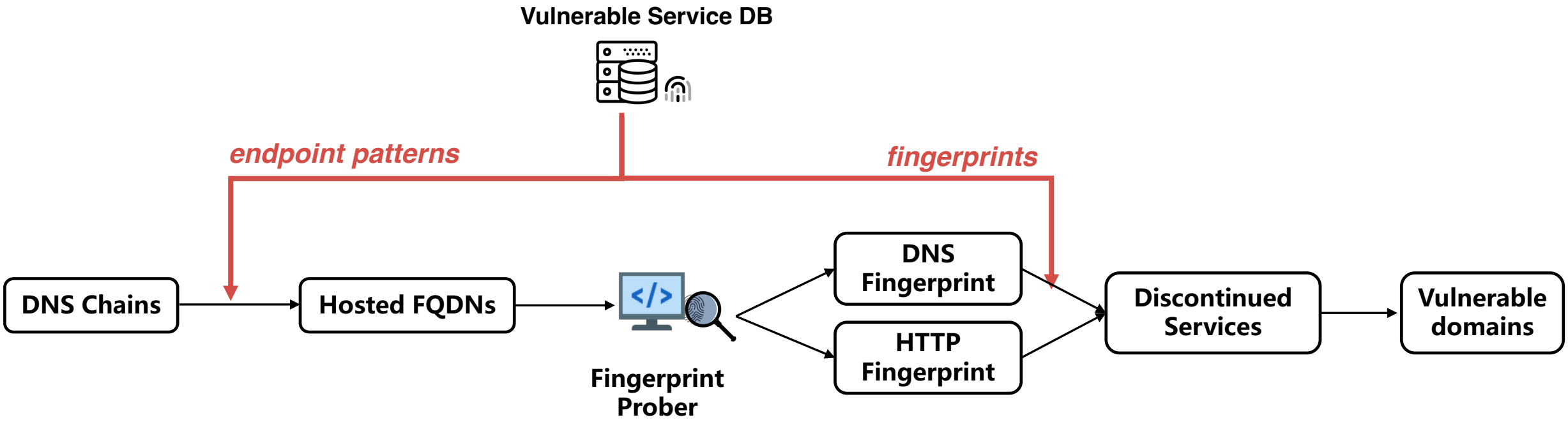
- ➢ Legal format **[RFC 1034] Domain Names - Concepts And Facilities**
- ➢ Filter disposable domains created on demand
  e.g., scanning, convey "one-time signals" $Total\ Query\ Volume > 100$

➢ Reconstructing domain dependencies (DNS chains)



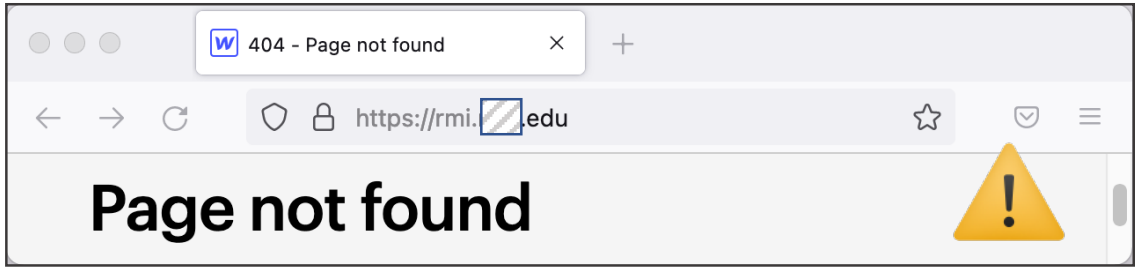
Part II: Detecting Hosting-based Dares

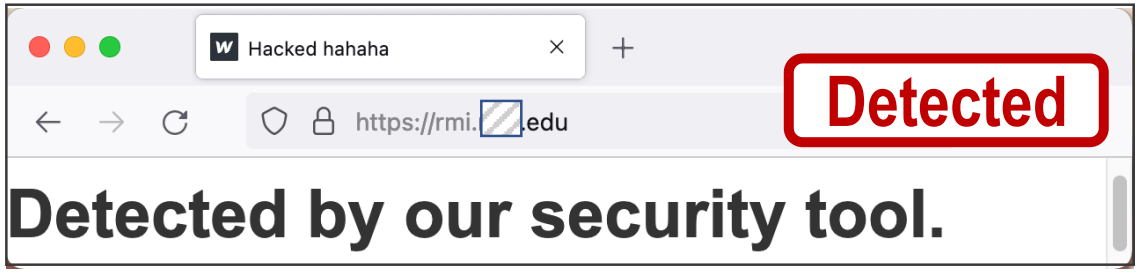
- Probing hosted domains to inspect service status



Part II: Detecting Hosting-based Dares

- **Probing hosted domains to inspect service status**



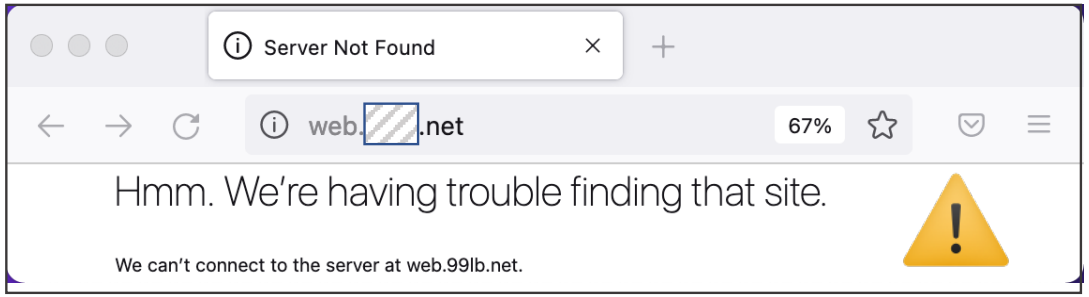


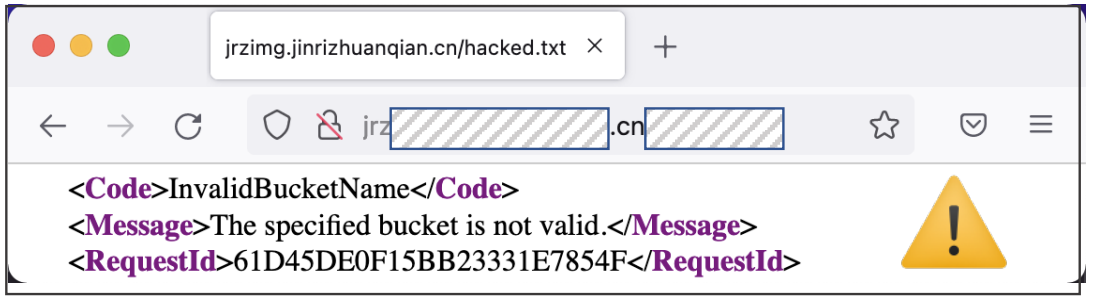
(1) Webflow
rmi.xxxx.edu

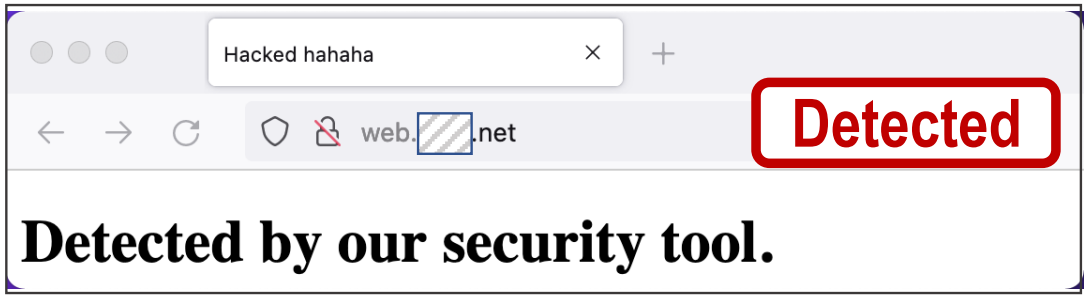
(2) Fastly
mrcd.xxxxxxxxx.vip

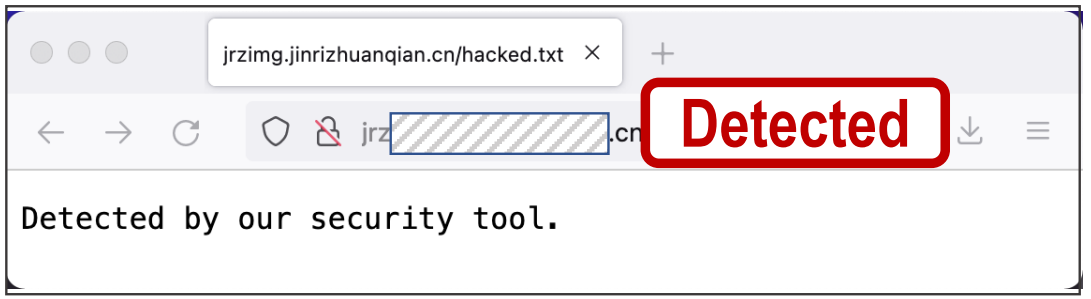
Part II: Detecting Hosting-based Dares

- **Probing hosted domains to inspect service status**









(3) Cloudflare
web.xxxx.net

(4) Alibaba Cloud
rrzxxx.xxxxxxxxxxxxx.cn

DareShark Deployment

- **Passive DNS dataset**
  - DNS response data from public DNS resolvers for **114DNS**, the largest DNS provider in China
  - **600B** DNS queries per day, covering **99.9%** of Tranco Top 1M domains
  - DNS queries originate from telecom companies (e.g., China Telecom), research institutions (e.g., MIT and NUS), and large providers (e.g., Alibaba and Google)

What did we find for hosting services?

- The current practice of hosting services is in a mass, resulting in various types of service vulnerable to domain takeover.

Vulnerable Hosting Services

- **65 services vulnerable to domain takeover threats.**
- **Vulnerable services comprise a variety of service types.**

Categories	# Vendor		# Endpoint Patterns		# Services	
	All	Vulnerable	All	Vulnerable	All	Vulnerable
Cloud Storage	7	7	130	118	12	9
CDN	25	7	247	31	44	8
Website Builder	51	40	156	105	60	44
Others	27	4	462	4	49	4
Newly Discovered	55	19	920	183	125	34
All	88	**52**	995	258	165	**65**

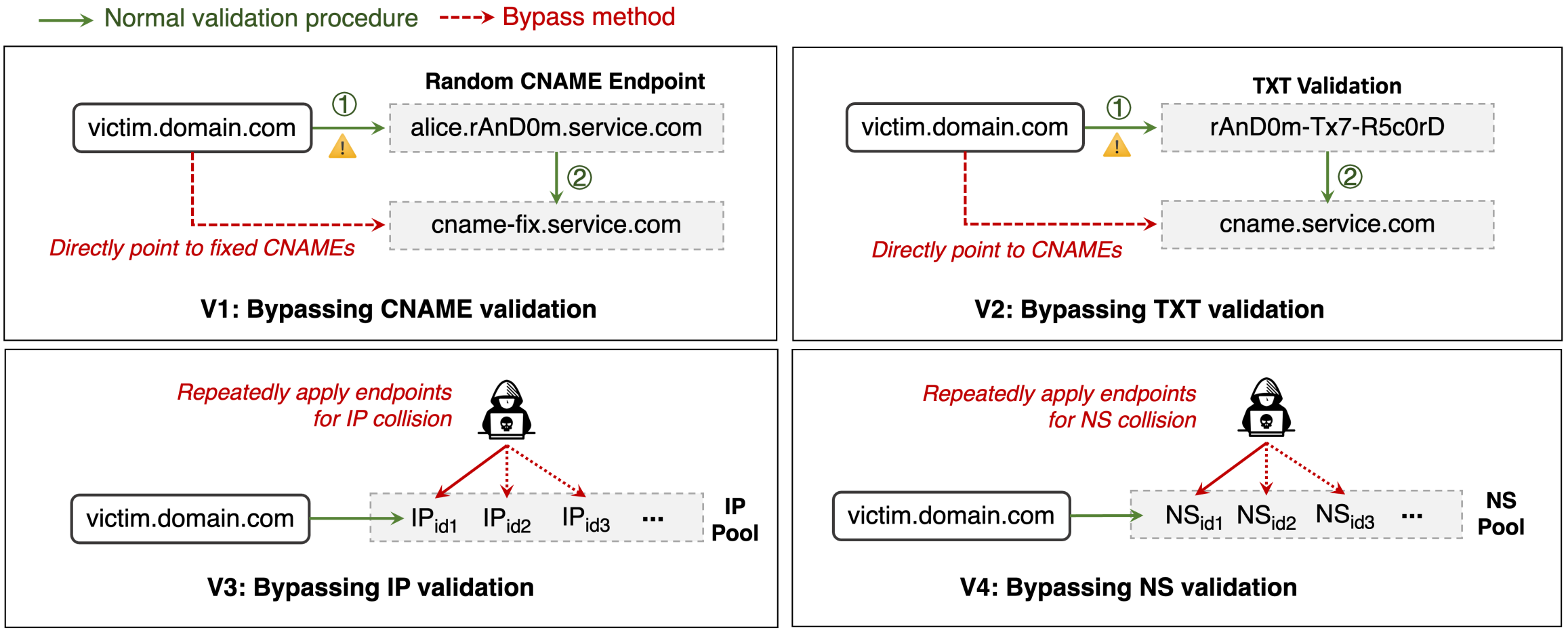
Vulnerable Hosting Services

- **7/9 domain connecting methods are exploitable**

Method	Type	Connect a custom domain to...	# Services	Exploitable
CNAME	M1	Fixed canonical domains	12	●
	M2	Any canonical domains customized by any users	70	●
	M3	New canonical domains customized by new users	12	○
	M4	The canonical domains allocated from a candidate pool	5	◐
	M5	Canonical domains containing newly generated random labels	47	○
NS	M6	Fixed nameservers	1	●
	M7	The nameservers allocated from a candidate pool	5	◐
IP	M8	Fixed IPs	8	●
	M9	The IPs allocated from a candidate pool	4	◐

Vulnerable Hosting Services

➢ 4 new threat models that can bypass flawed DOV



Vulnerable Hosting Services

- **Top 20 vendors with 70% market share are vulnerable**

Category	Vendor	Service	Connecting method*	Vulnerable DOV				# $D_{vulhost}$
				V1	V2	V3	V4	
Cloud Strorage	Alibaba	OSS	M_2	✓	-	-	-	86
	Amazon	Elasticbeanstalk	M_2	✓	-	-	-	192
	Huawei	OBS	M_2	✓	-	-	-	178
	JD.COM	OBS	M_2	✓	-	-	-	51
CDN	Baidu	BOS, CDN, BCH	M_2	✓	-	-	-	1,309
	Cloudflare	CDN	M_2, M_7	✓	✓	-	-	543
	Fastly	CDN	M_2	✓	-	-	-	54
	Tencent	CDN	M_2	✓	-	-	-	119
Website Builder	Duda	Website Builder	M_1, M_8	✓	-	✓	-	10
	Jimdo	Website Builder	M_1, M_7, M_8	✓	-	✓	✓	5
	Medium	Blog	M_8	-	-	✓	-	3
	Netlify	Website Builder	M_1, M_2, M_7, M_8	✓	-	✓	✓	21
	Shopify	Website Builder	M_1, M_8	✓	-	✓	-	34
	Tilda	Website Builder	M_9	-	-	✓	-	4
	Tumblr	Blog	M_1, M_8	✓	-	✓	-	11
	Unbounce	Website Builder	M_5	✓	-	-	-	212
	Webflow	Website Builder	M_1, M_8	✓	-	✓	-	30
	Wix	Website Builder	M_4, M_7	✓	-	-	✓	26
	Wordpress	Website Builder	M_3, M_6, M_8	✗	-	✓	✓	27
	WP Engine	Website Builder	M_3, M_9	✗	-	✓	-	12

What did we find for domain takeover?

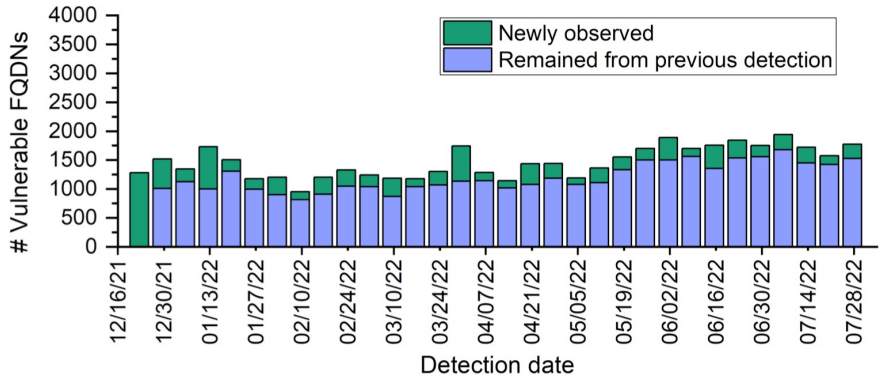
- Hosting-based domain takeover threats are still prevalent.

Measurement and Findings

- **Detection target domains**
  - **Tranco Top 1M apex domains +9,808 .edu and 7,198 .gov apexes**
  - **We collect 11,446,359 subdomains from PDNS for all apexes.**
- **Longitudinal and periodic measurement**
  - **101 rounds (Dec. 16, 2021 – Jul. 28, 2022)**
  - **~1 day/round**

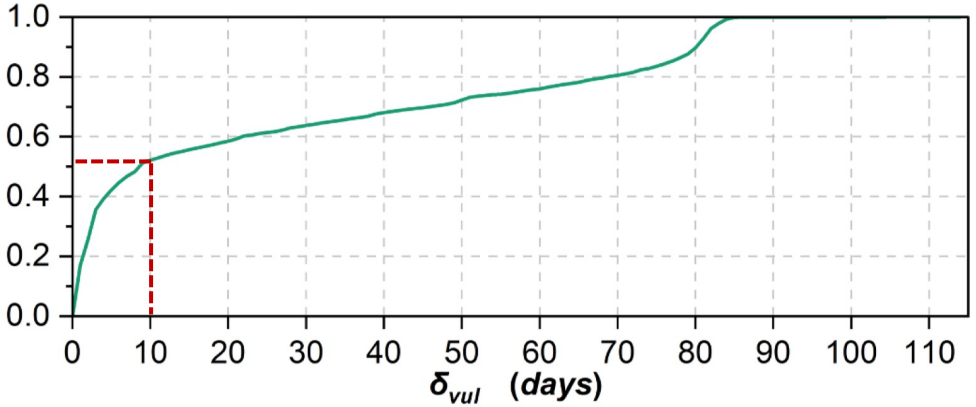
Measurement and Findings

- **114,063 (1.0%) FQDNs have been hosted on vulnerable services**
- **10,351 FQDNs are vulnerable, covering 2,096 apex domains**
  - Reputable universities (e.g., Stanford and Rice)
  - Famous companies (e.g., Baidu, Huawei, and Marriott).
- **Hosting-based domain takeover appears frequently and long-lasting**



Weekly cumulative detection results.

270 new vulnerable domains emerge per week.



Distribution of vulnerable days

Over 50% remain vulnerable for over 10 days.

Conclusion

- **DareShark: A novel and effective detection framework**
  - High efficiency and coverage
- **Comprehensive measurements**
  - 7-month longitudinal measurement on Tranco 1M apexes' subdomains
  - Detect 10,351 vulnerable domains (8x more than previous study)
- **Systematic service inspection and threat analysis**
  - Discover 65 vulnerable services and new security flaws
  - Receive vulnerability confirmation from 10 vendors, and provide solutions

Thanks for listening!

Any question?

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