

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

June 22th, 2023



Domain Takeover (DT)

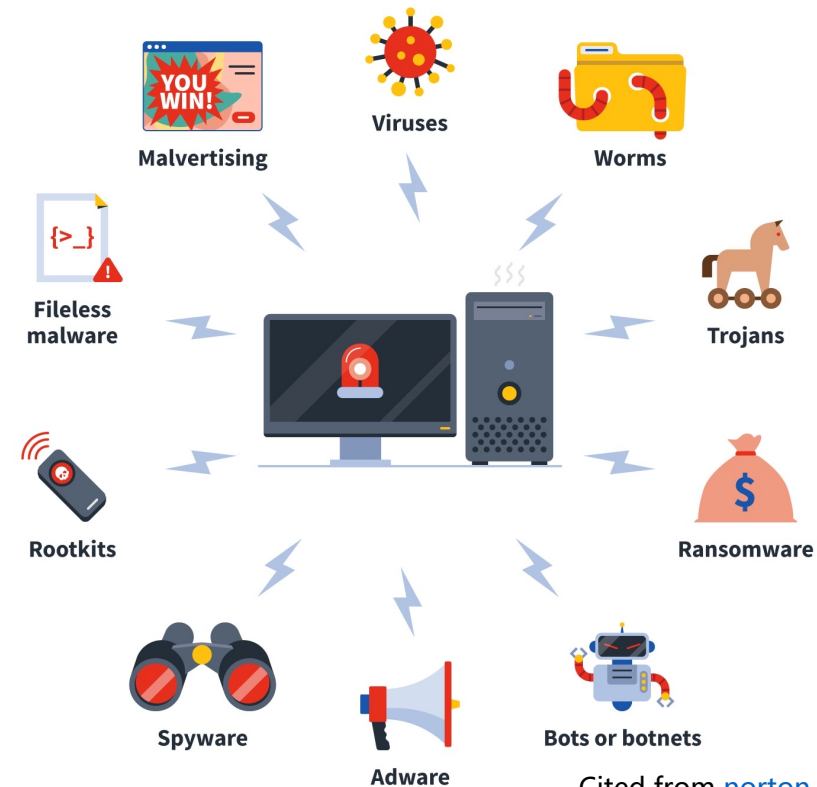
- Adversaries could exploit the domain names outside of their authority for malicious activities
 - Botnet, phishing, malware distribution, etc.



Cited from bleepingcomputer.com



Cited from scmp.com

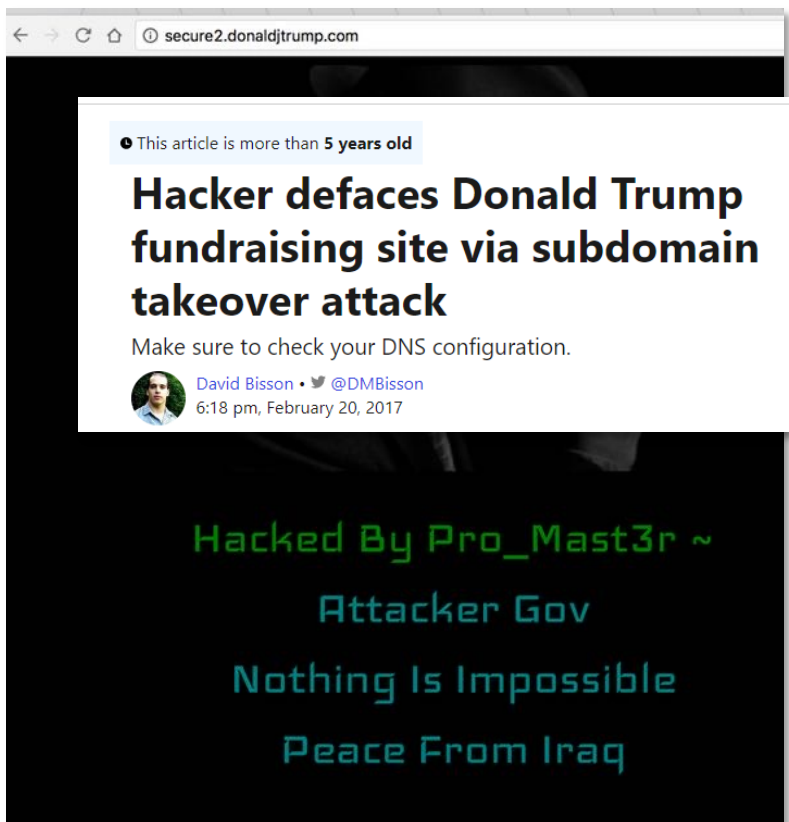


Cited from norton.com

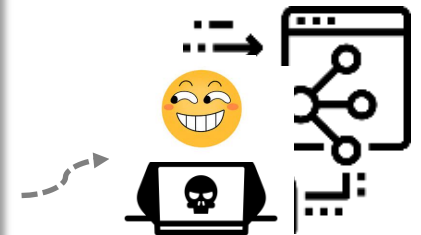
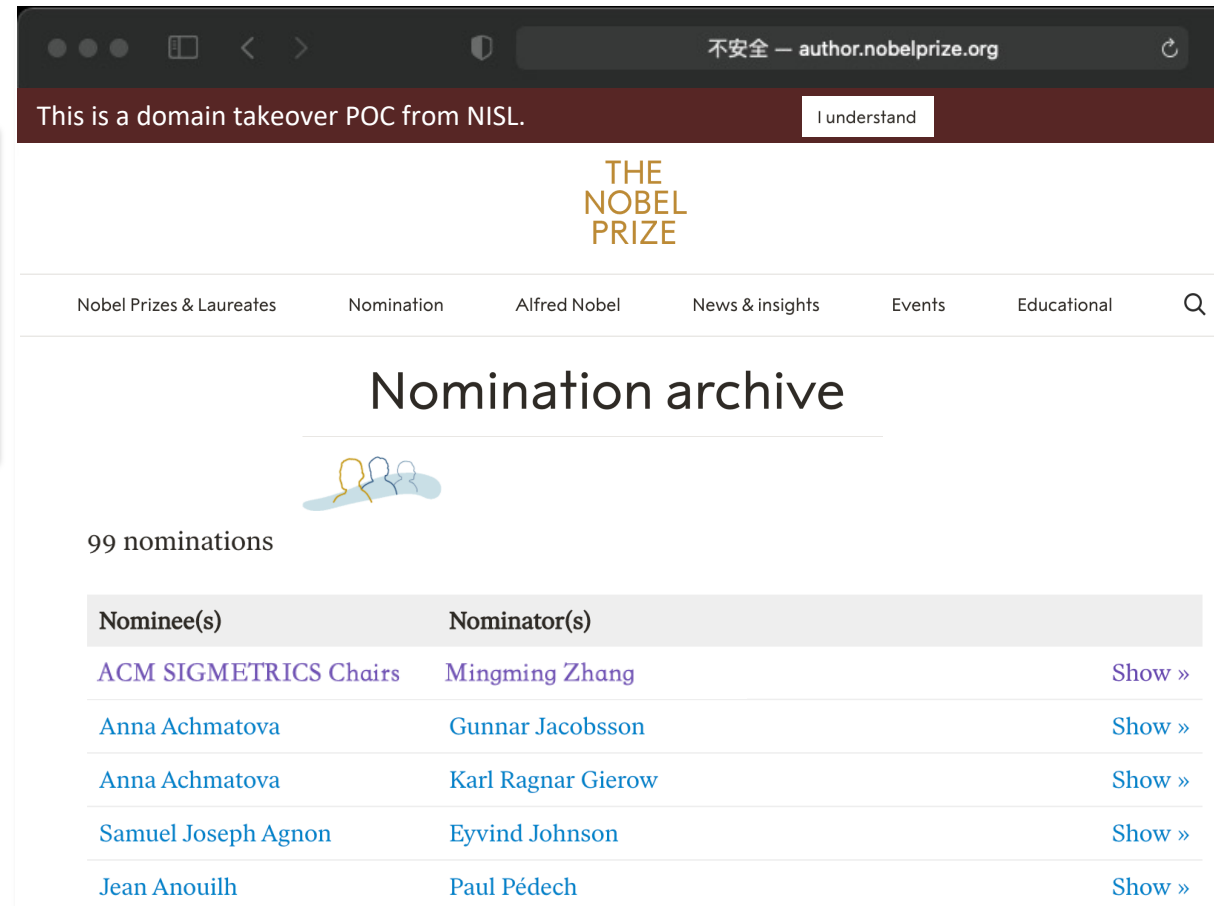
Seeing is Believing?

Perhaps Not ! The accessed domain might be controlled by attackers.

secure2.donaldjtrump.com

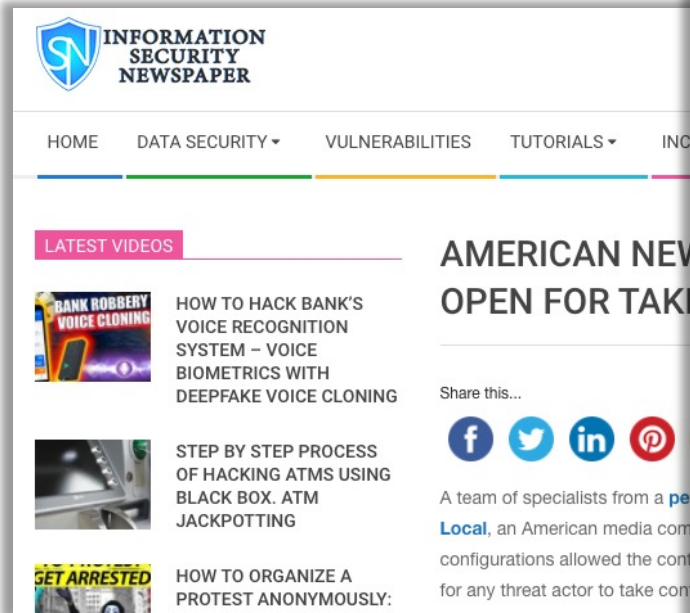


author.nobelprize.org



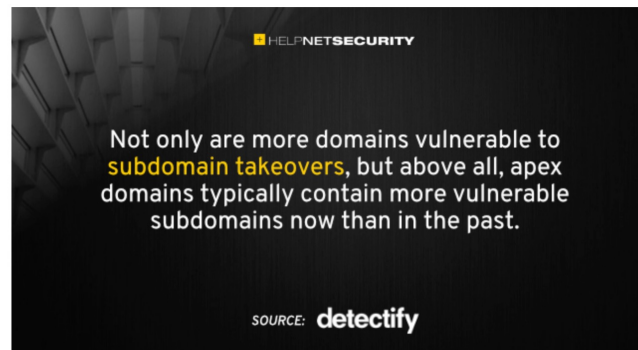
DT Threats are constantly emerging!

- **Domain takeover^[1] may occur when a domain is pointed to**
 - (1) expired domains,
 - (2) discontinued hosting services (e.g., CDN, Web Hosting),
 - (3) deprovisioned cloud instances (e.g., VPS)
- **Many domain takeover incidents appear in recent years**

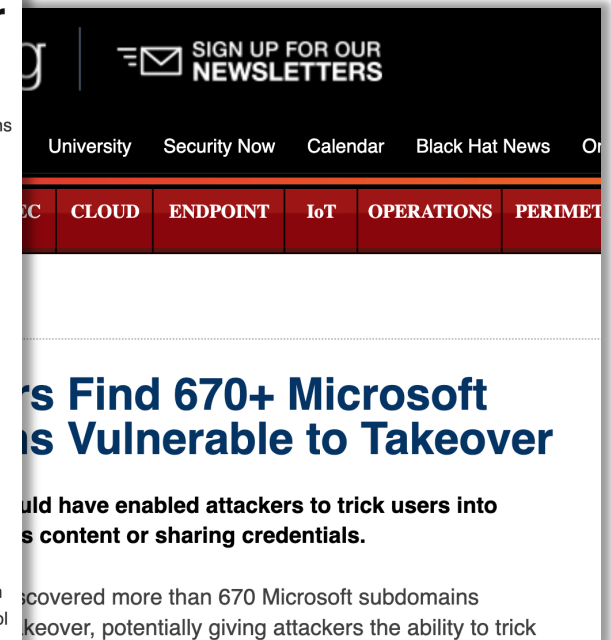


Subdomain takeover attacks on the rise and harder to monitor

A research from Detectify found that subdomain takeovers are on the rise but are also getting harder to monitor as domains now seem to have more vulnerabilities in them.



In 2021, Detectify detected 25% more vulnerabilities in its customers' web assets compared to 2020 with twice the median number of vulnerabilities per domain, demonstrating the outsized impact an external attack surface monitoring (EASM) tool can have on an organization's cybersecurity programme.



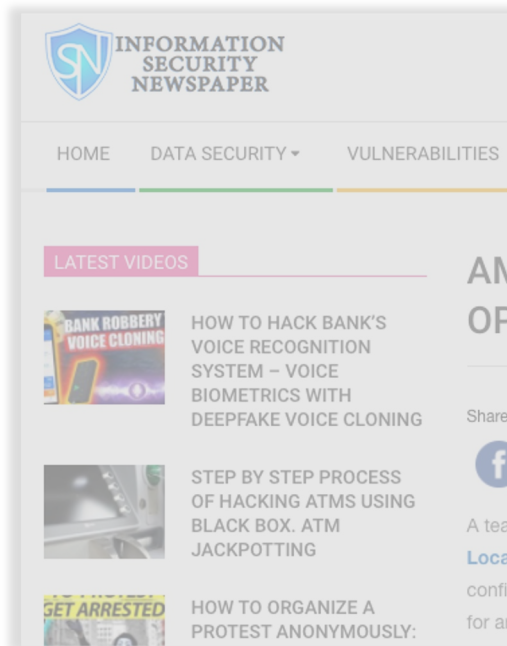
[1] All Your DNS Records Point to Us [CCS]

Web Hosting: Key Avenue for Domain Takeover

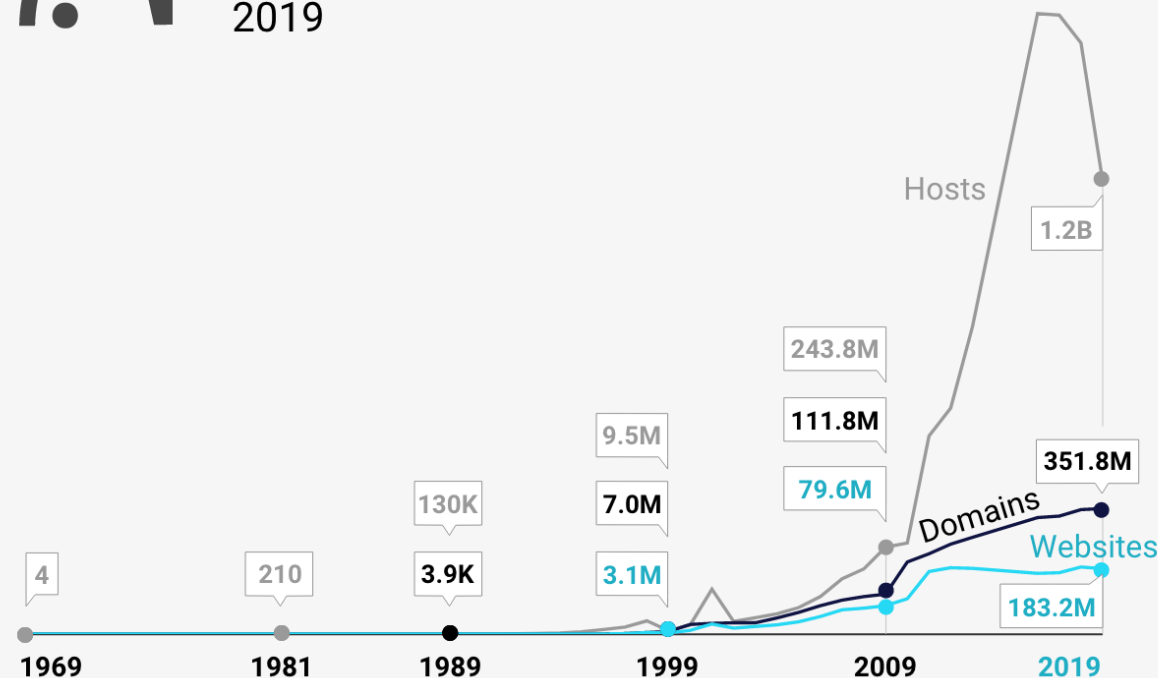
➤ Many domains

Web Hosting Statistics 2023: State of The Website Hosting Industry

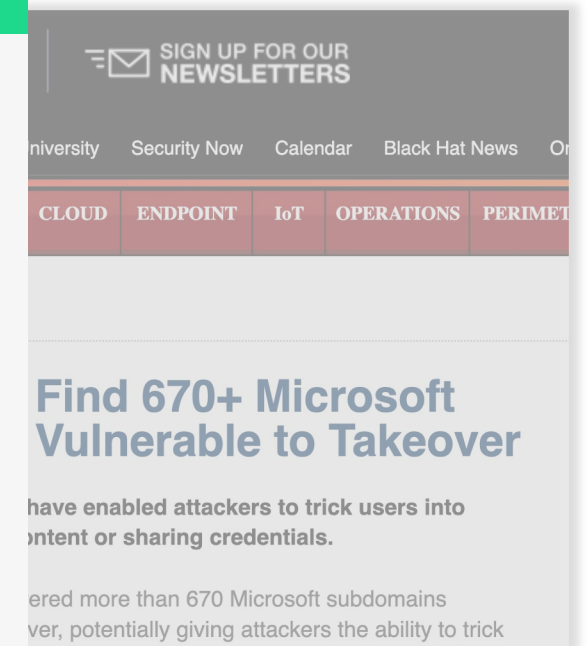
Recent years



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



Source: netvalley .com, firstsitefuide.com



Our Research Scope

➤ Many domain takeover incidents occur in recent years

Web Hosting Statistics 2023: State of The Website Hosting Industry

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

A team of specialists from a [pentesting course](#) found a vulnerability on the website of [CBS Local](#), an American media company. In addition to the flaw, the site's weak security configurations allowed the content of 3 subdomains belonging to the company to be exposed for any threat actor to take control over them.



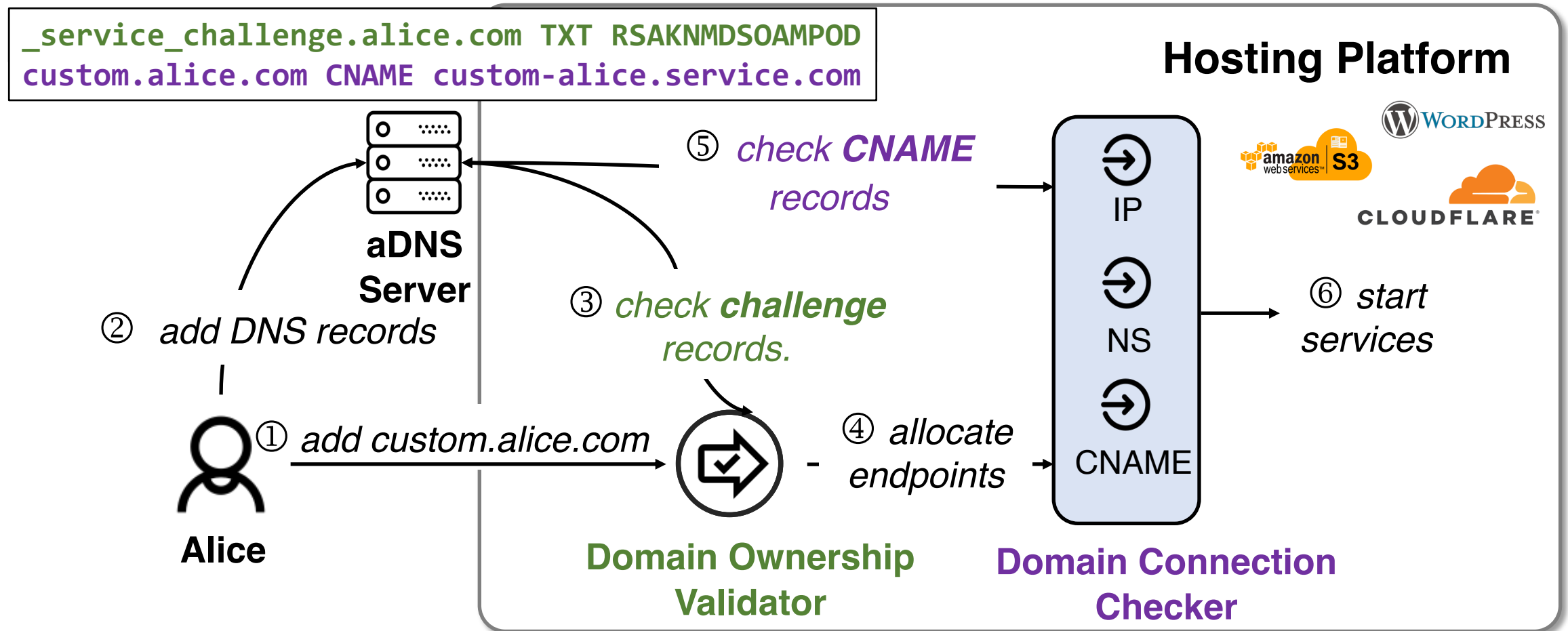
Source: [netvalley.com](#), [firstsiteguide.com](#)

What is hosting-based domain takeover?

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

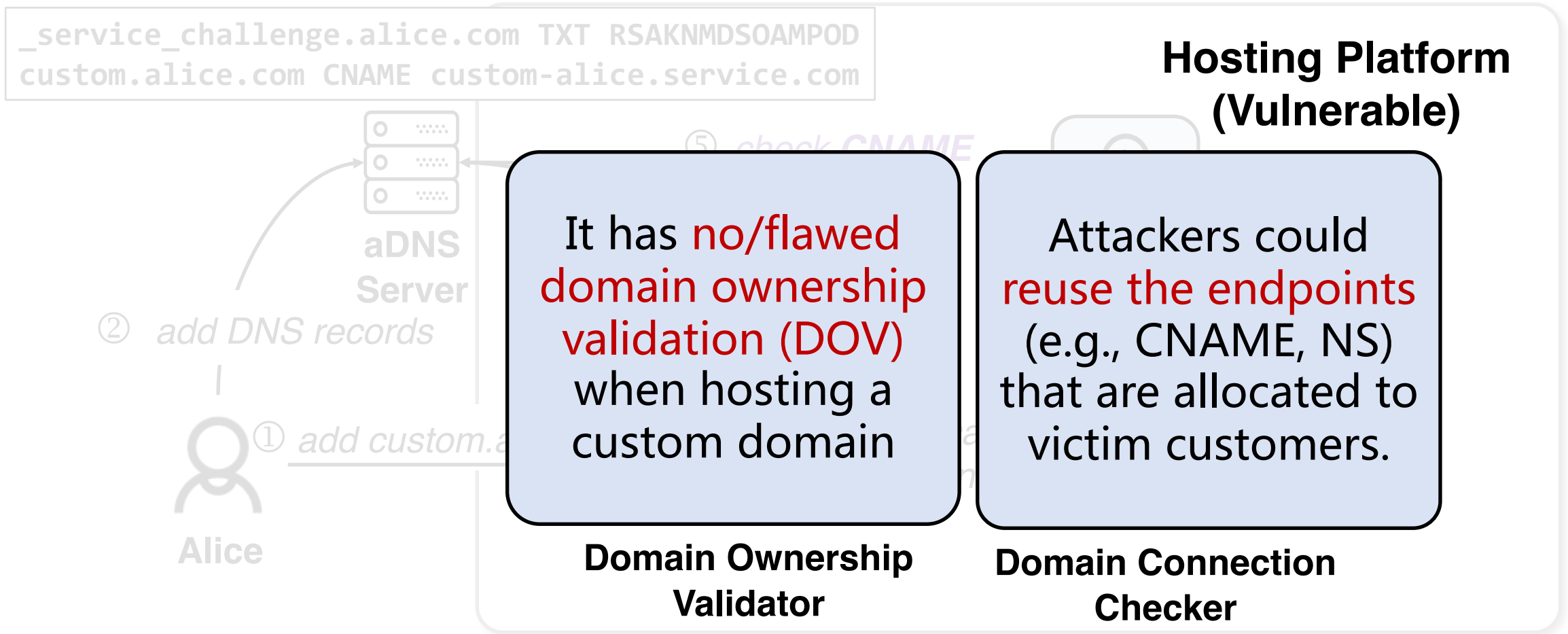
Public Hosting Service

- Customers configure domains to hosting services (e.g., CDN)



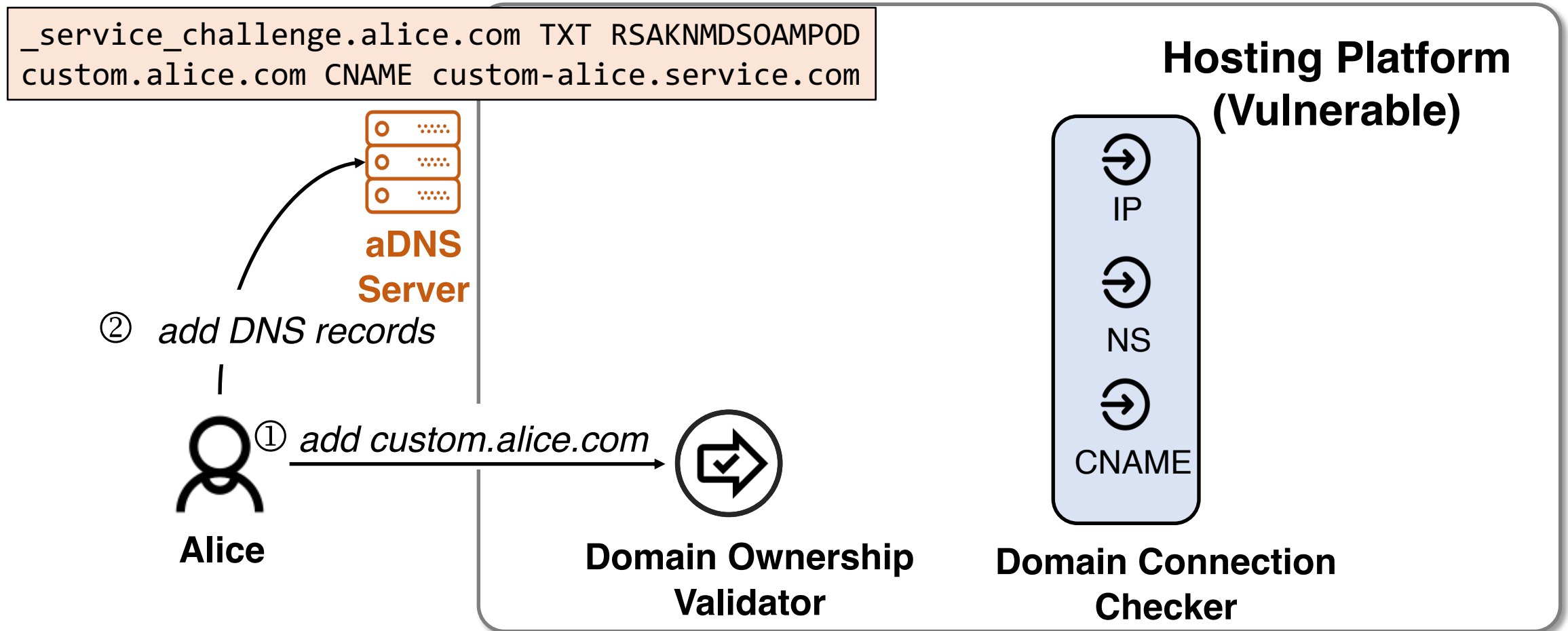
Vulnerable Hosting Services

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



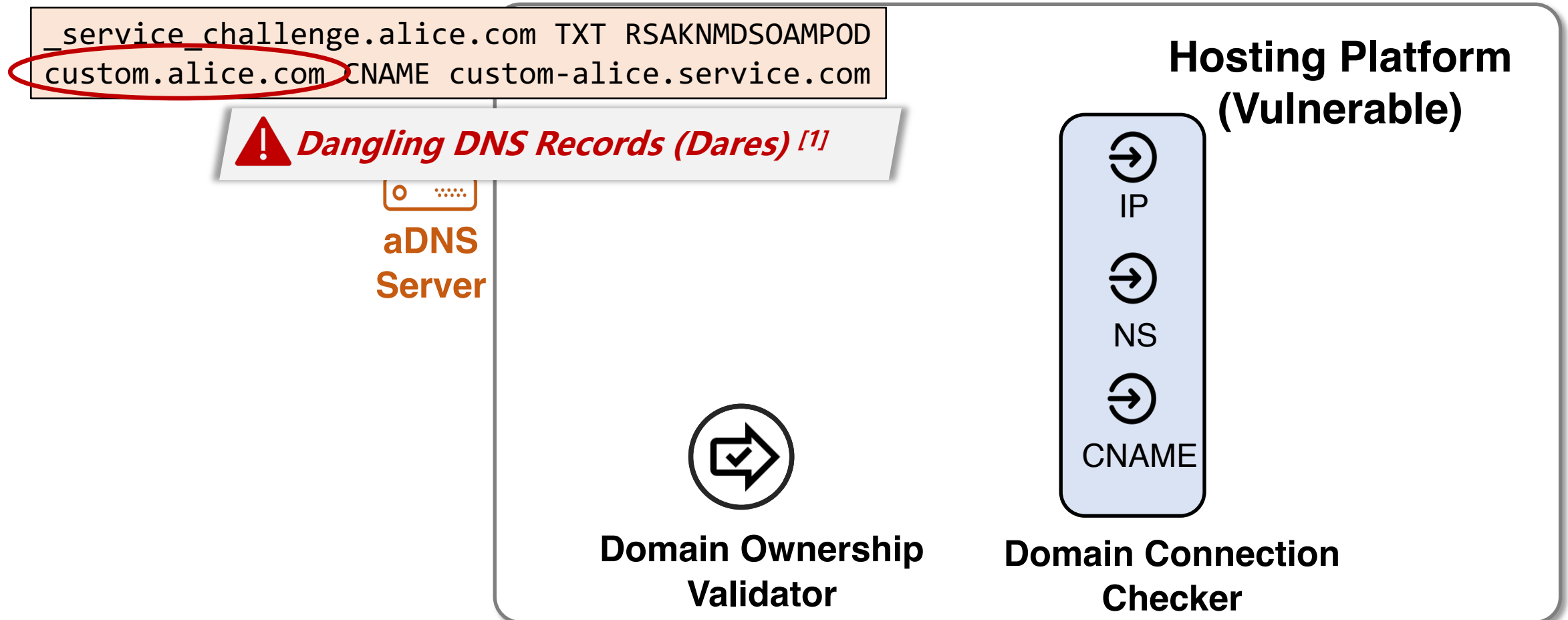
Hosting-based Domain Takeover

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



Hosting-based Domain Takeover

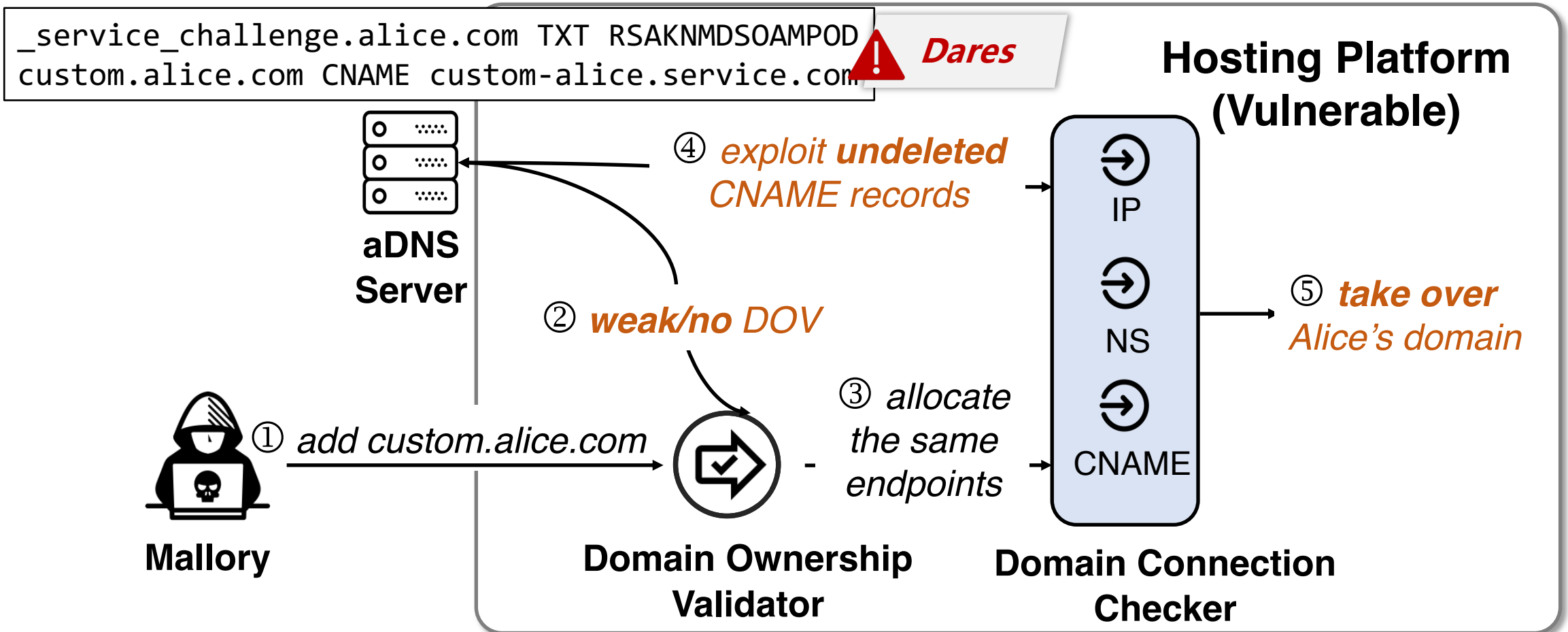
- Alice's domain RRs become dangling -> Use-after-free.



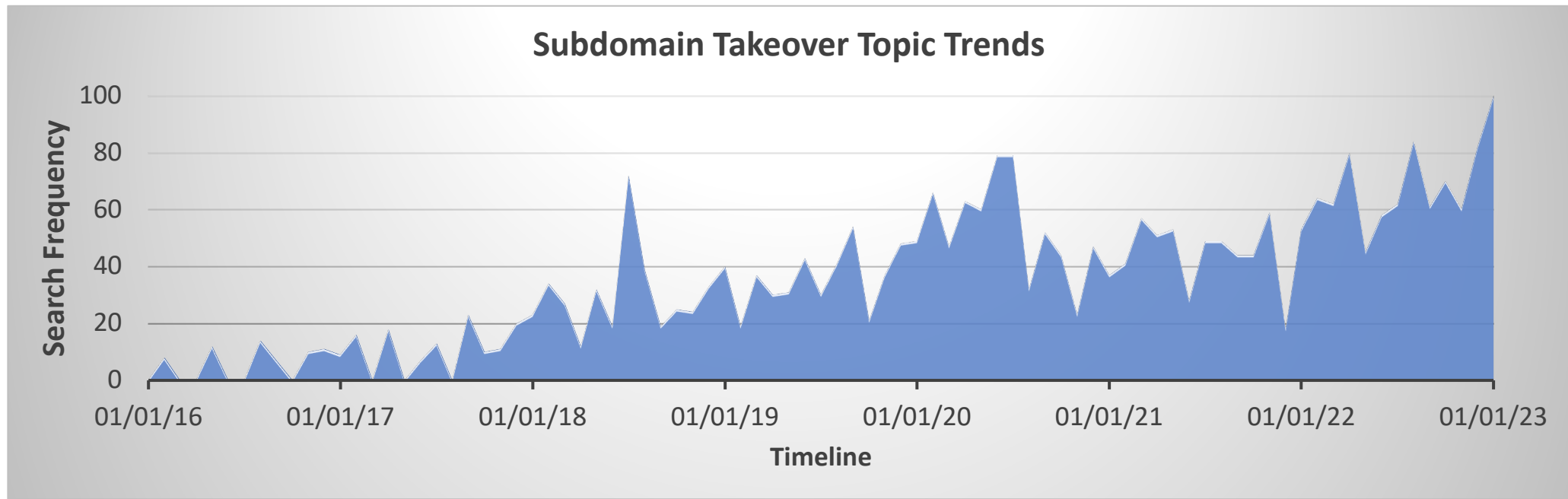
[1] All Your DNS Records Point to Us [CCS '16]

Hosting-based Domain Takeover

- Attacker could apply the same CNAME from the platform, bypass DOV, and take over Alice's domain



Why domain takeover occurs constantly?



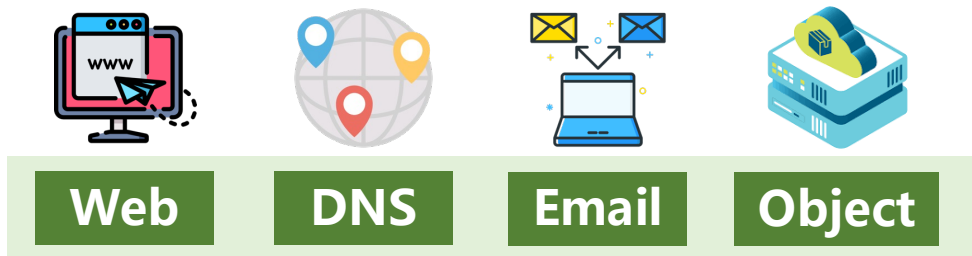
"Domain takeover incidents are still on the rise, increasing by 25% from 2020 to 2021."¹

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

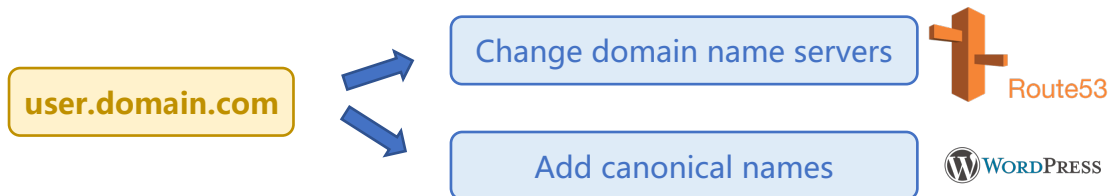
Challenges

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

45		Subdomain Takeover - https://competition.shopify.com/ By Ilt41 to Shopify Resolved Medium \$750.00
55		Subdomain takeover on partners.ubnt.com due to non-used CloudFront DNS entry By fransrosen to Ubiquiti Inc. Resolved \$1,000.00
47		Bypassing callback_url validation on Digits By filedescriptor to Twitter Resolved \$2,520.00
22		Account Takeover on https://www.delivery-club.ru через партнерский аккаунт. By danila to Mail.ru Resolved Critical \$1,000.00
19		Unclaimed Github Repository Takeover on https://www.data.gov/labs By noobzombie to GSA Bounty Resolved Low \$150.00

Challenges

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?

Domain characteristics of hosting services.

DNS chains of vulnerable domains.

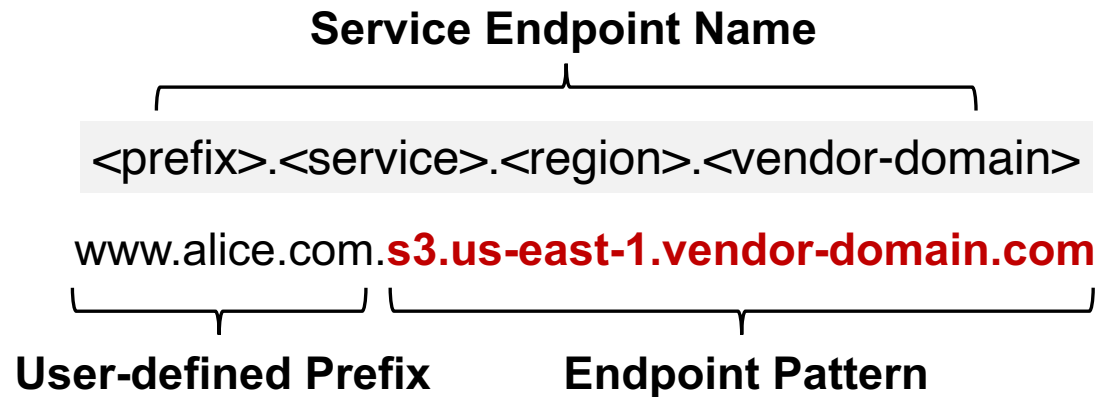
Logged in

DNS traffic

Empirical Observations

O1. Hosting services (e.g., CDN, OSS, Web Hosting) adopt similar endpoint naming conventions

➤ Service Endpoint Patterns



```
// Amazon S3
s3.cn-north-1.amazonaws.com.cn
s3.dualstack.ap-northeast-1.amazonaws.com
s3.dualstack.ap-northeast-2.amazonaws.com
s3.ap-northeast-2.amazonaws.com
s3-website.ap-northeast-2.amazonaws.com
s3.dualstack.ap-south-1.amazonaws.com

// AWS Elastic Beanstalk
cn-north-1.elb.amazonaws.com.cn
cn-northwest-1.elb.amazonaws.com.cn
elasticbeanstalk.com
ap-northeast-1.elasticbeanstalk.com
ap-northeast-2.elasticbeanstalk.com
ap-northeast-3.elasticbeanstalk.com
```

AWS Endpoint Pattern Examples¹

¹ Public Suffix List. <https://publicsuffix.org/list/> 17

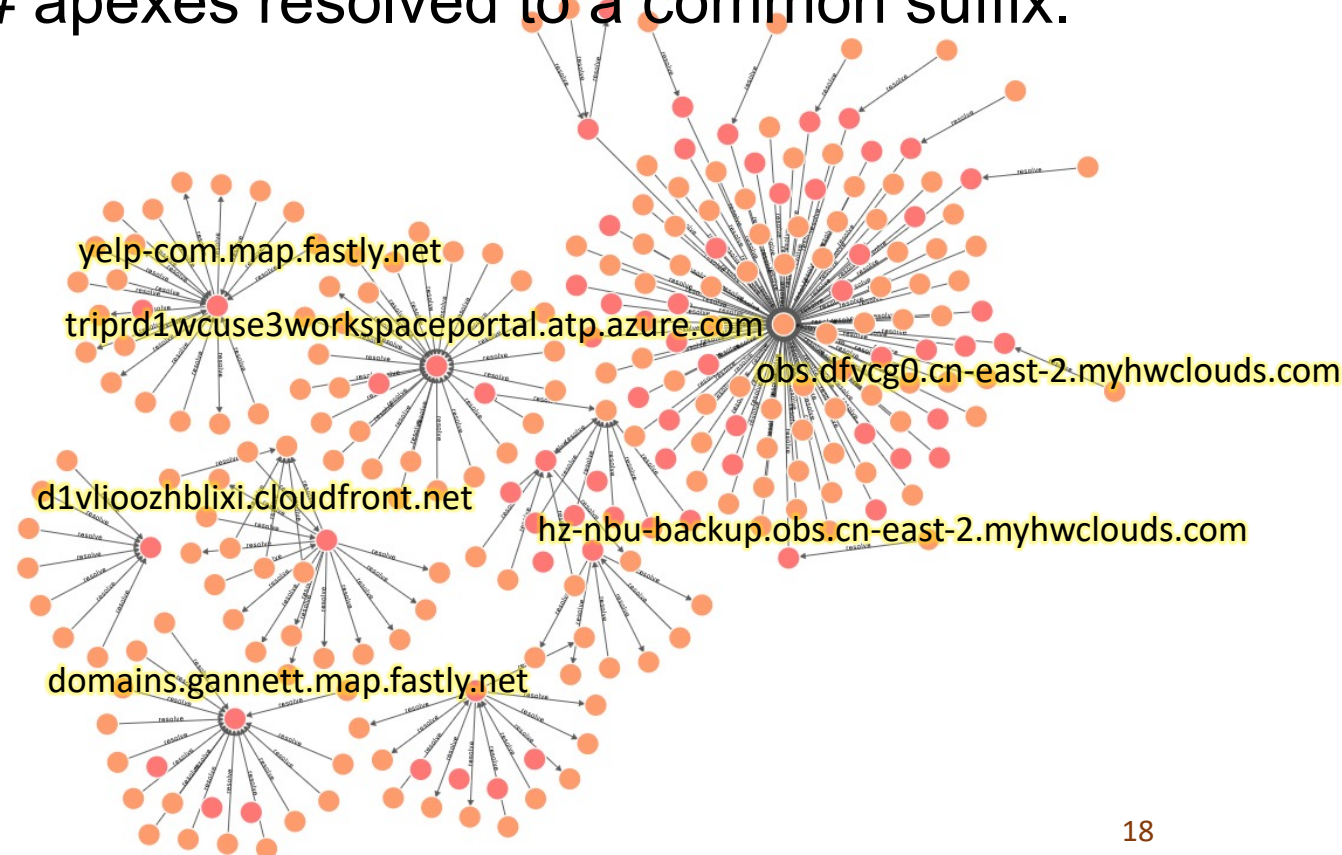
Empirical Observations

O2. High domain dependency number

- Service endpoint domains may serve thousands of custom domains
- **Domain dependency number:** # apexes resolved to a common suffix.

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

$$DN("service.com") = N$$



Our solution



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



HostingChecker: System Goals

➤ A novel framework that can assist in:

1. Discovering vulnerable hosting services

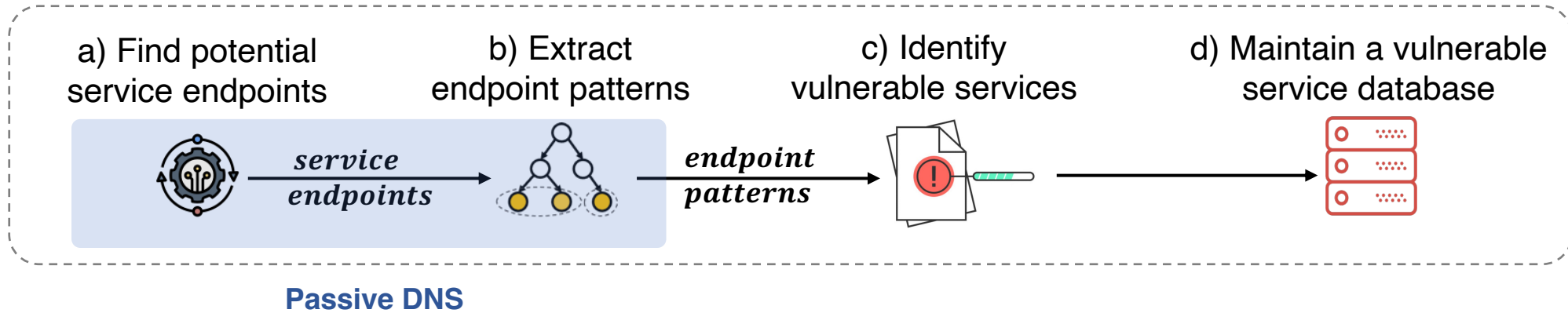
➤ *Expand the detection scope*

2. Detecting hosting-based vulnerable domains efficiently

➤ *Prevent potential security threats*

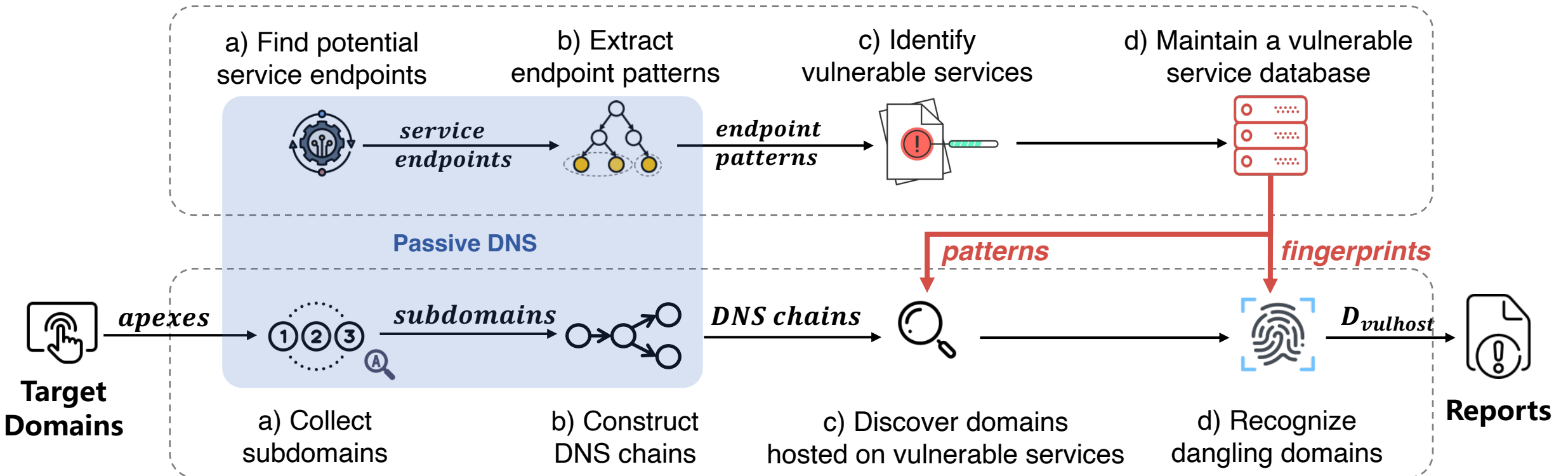
HostingChecker Workflow

Part 1. Vulnerable service discovery (offline procedure)



HostingChecker Workflow

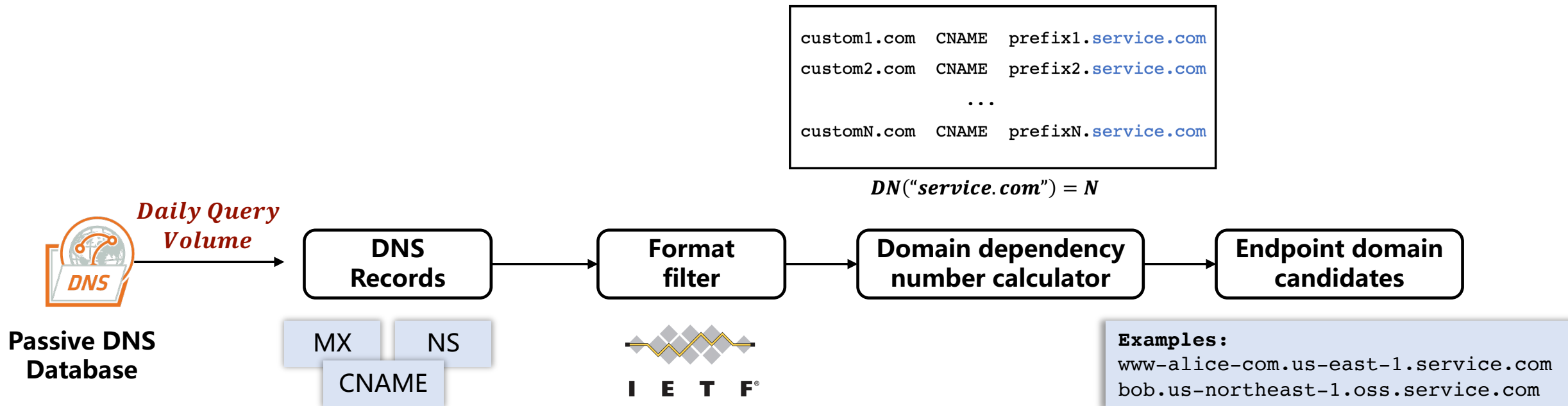
Part 1. Vulnerable service discovery (offline procedure)



Part I: Discovering Vul. Services

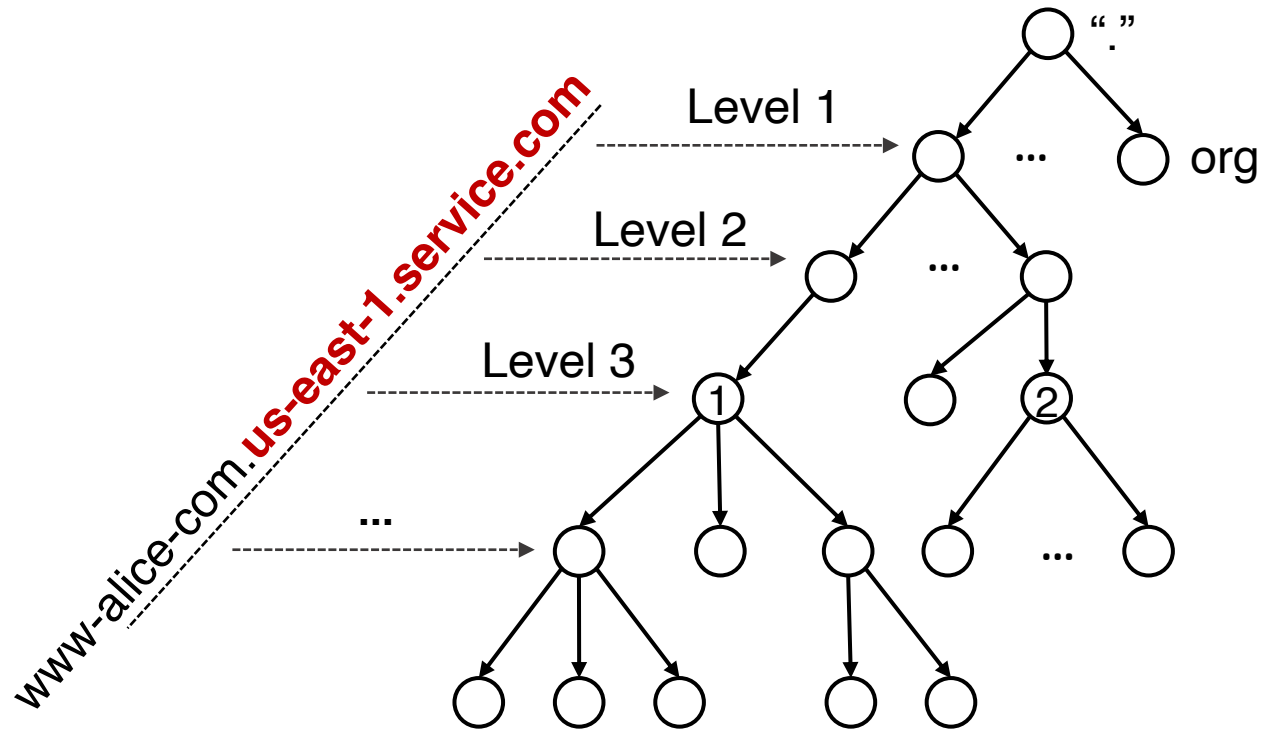
➤ Step 1: Finding service endpoint candidates

- Filtering endpoint domains by domain dependency (referring to Observation 2).



Part I: Discovering Vul. Services

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



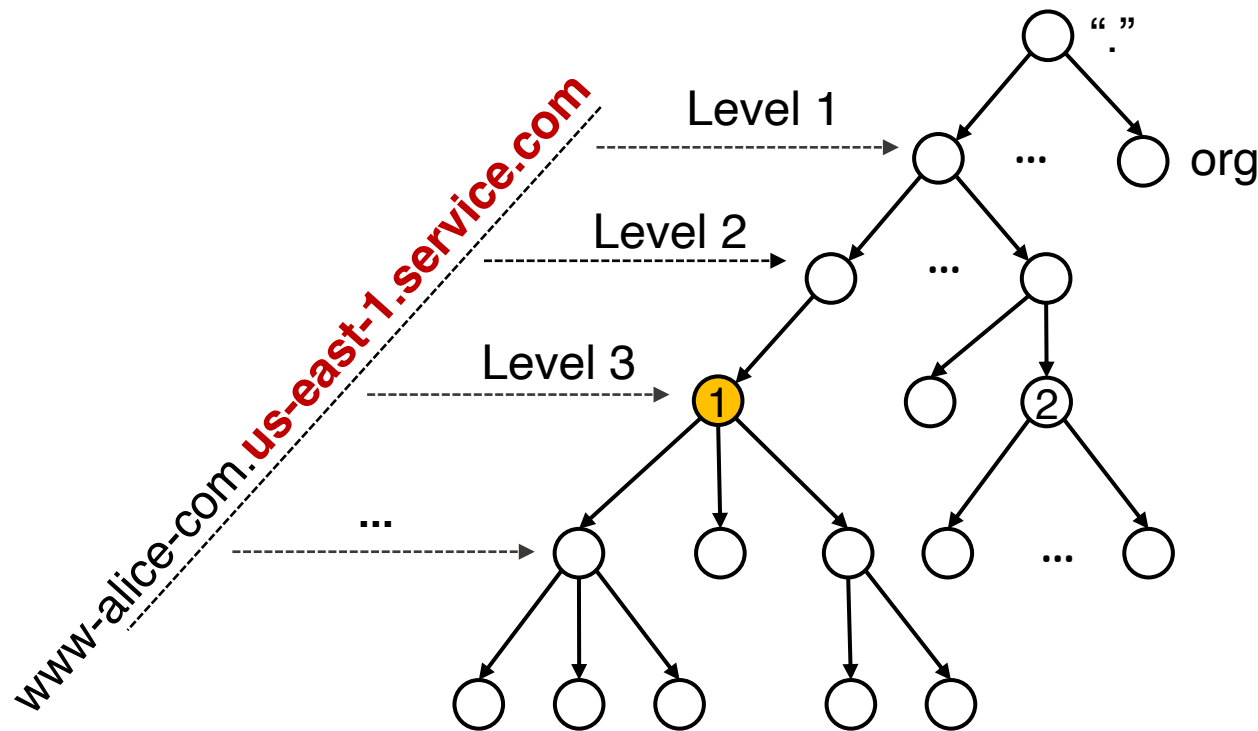
Domain Tree

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**



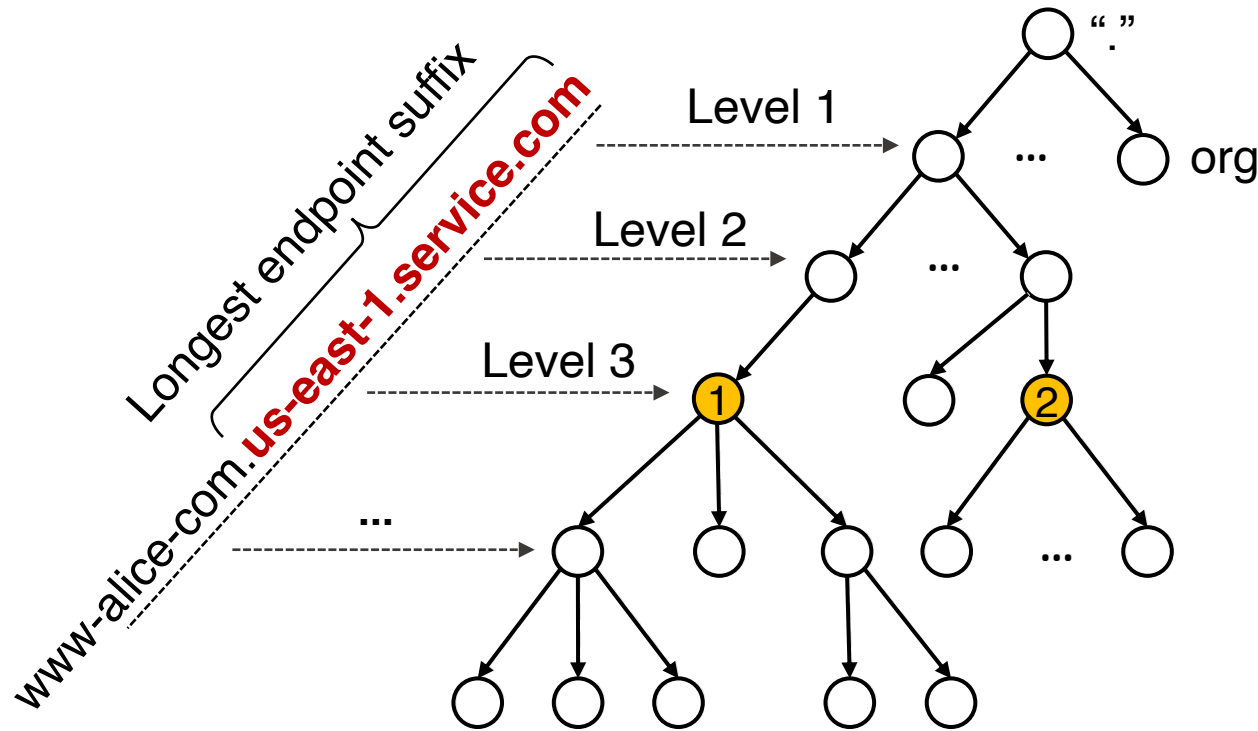
Domain Tree

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

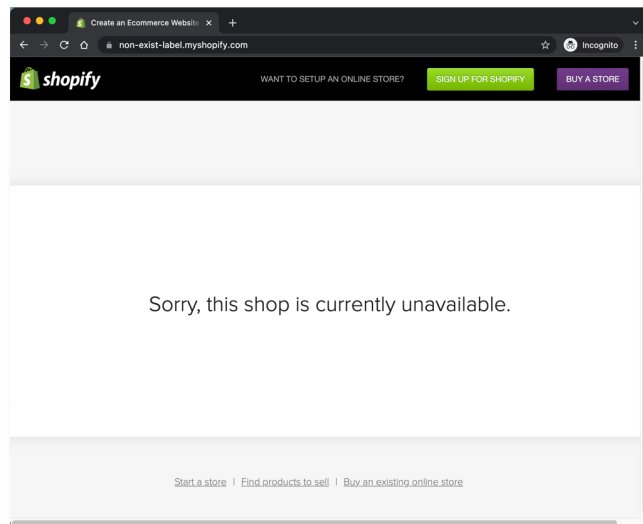
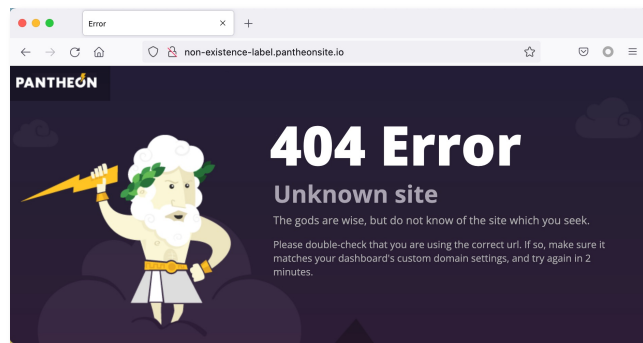
Services	Endpoint Names (endpoint patterns)
Aliyun OSS	alice.storage.com. oss-cn-hongkong.aliyuncs.com
Amazon S3	a.b.c.d. s3.us-east-1.amazonaws.com ab-cd. s3.dualstack.us-gov-west-1.amazonaws.com
GitHub	abcd. github.io

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

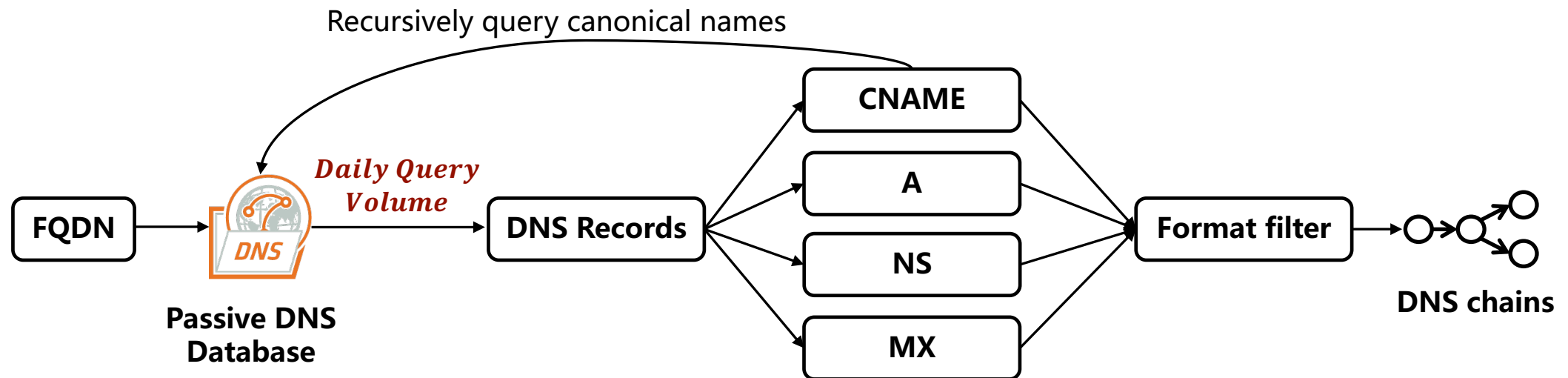
Type	Response Example	# Banner	# Service	# Vendor
HTTP Response		106	59	48
Header	"404 Unknown site"	14	13	10
Body	"NoSuchBucket"	92	52	47
DNS Answer		4	13	9
NX-CNAME ¹	status:NXDOMAIN	1	11	7
Default Rdata ²	127.0.0.1 nx.aicdn.com	3	2	2
Total		110	64	51

Part II: Detecting Vul. Domains

➤ Collecting subdomain names from passive DNS logs

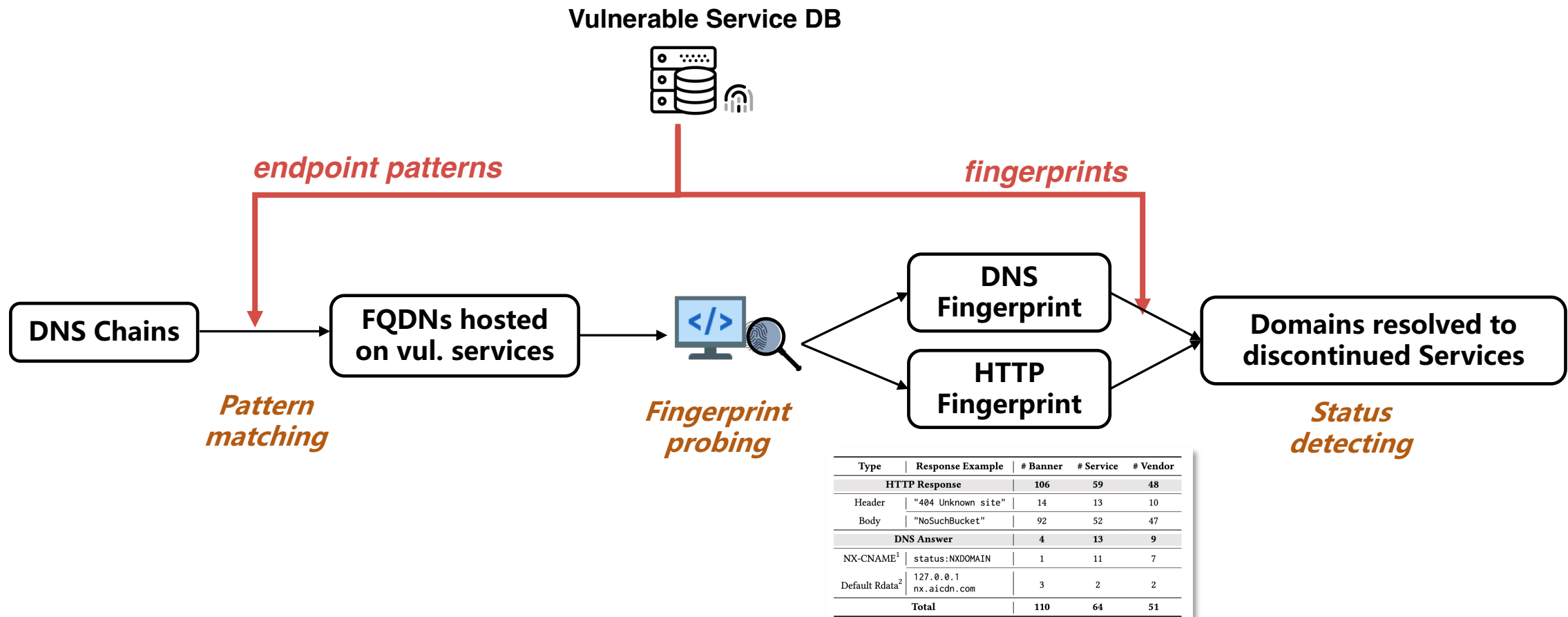
- Legal format **[RFC 1034] Domain Names - Concepts And Facilities**
- Filter disposable domains created on demand
e.g., scanning, convey “one-time signals” ***Total Query Volume > 100***

➤ Reconstructing domain dependencies (DNS chains)



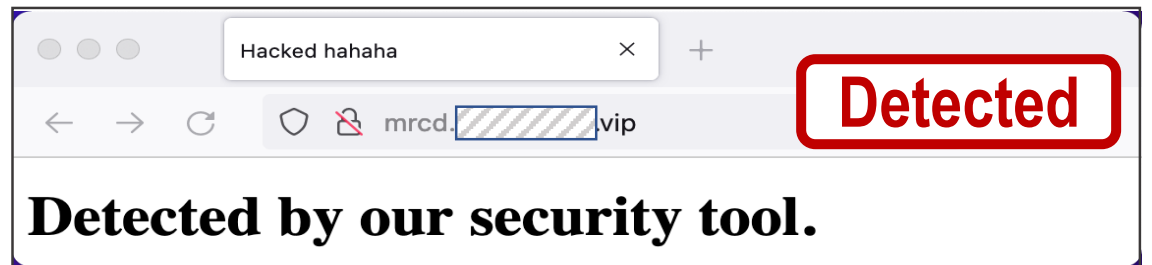
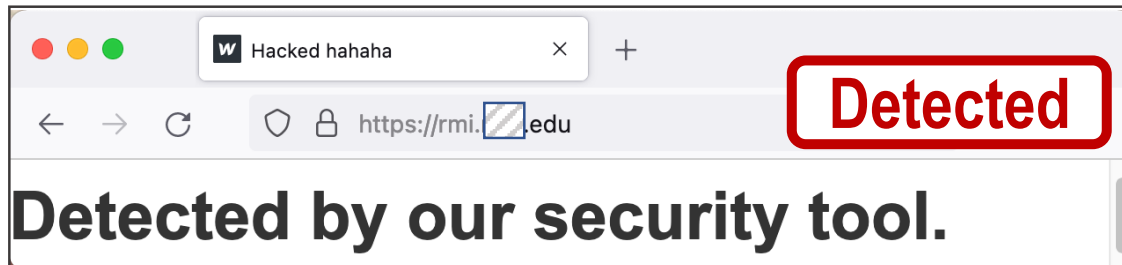
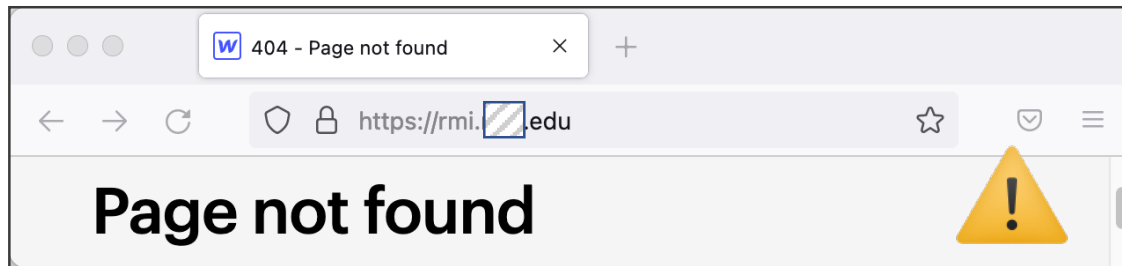
Part II: Detecting Vul. Domains

➤ Probing hosted domains to inspect service status



Part II: Detecting Vul. Domains

➤ Probing hosted domains to inspect service status

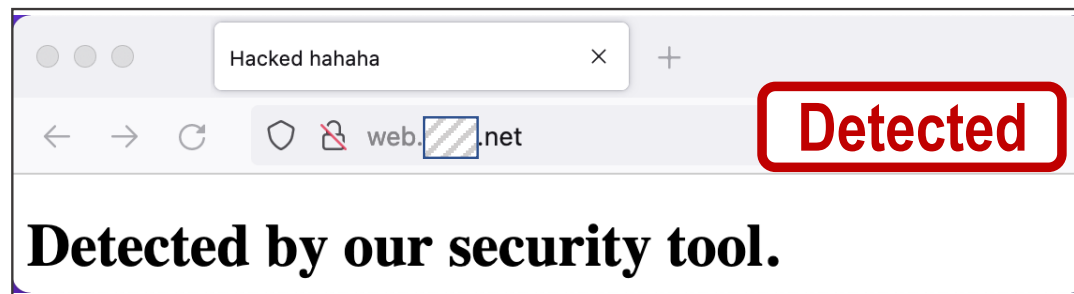
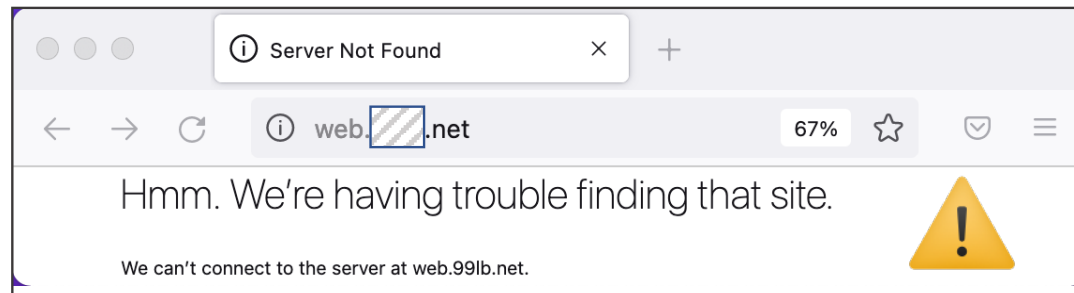


(1) Webflow
rmi.xxxx.edu

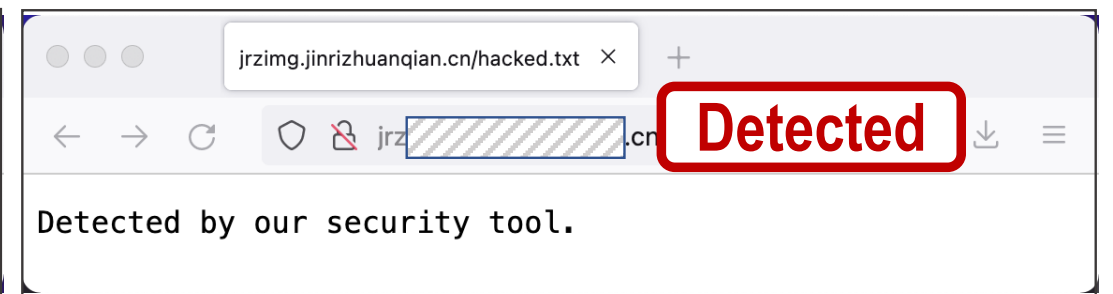
(2) Fastly
mrcd.xxxxxxxx.vip

Part II: Detecting Vul. Domains

➤ Probing hosted domains to inspect service status



(3) Cloudflare
web.xxxx.net



(4) Alibaba Cloud
jrzxxx.xxxxxxxxxxxxxxxxxx.cn

Deployment

➤ Passive DNS dataset

- Collected from public resolvers of **114DNS**¹.
- **High coverage:** **600B** DNS queries per day, covering **99.9%** of Tranco Top 1M domains.

➤ 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

¹ 114DNS: the largest DNS provider in China. <https://www.114dns.com/>

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.**
 - e.g., Cloudflare, Alibaba OSS, Unbounce
- **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

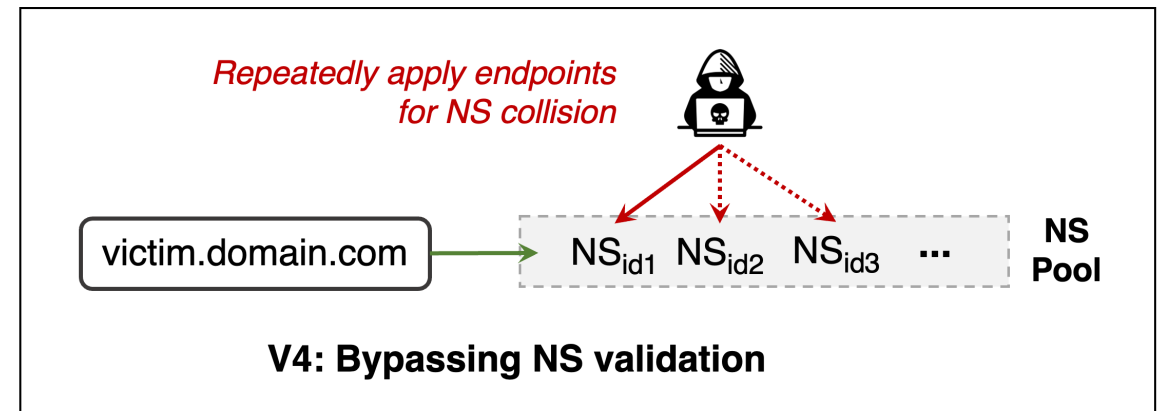
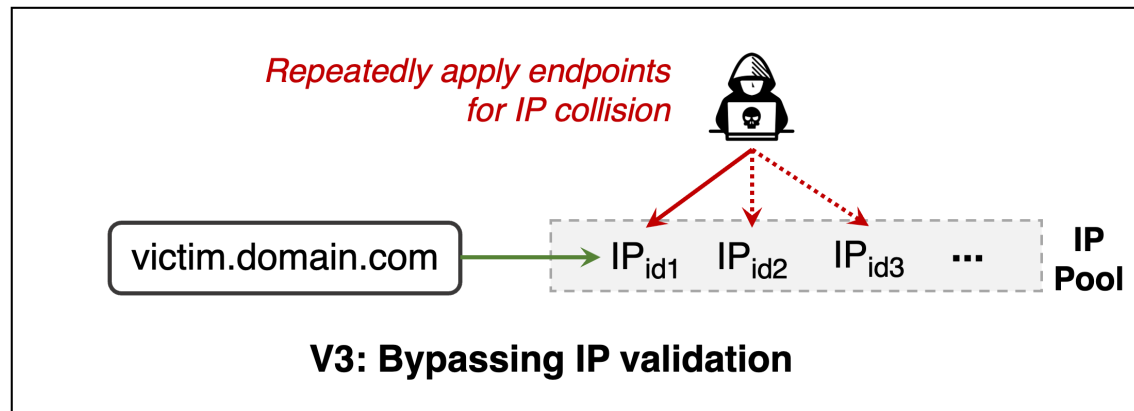
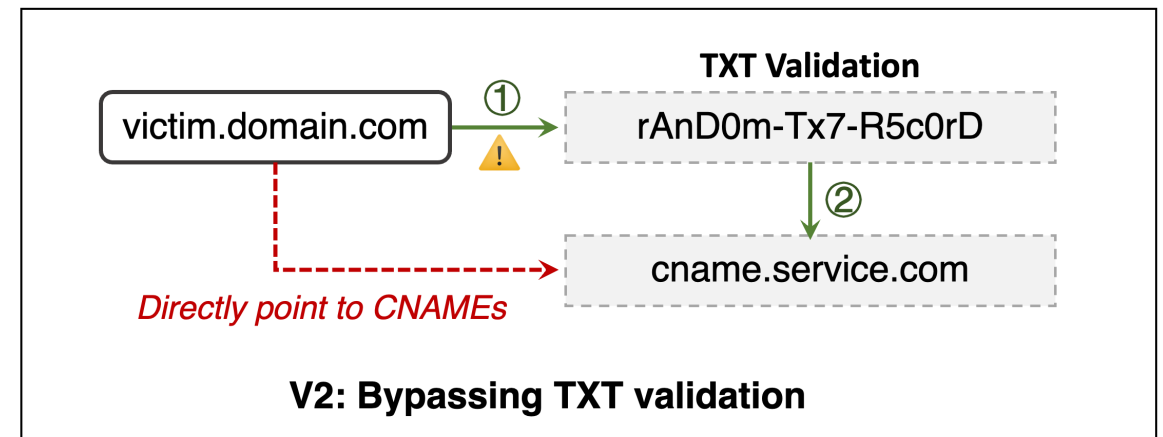
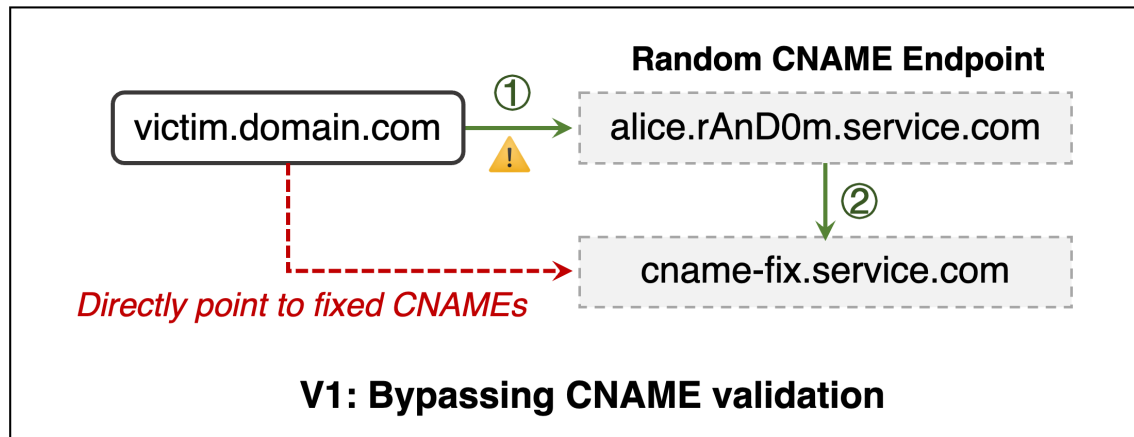
➤ 7/9 domain connecting methods are exploitable

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

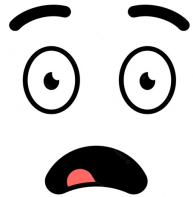
→ Normal validation procedure - - - -> Bypass method



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 Storage	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

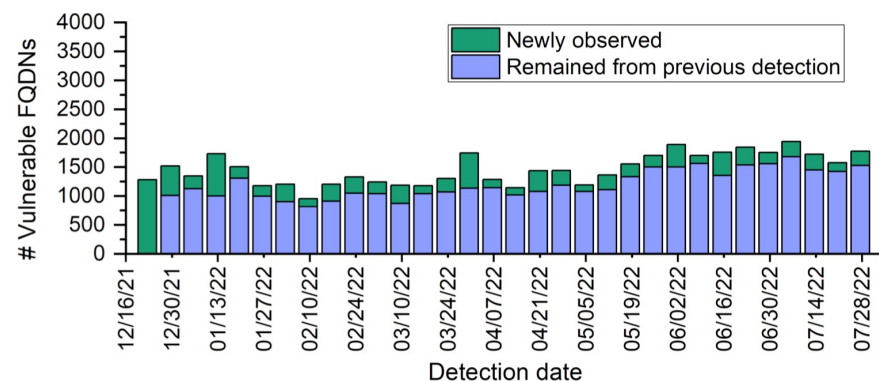


What did we find for domain takeover?

- Hosting-based domain takeover threats are still **prevalent**.

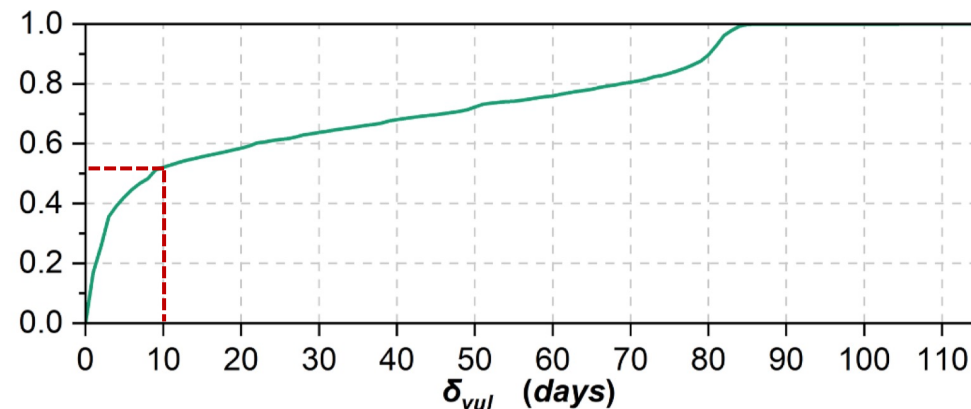
Detected Vulnerable Domains

- **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

➤ **HostingChecker: 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



HUAWEI CLOUD



Our Lab

NISL@THU

News

People

Publications

Talks

Teaching

Seminars

Security Monitor

Hacking

Contact



Network and Information Security Lab @ Tsinghua University

A research team focusing on cyber security at Tsinghua University.

A playground for fun hacking and fundamental research.

Base of the CTF teams Blue-Lotus and RedBud.

News

May 2023 - Our paper [Efficient 3PC for Binary Circuits with Application to Maliciously-Secure DNN Inference](#) was accepted by USENIX Security 2023.

May 2023 - Our paper [AlphaEXP: An Expert System for Identifying Security-Sensitive Kernel Objects](#) was accepted by USENIX Security 2023.

May 2023 - Our paper [1dFuzz: Reproduce 1-day Vulnerabilities with Directed Differential Fuzzing](#) was accepted by ISSTA 2023.

April 2023 - Our paper [RaceBench: A Triggerable and Observable Concurrency Bug Benchmark](#) was accepted by ASIACCS 2023.

Mar 2023 - Our paper [Under the Dark: A Systematical Study of Stealthy Mining Pools \(Ab\)use in the Wild](#) was accepted by ACM CCS 2023.

Mar 2023 - Our paper [ODDFUZZ: Discovering Java Deserialization Vulnerabilities via Structure-Aware Directed Greybox Fuzzing](#) was accepted by IEEE S&P 2023.

Feb 2023 - Our paper [PTStore: Lightweight Architectural Support for Pa](#) accepted by DAC 2023.

Feb 2023 - Our paper [MPass: Bypassing Learning-based Static Malware](#) by DAC 2023.

Network Security



Web Security



Software Security



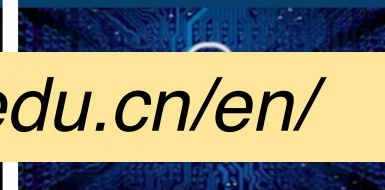
System Security



AI Security



Data-driven Security



<https://netsec.ccert.edu.cn/en/>

Thanks for listening!

Any questions?

Mingming Zhang

zhangmm717@gmail.com

<https://www.zhangmingming.org>

