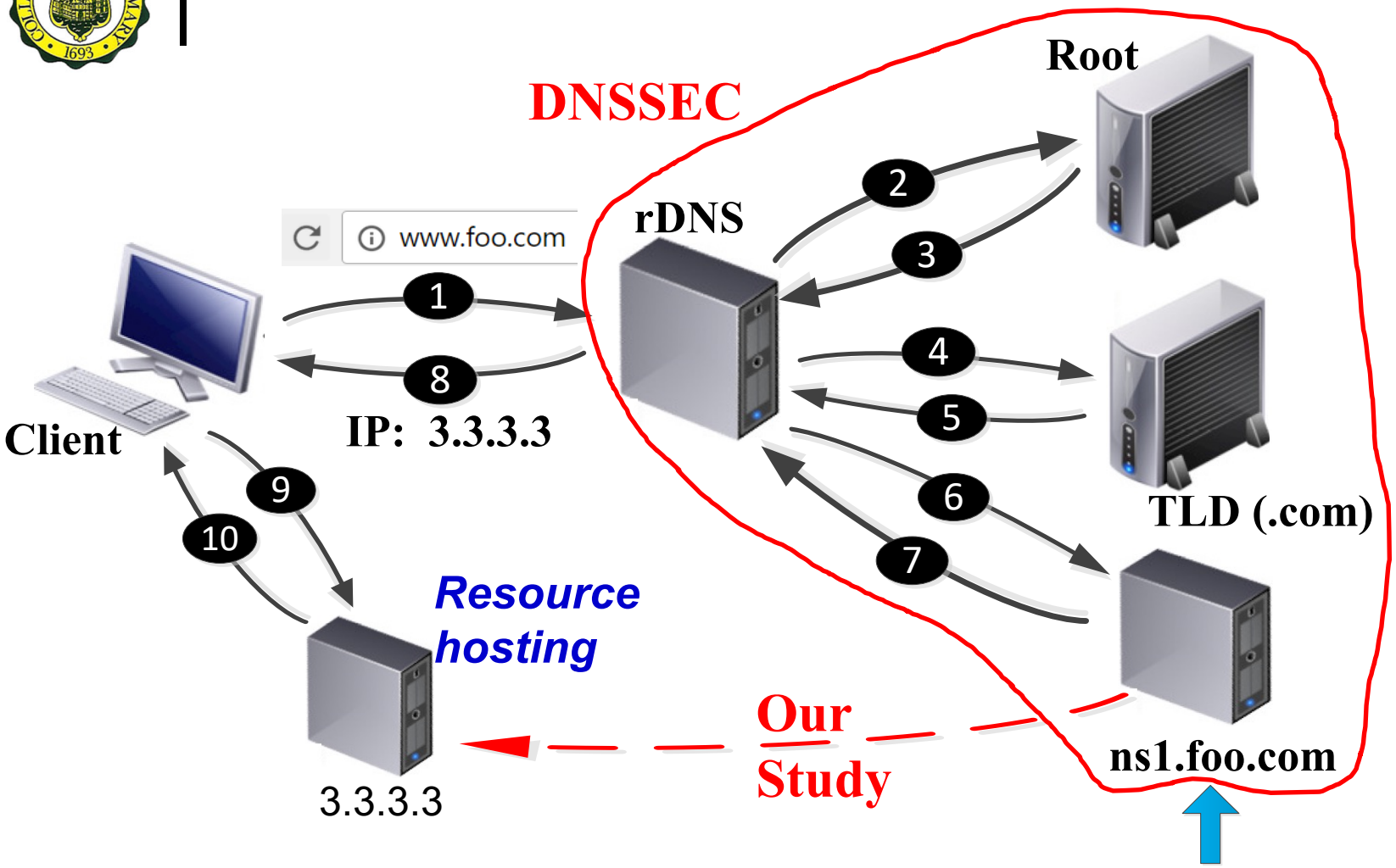
All Your DNS Records Point to Us: Understanding the Security Threats of Dangling DNS Records

Daiping Liu, Shuai Hao, Haining Wang

University of Delaware
College of William and Mary

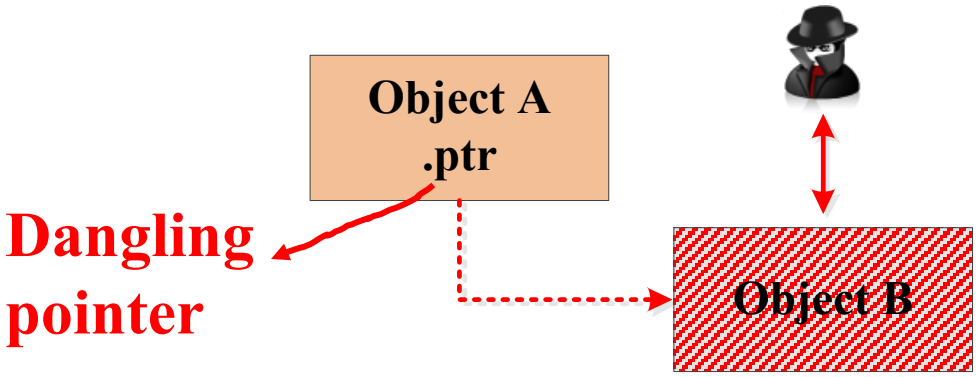
Presenter: Shuai Hao, ODU
Sep. 2022

DNS Workflow

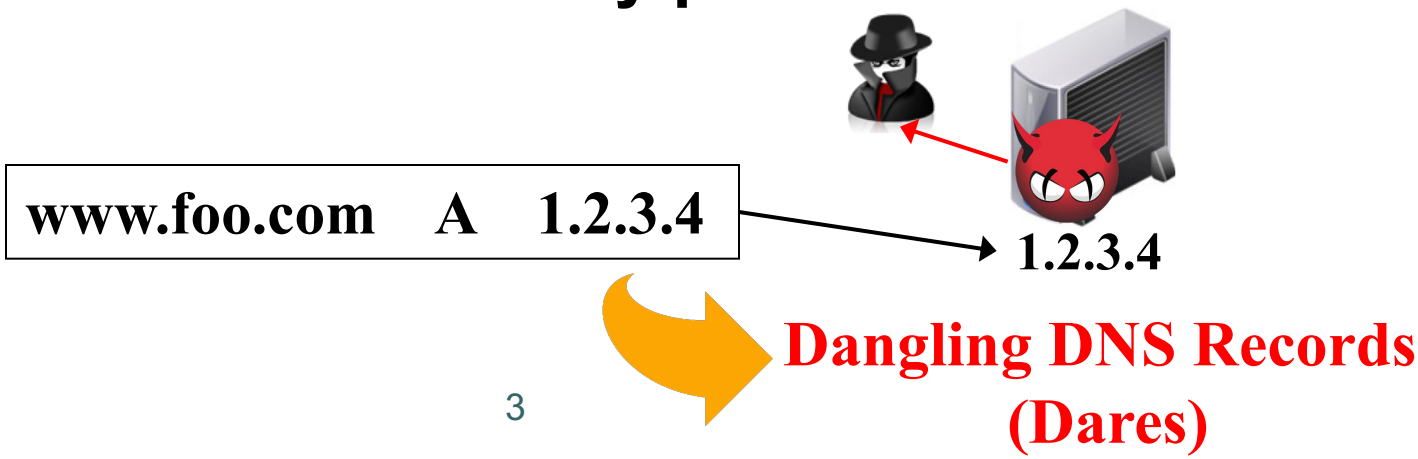


When Use-after-Free Meets DNS

Inspired by use-after-free vulnerabilities



DNS records are essentially pointers



Dangling DNS Records (Dare)

A DNS record *r:= <name, TTL, class, type, data>* is dangling if the resources to which the *data* field points is released.

Security Sensitive Dares

- 4 out of ~40 types of DNS records are security sensitive

Dare	RR	Description
Dare-A†	A	Returns an IPv4 address
Dare-CN‡	CNAME	Alias of a name to another
Dare-MX	MX	Maps to a list of message transfer agents
Dare-NS	NS	Delegate to an authoritative name server

Dangling DNS Records (Dare)

Canonical name

Dare-A

- www.foo.com A 3.3.3.3
- www.foo.com gets hijacked

Dare-CN

- www.foo.com CNAME bar.com
  bar.com A 4.4.4.4
- www.foo.com gets hijacked

Dare-MX

- foo.com MX 10 a.mail.com
  foo.com MX 10 b.mail.com
  foo.com MX 20 c.mail.com
  a.mail.com A 2.2.2.2
- Send/Receive emails under foo.com

Dare-NS

- foo.com NS ns1.foo.com
  ns1.foo.com A 5.5.5.5
- All domain names depending on ns1.foo.com get hijacked

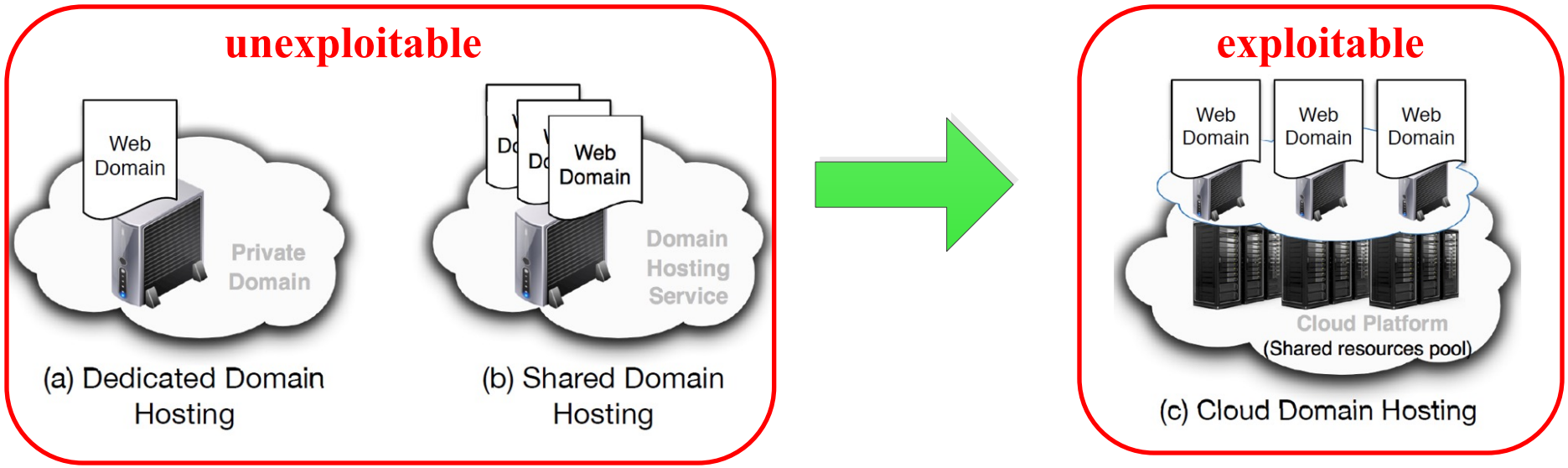
Exploiting Dares

- **Two Data Types in the "Data" Fields**
  - IP address
  - Domain names

- **Three Attack Vectors**
  - IP in Cloud
  - Abandoned Third-Party Services
  - Expired Domains

Attack Vector I
-- IP in Cloud

How a domain is hosted determines if its IP address is exploitable



amazon web services™ | EC2

Windows Azure

Attack Vector II
-- Abandoned Services

Modern websites extensively use third-party services

shop.alice.com CNAME alice.myshopify.com	*.myshopify.com CNAME shops.shopify.com

Dare-CN


Attack Vector III -- Expired Domains

The `data` fields of `CNAME`, `MX` and `NS` records may point to expired domains

- Previous works have studied apex domain re-registration [S&P'16]

expired.com

- We study the domains pointing to the expired ones

example.com CNAME expired.com


Measurement Study -- Domain Collection

Apex Domains

- Choose popular ones

Dataset	Data Space
D	Unexpired apex domains in Alexa top 1M during 2010 $\sim$ 2016
S_t	Subdomains of top 10,000 general
S_e	Subdomains of top 2,700 .edu
S_g	Subdomains of top 1,700 .gov

Subdomains

- Derive a word list (subdomain name candidate) at the size of 20K from zone transfer results of 320 domains
- Brute-force scanning

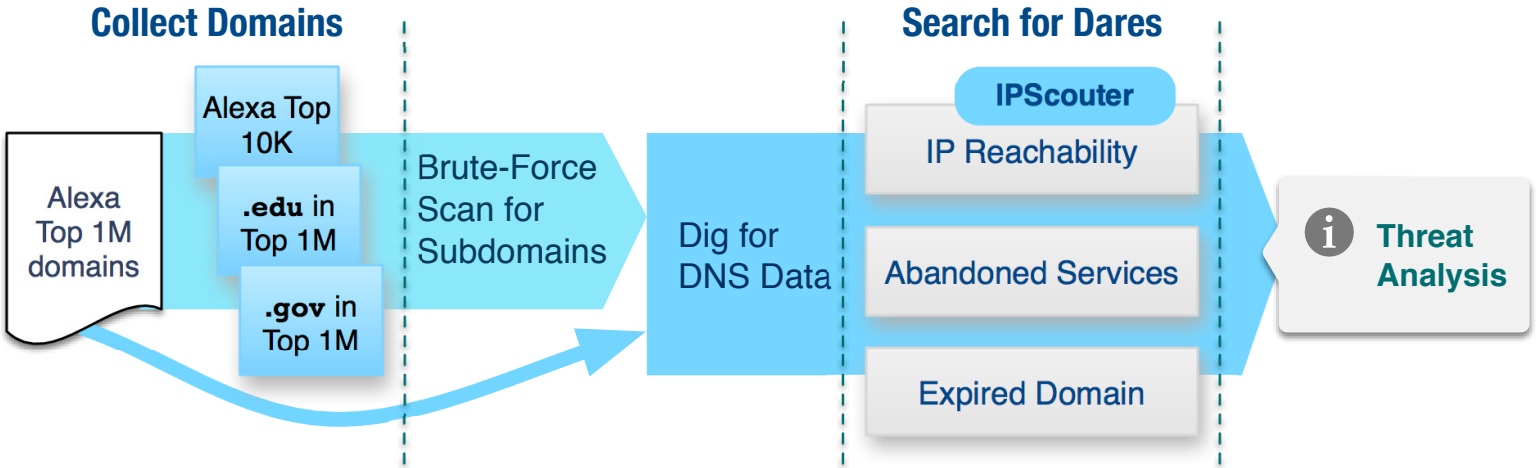
DNS Data Retrieval using dig

Measurement Study -- Domain Collection

Apex Domains

- Choose popular ones

Dataset	Data Space
D	Unexpired apex domains in Alexa top 1M during $2010 \sim 2016$
S_t	Subdomains of top 10,000 general
S_e	Subdomains of top 2,700 .edu
S_g	Subdomains of top 1,700 .gov



Search for Dares

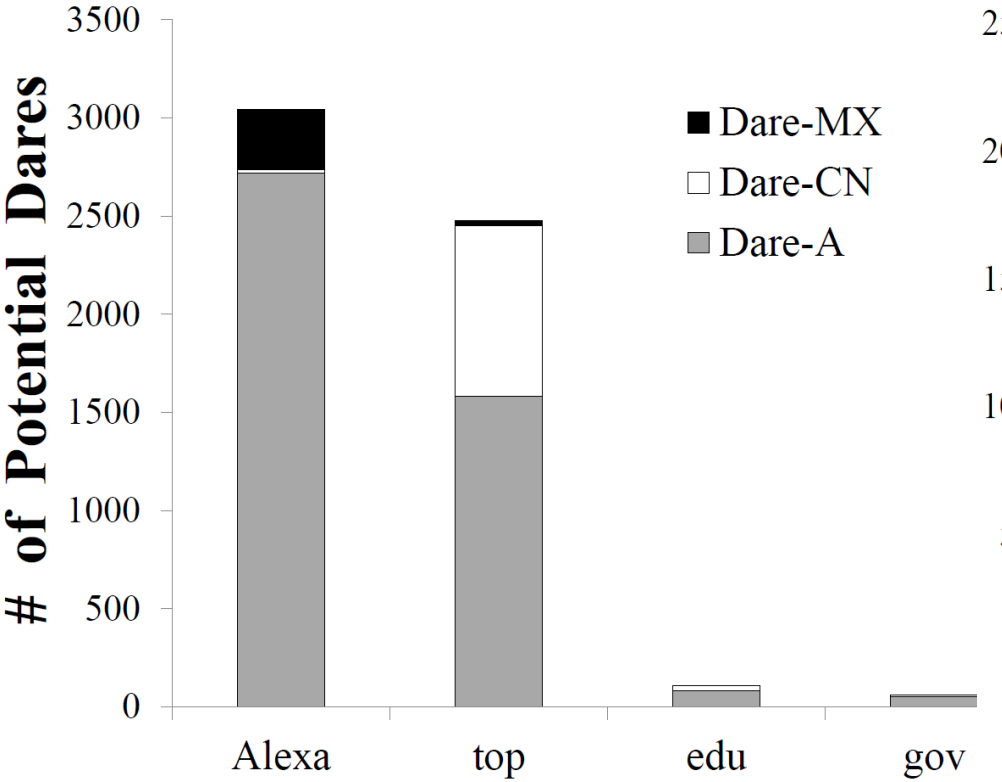
- Based on DNS data collected from $D+S_t+S_e+S_g$
  - IP in Cloud
  - Abandoned Third-party Service
  - Expired domains


Measurement Study -- IP in Cloud

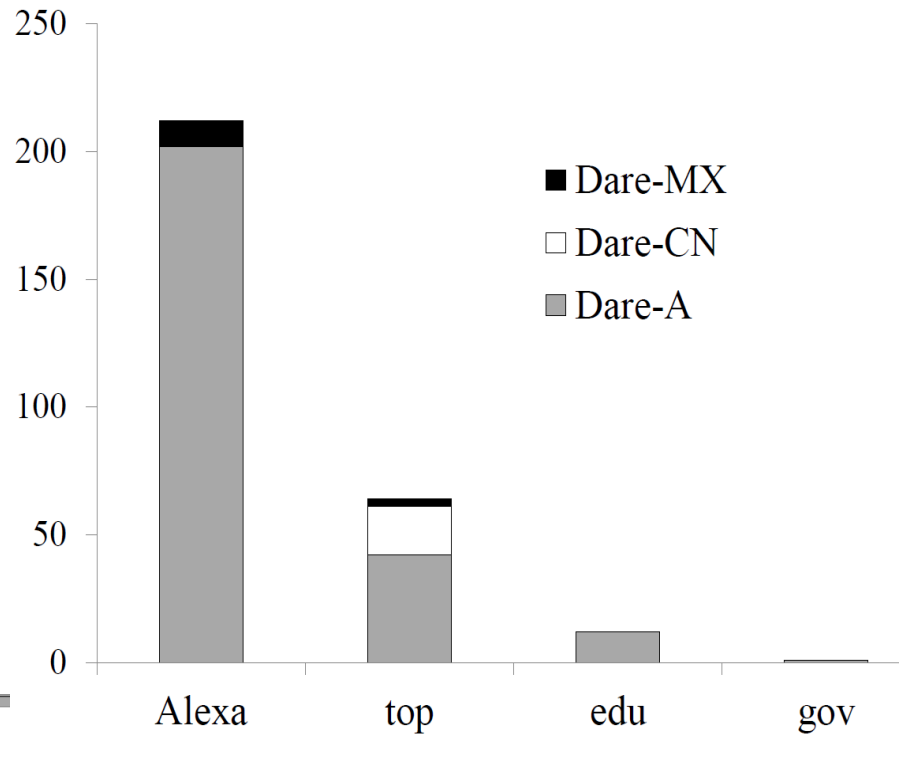
What is the potential magnitude of Dares in the wild?

- Step 1: Filter unexploitable IPs
  - IPs not in the cloud
  - IPs reserved by cloud vendors
- Step 2: Remove live IPs
  - Scan all ports using ZMap

Measurement Study -- IP in Cloud



(a) Amazon EC2



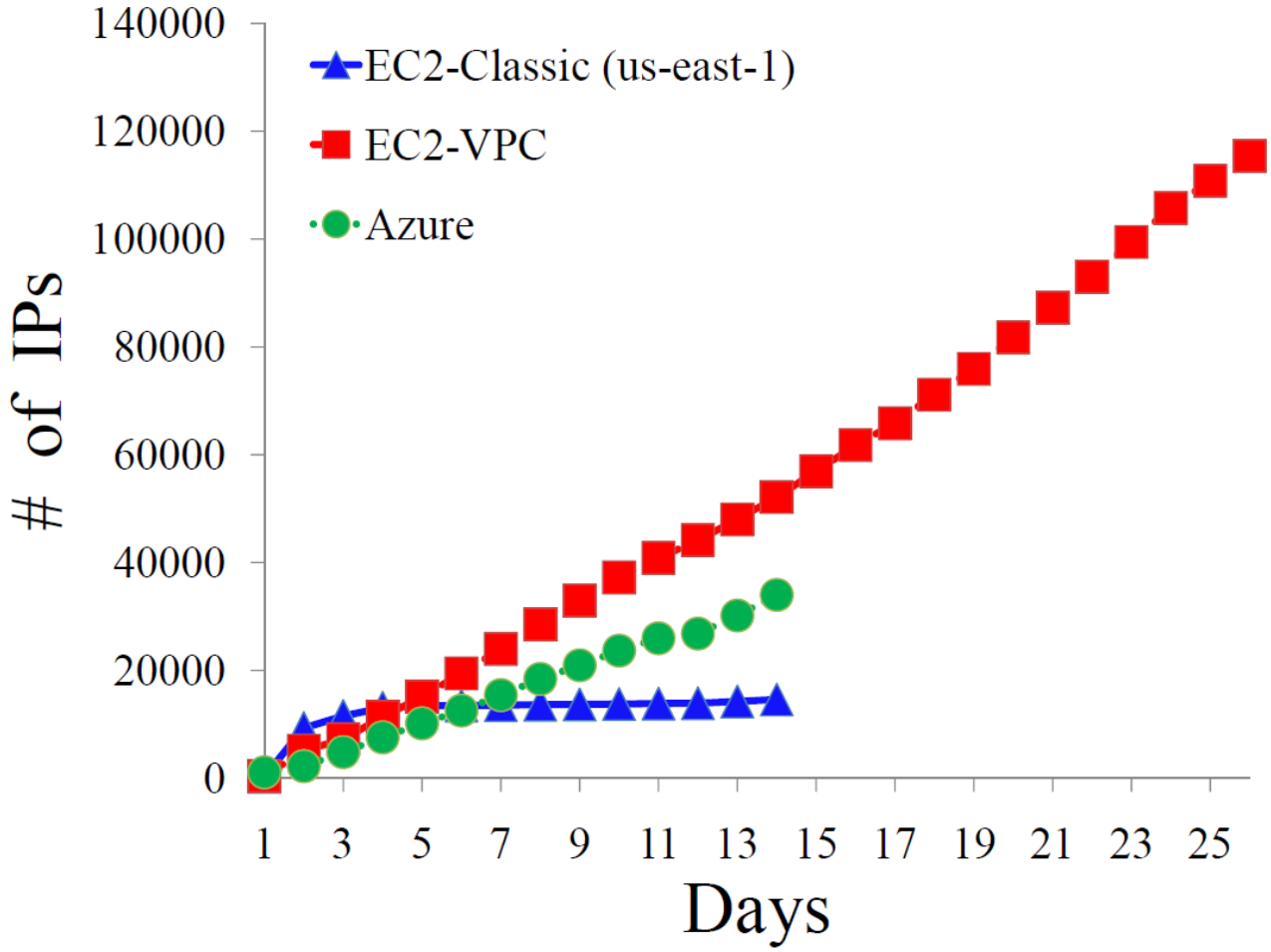
(b) Microsoft Azure


Measurement Study -- IP in Cloud

How practical an attacker can obtain a desired IP?

- Continuously milk IP addresses from EC2 and Azure
  - Immediately release after being logged
  - NO virtual machine is launched

Measurement Study -- IP in Cloud



EC2 (per Day):

7,900 requests

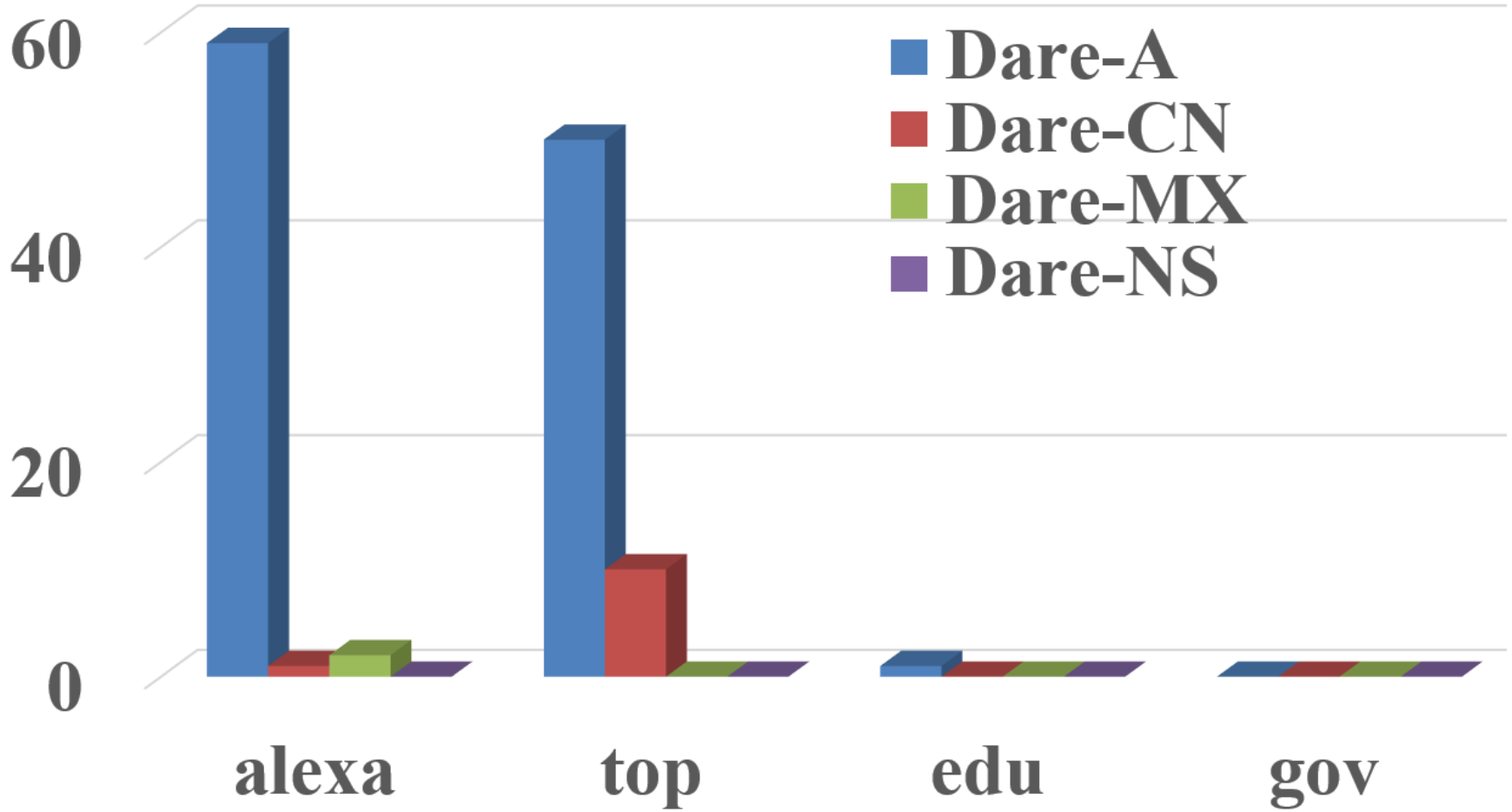
5,000 new IPs

Azure (per Day):

4, 300 requests

2,200 new IPs

Measurement Study -- IP in Cloud



Measurement Study -- Abandoned Services

Top 200 non-email

All email

foo.com	CNAME	foo.myshopify.com
bar.com	CNAME	bar.myshopify.com
zxc.com	CNAME	zxc.wordpress.com
foo.com	MX	mx.mailgun.com

rank

myshopify.com	2
wordpress.com	1
mailgun.com	1

- Free account
- Don't verify ownership claim

8 non-email services
1 email service

Dares ?

Selenium

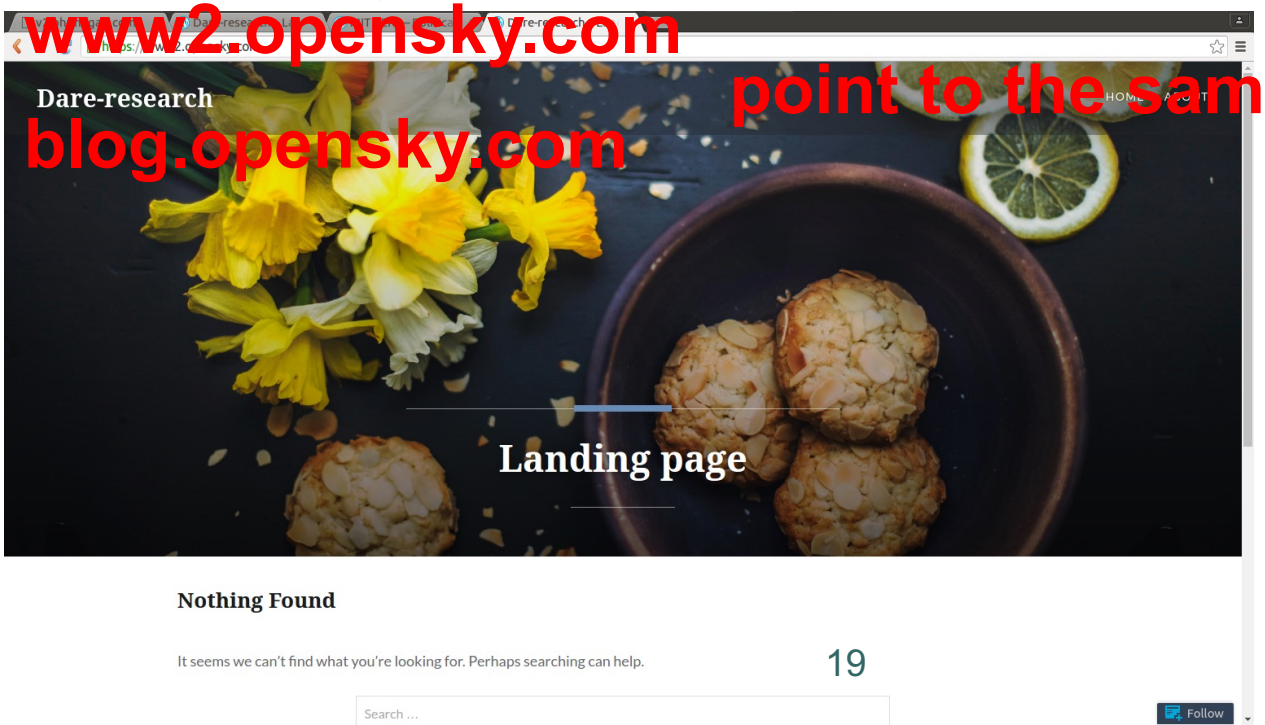
Measurement Study -- Abandoned Services

```
www2.opensky.com@ns-1448.awsdns-53.org.:
www2.opensky.com. CNAME blog.opensky.com.
blog.opensky.com. CNAME openskymerchants.wordpress.com.
```

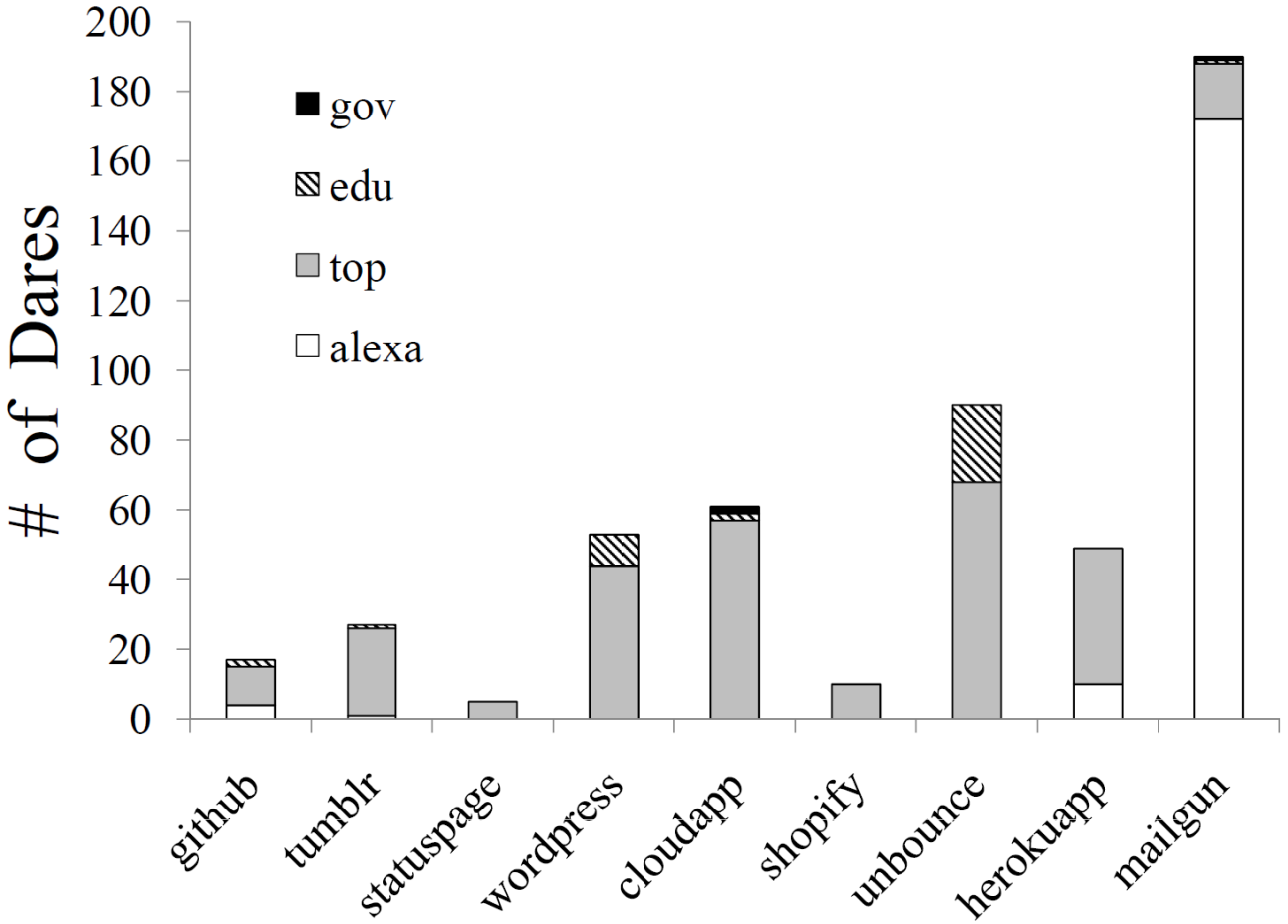
www2.opensky.com

blog.opensky.com

point to the same landing page?



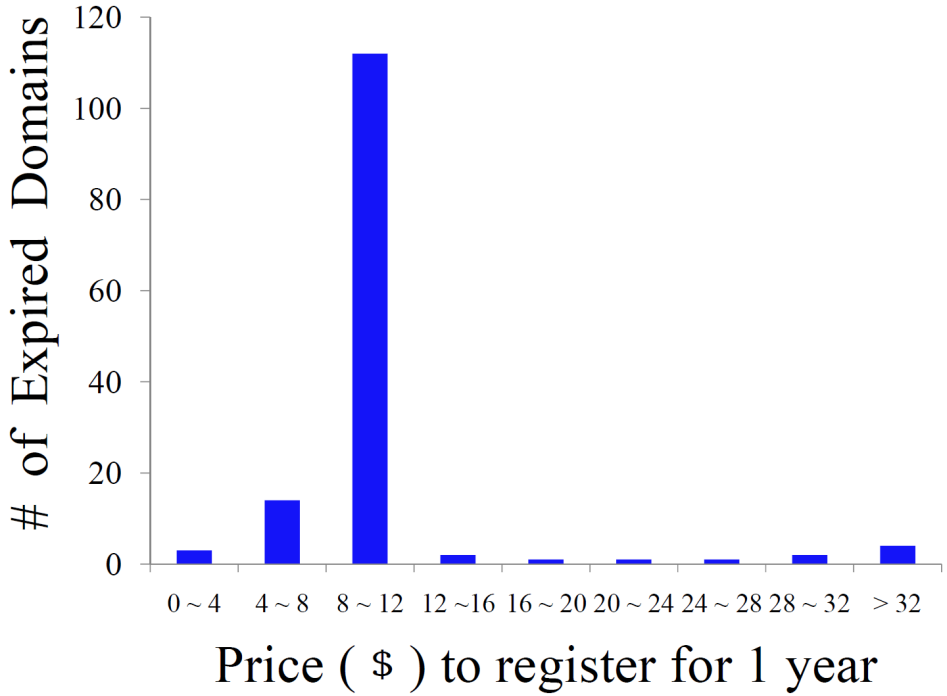
Measurement Study -- Abandoned Services



Measurement Study -- Expired Domains

Step 1: check WHOIS

Step 2: confirm with GoDaddy for re-registration



Measurement Study -- Expired Domains

Pattern	Examples	%
Similar to alias	module.rabobank.nl → rabobank-hoi.nl rps.berkeley.edu → rpsberkeley.org	39%
Expired external services	js.jiayuan.com → 21vcdn.com shopping.segye.com → ticketdamoa.com	21%
Typo	b.ns.trnty.edu → awsnds-18.net customizedgirl.com → shoplattitude.com	7%

Existing defenses by domain registrars

- **Blacklist:**
  - **NO expired domains appeared in blacklists**
- **Similar to well-known domains:**
  - **Can prevent only 46%**

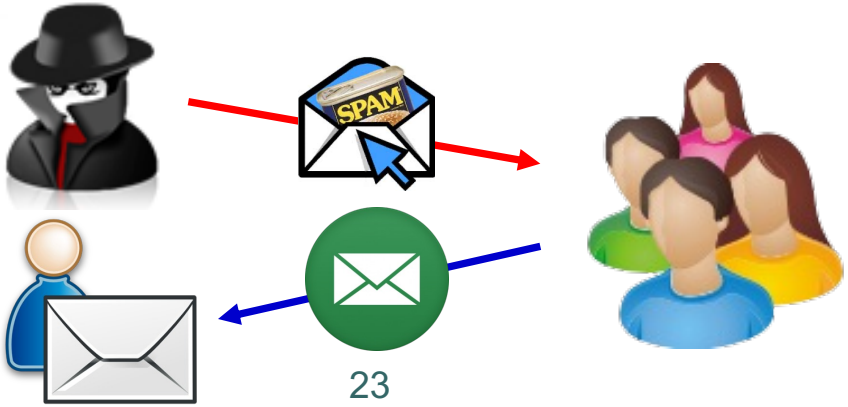
Threat Analysis -- Email Fraud

Still one of the favorite attack vectors in online fraud

Traditional email attacks have two main weaknesses

- **Fake mail server**

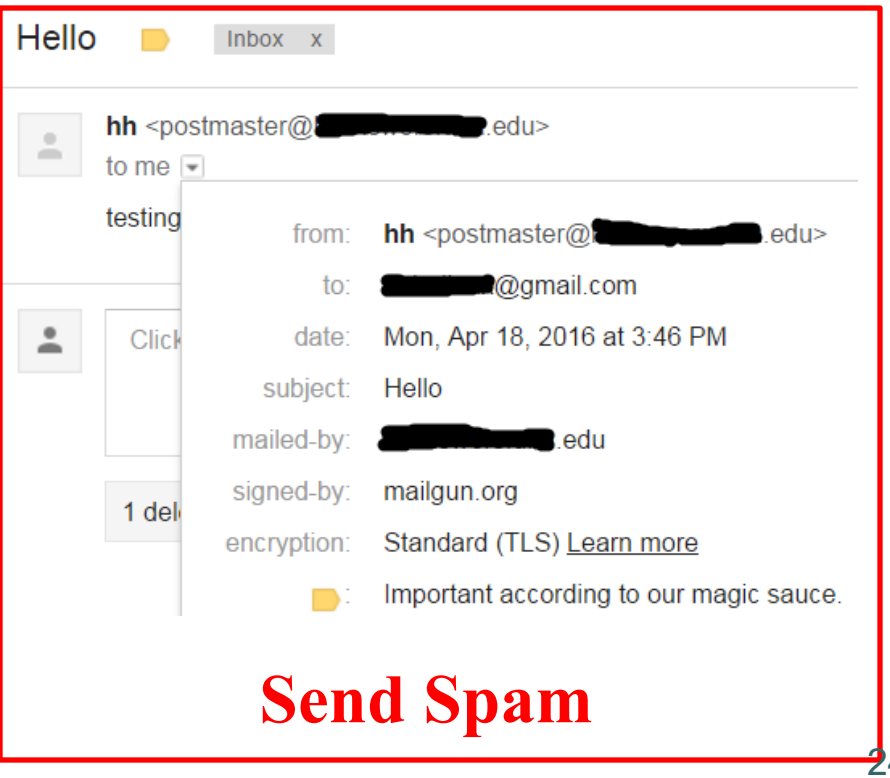
- **Open-looped**



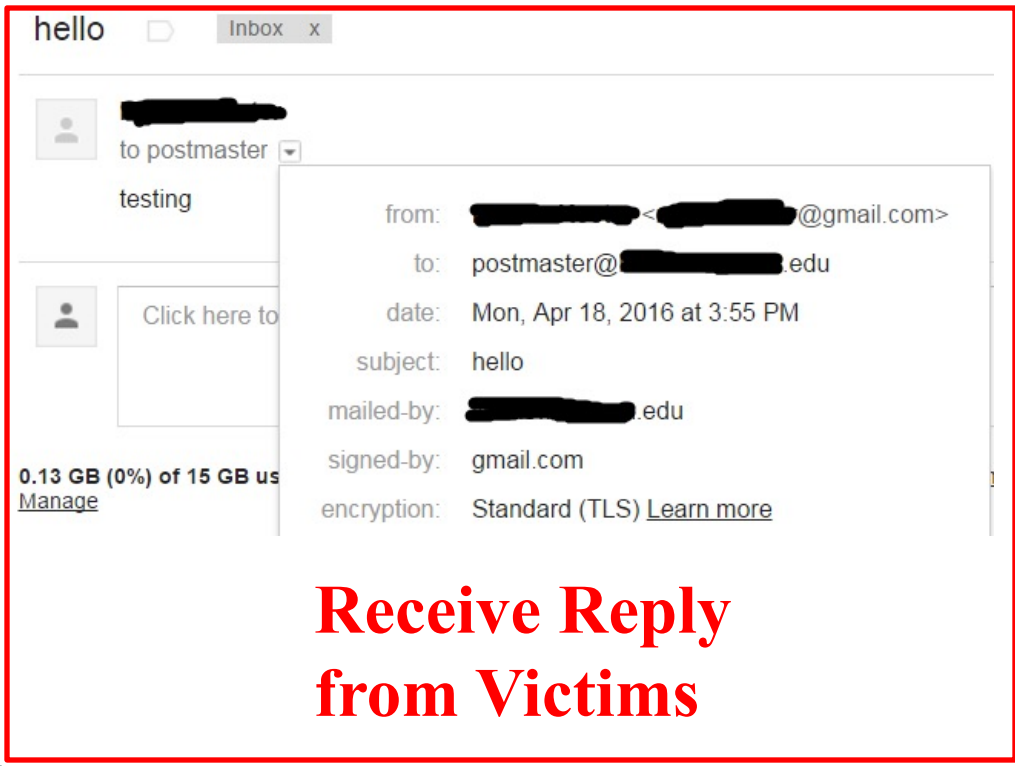
Threat Analysis -- Email Fraud

Use authentic mail servers

Make closed-loop attacks easy and pervasive



Send Spam



Receive Reply from Victims

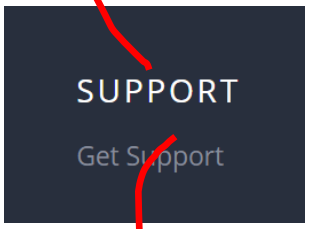
Threat Analysis -- Scamming & Phishing

Inherited trust from apex domains

dig

```
support.mediafire.com@ns-1179.awsdns-19.org.:
     support.mediafire.com. 86400 A 23.21.94.181
```

Check archive.org



www.mediafire.com/help/

email.netcombo.com.br

payment.statista.com

shop.1sale.com

jobs.zdbb.net

Mitigations

Authenticate ephemeral IP addresses

Break DNS resolution chain in third-party services

- **Isolate name space for each user**
- **Avoid wildcard DNS record**
- **Correctly handle CNAME redirection chains**

Check for expired domains

- **Continuously check at the time when a domain is about to expire**
- **Use tools like Alembic [S&P'16] to locate potential changes in domain ownership**

Notifications

We have notified all affected domains

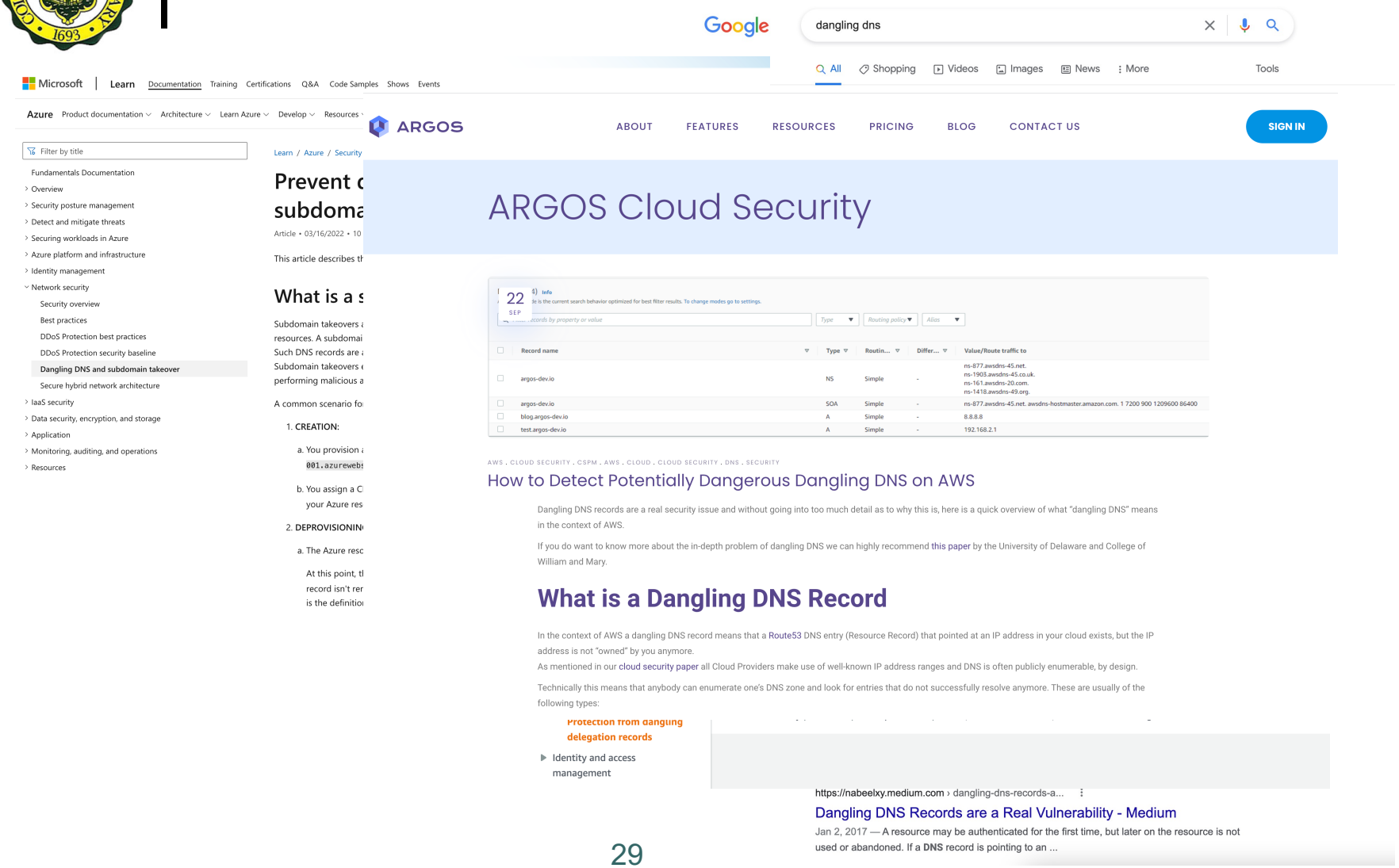
Response from about half of them

- **Most subdomains have acknowledged**
- **Only two thirds have taken action**
- **Most affected apex domains did not reply**

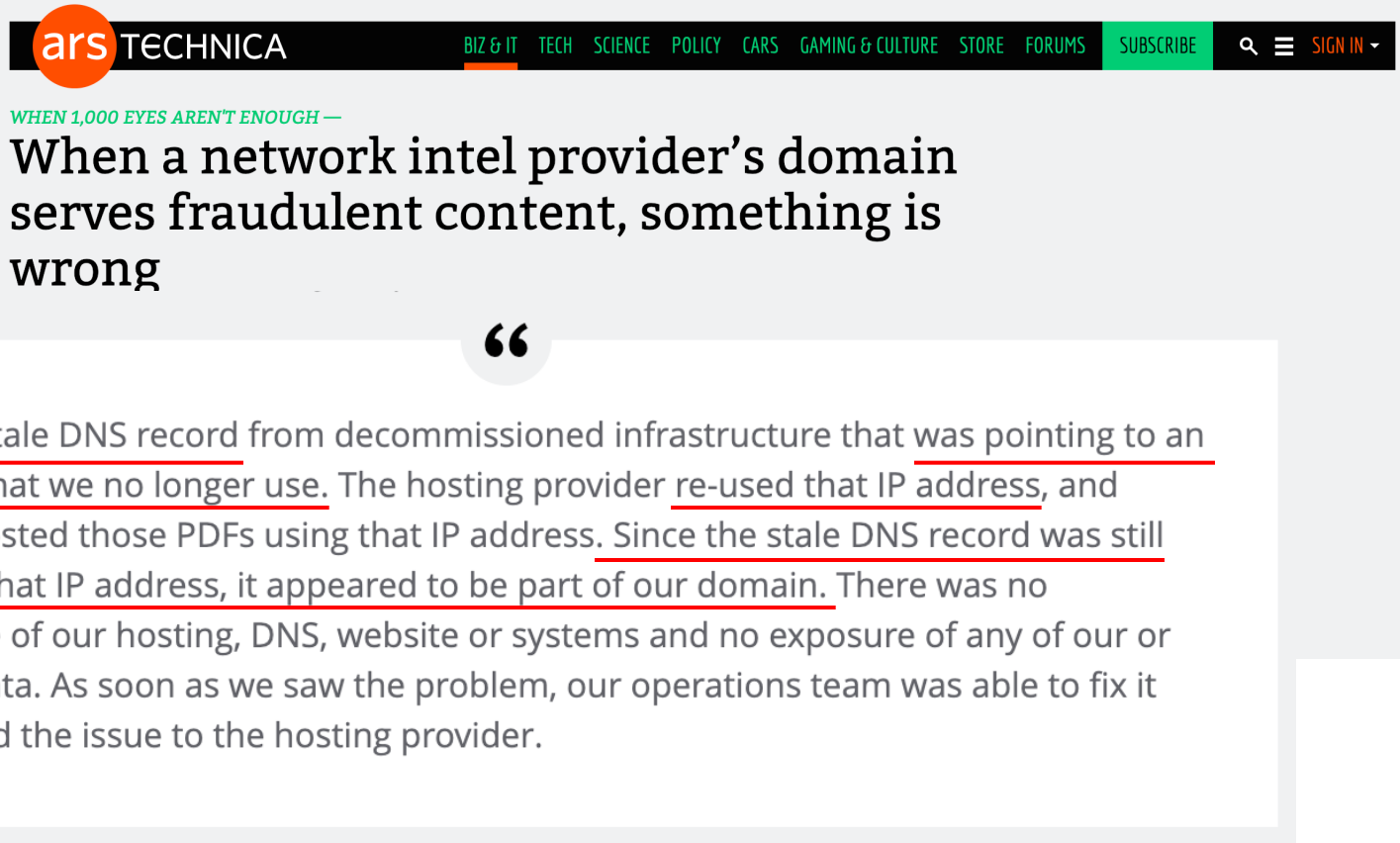
Conclusion

- ✓ **Dare is a serious and widespread security threat**
- ✓ **All three attack vectors are quite effective to exploit Dares**
- ✓ **Dares can notably enhance many forms of online fraud**
- ✓ **Three mechanisms are proposed to mitigate Dares with minor human effort**

Practical Impacts



Real-World Attacks



Thank You!

Questions?