



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

Daiping Liu, Shuai Hao, Haining Wang

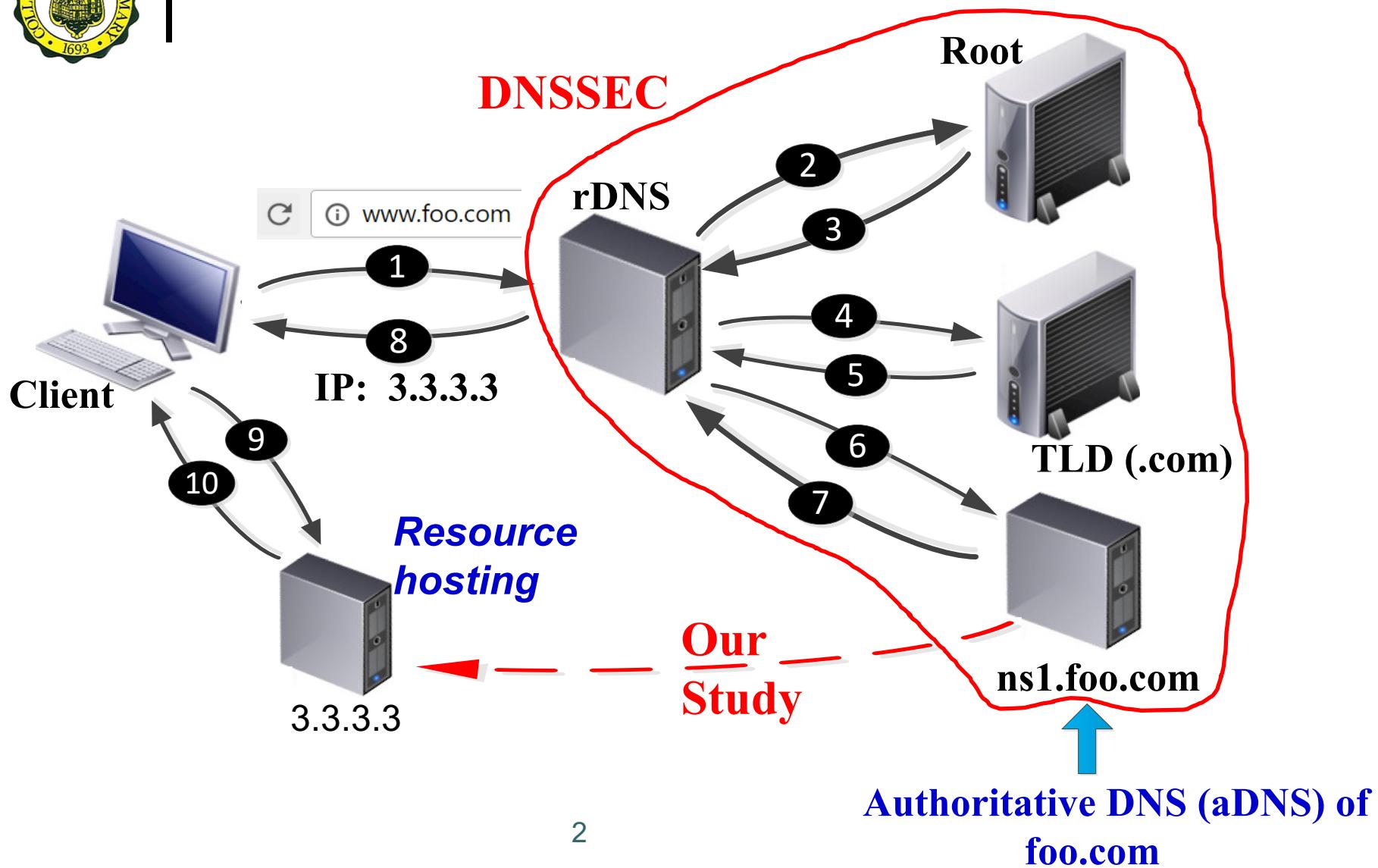
University of Delaware
College of William and Mary



Presenter: Shuai Hao, ODU
Sep. 2022



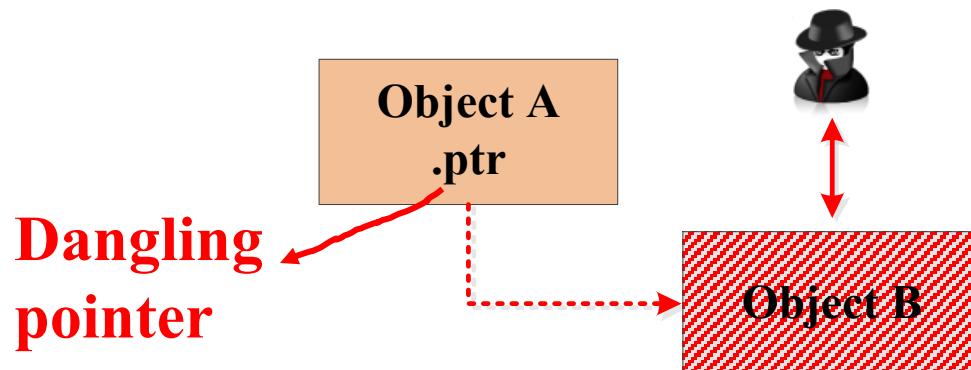
DNS Workflow



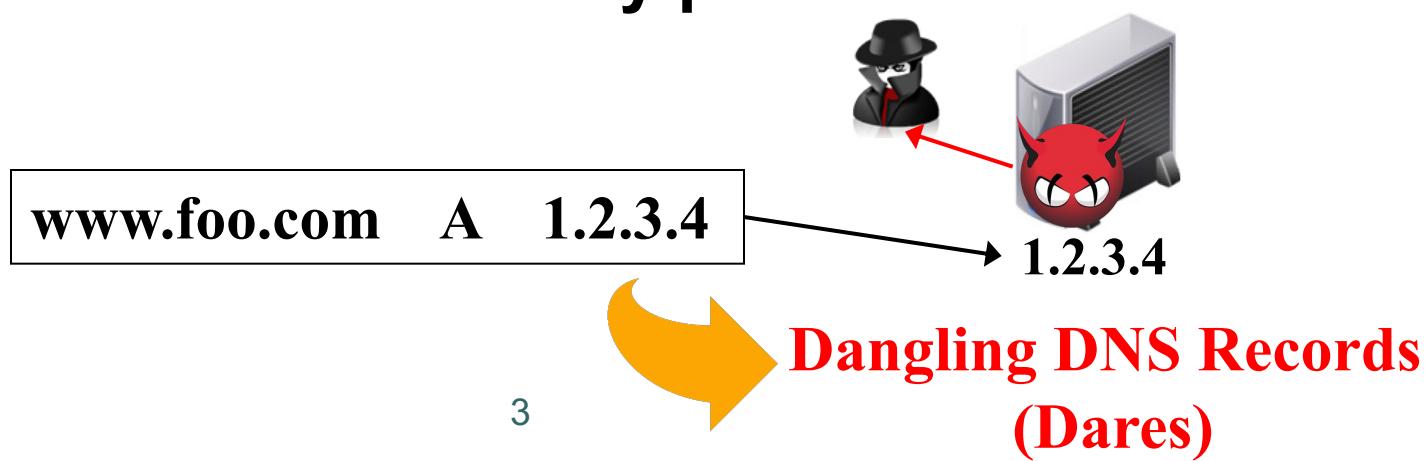


When Use-after-Free Meets DNS

Inspired by use-after-free vulnerabilities



DNS records are essentially pointers





Dangling DNS Records(Dare)

A DNS record $r := \langle name, TTL, class, type, data \rangle$ 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)

Dare-A

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

Canonical name

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

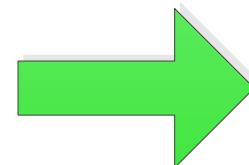
unexploitable



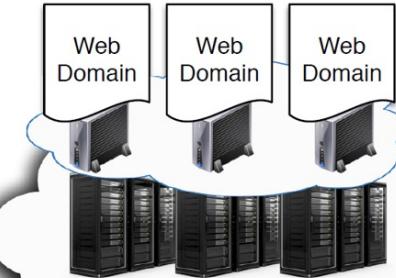
(a) Dedicated Domain Hosting



(b) Shared Domain Hosting



exploitable



(c) Cloud Domain Hosting

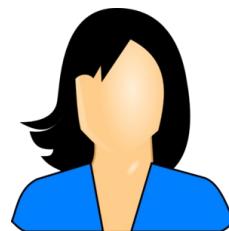




Attack Vector II

-- Abandoned Services

Modern websites extensively use third-party services



shop.alice.com

alice.myshopify.com

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 ~ 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



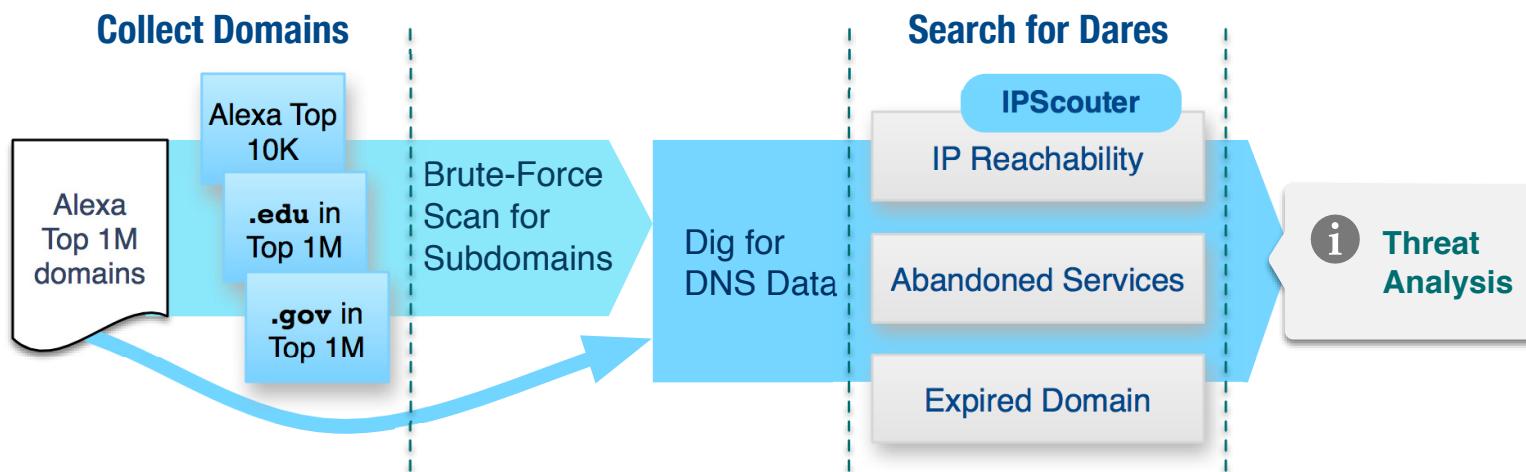
Measurement Study

-- Domain Collection

Apex Domains

- Choose popular ones

Dataset	Data Space
D	Unexpired apex domains in Alexa top 1M during 2010 ~ 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

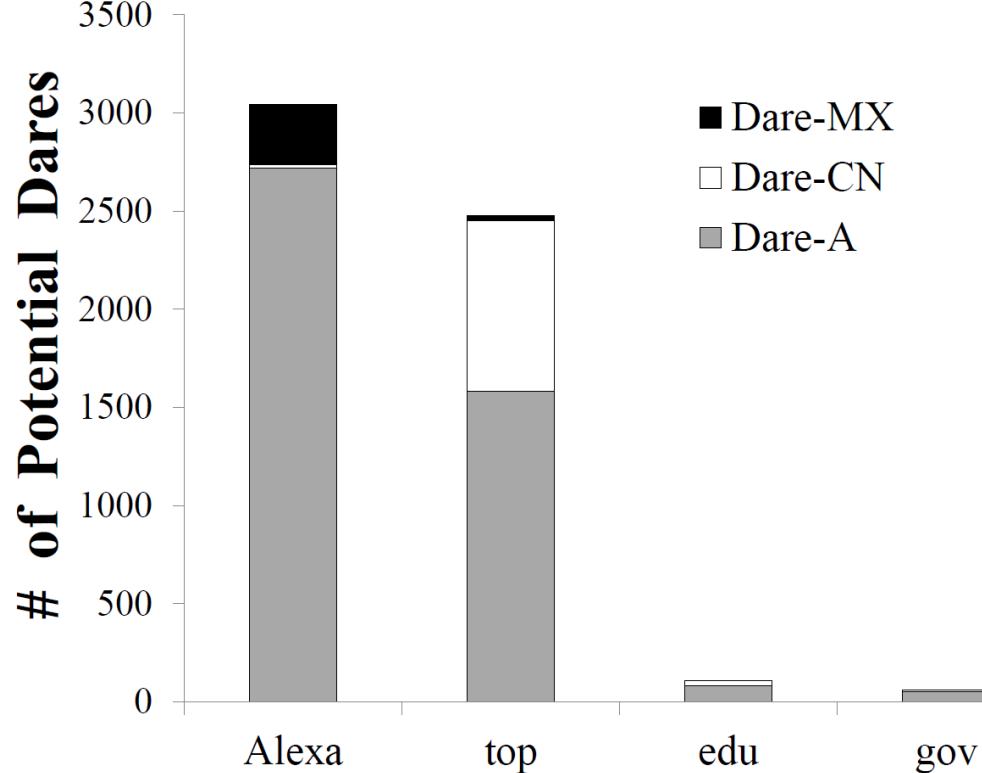
What is the potential magnitude of Dares in the wild?

- 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

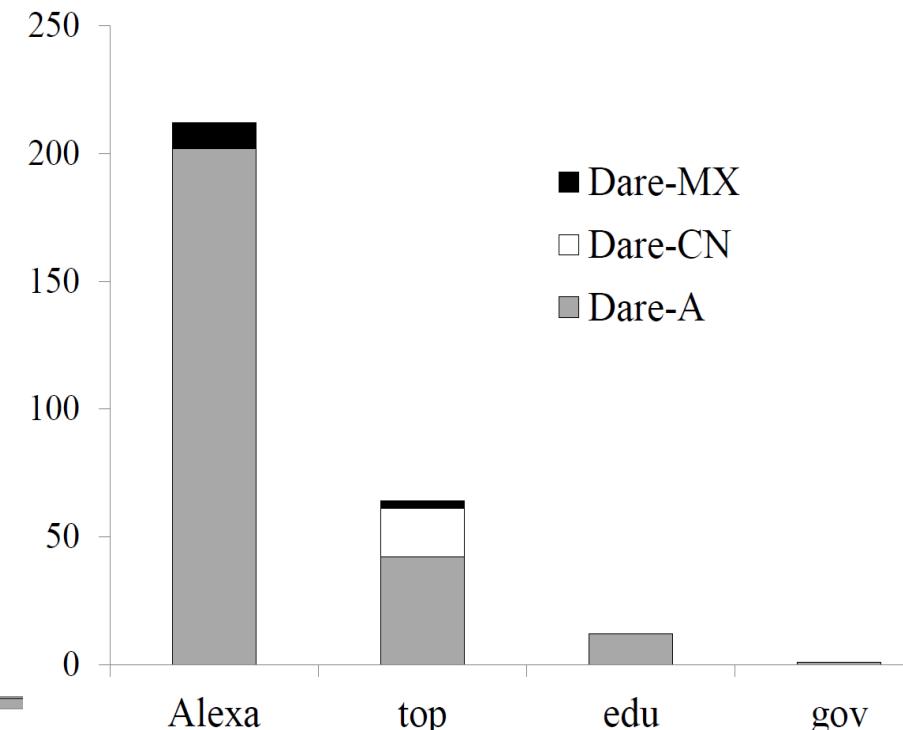


Measurement Study

-- IP in Cloud



(a) Amazon EC2



(b) Microsoft Azure



Measurement Study -- IP in Cloud

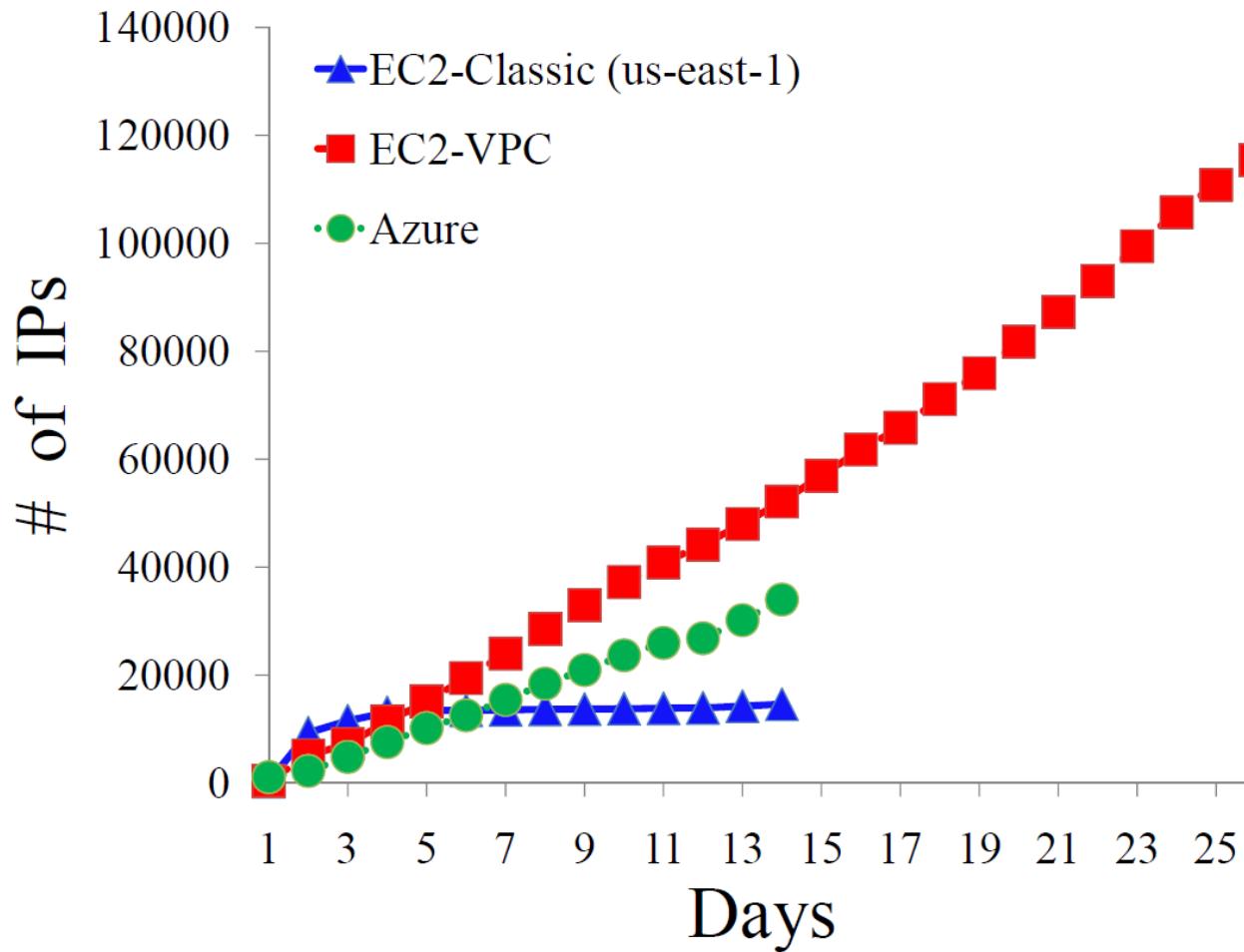
How practical an attacker can obtain a desired IP?

- 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):

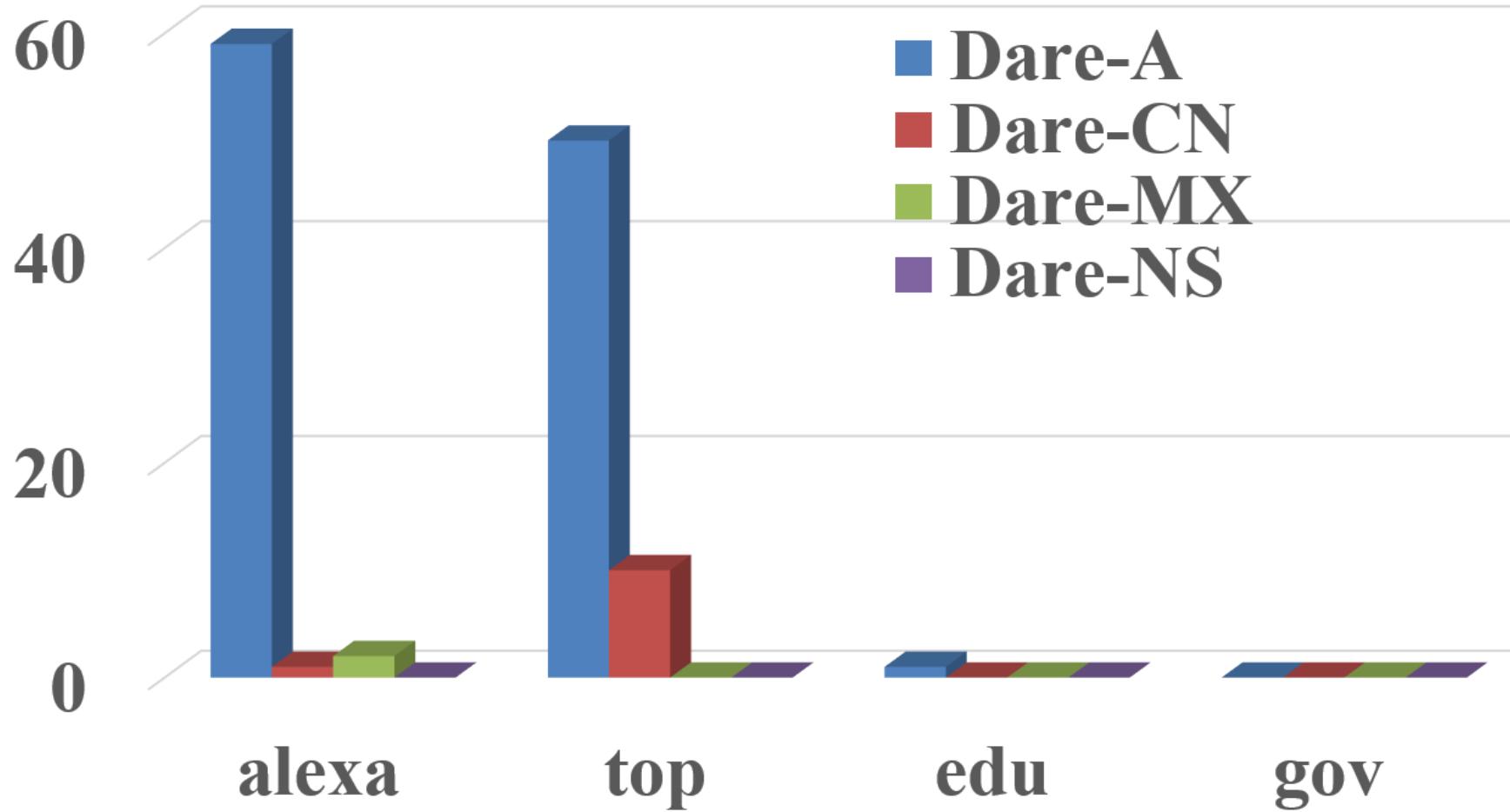
4,300 requests

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

Dares ?

Selenium



8 non-email services
1 email service

- Free account
- Don't verify ownership claim



Measurement Study -- Abandoned Services

www2.opensky.com@ns-1448.awsdns-53.org.:80

www2.opensky.com. CNAME blog.opensky.com.

blog.opensky.com. CNAME openskymerchants.wordpress.com.



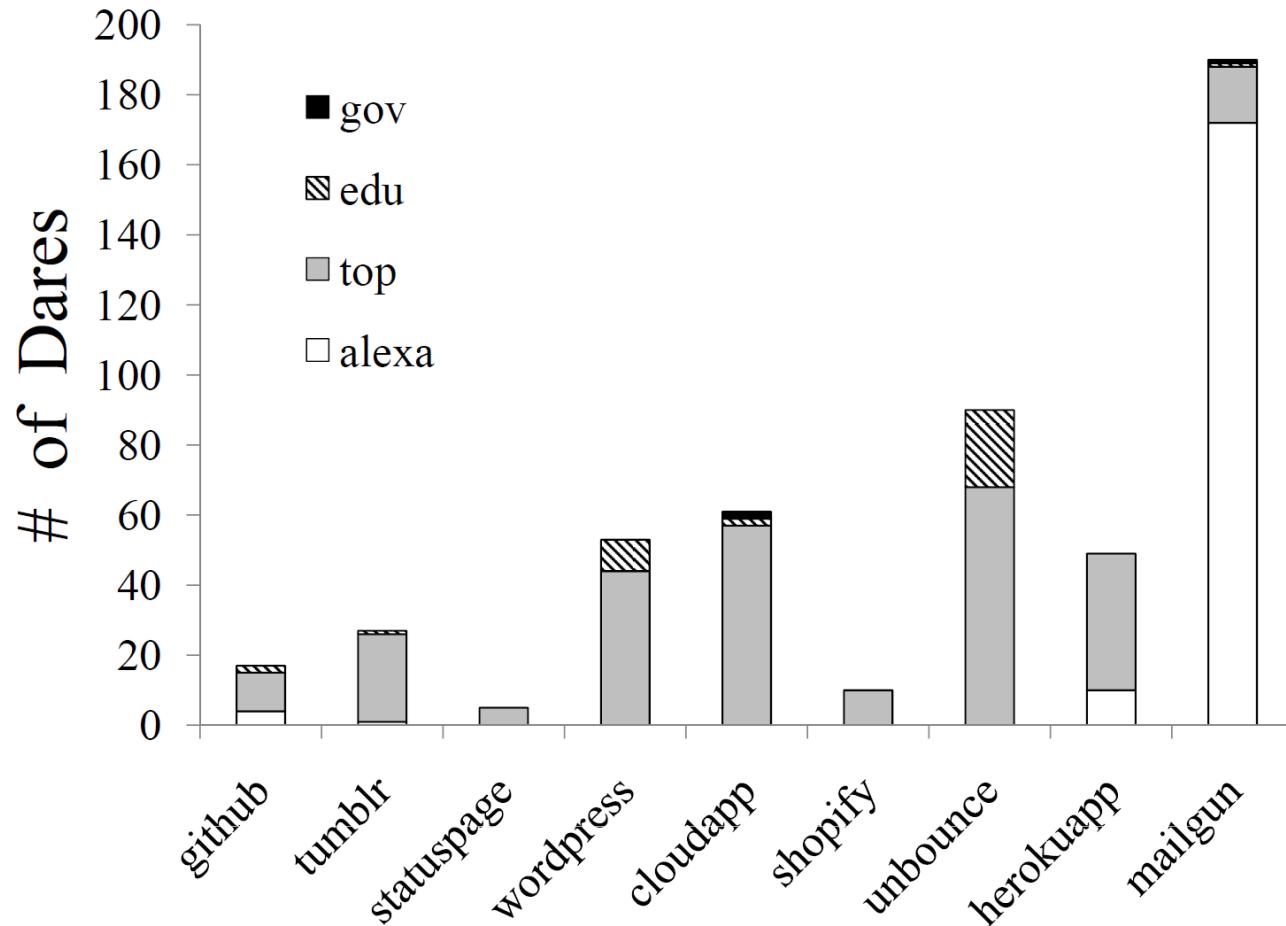
Nothing Found

It seems we can't find what you're looking for. Perhaps searching can help.



Measurement Study

-- Abandoned Services

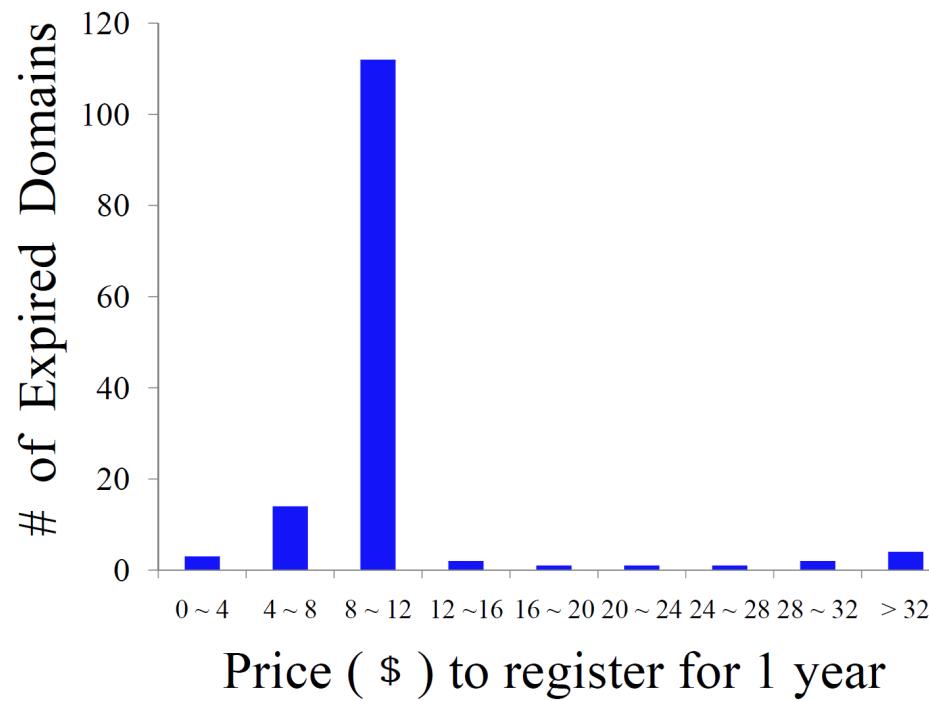




Measurement Study -- Expired Domains

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%**



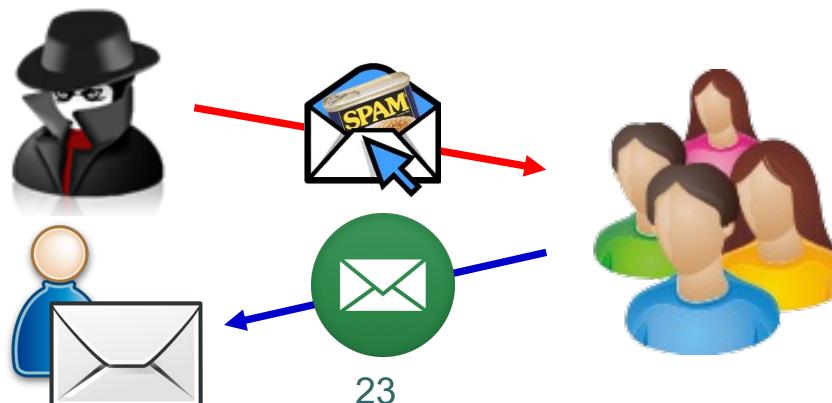
Threat Analysis

-- 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

The screenshot shows an email inbox with one message. The message is from "hh <postmaster@[REDACTED].edu>" to the user. The subject is "testing". The message body contains the text "Hello", "from: hh <postmaster@[REDACTED].edu>", "to: [REDACTED]@gmail.com", "date: Mon, Apr 18, 2016 at 3:46 PM", "subject: Hello", "mailed-by: [REDACTED].edu", "signed-by: mailgun.org", "encryption: Standard (TLS) [Learn more](#)", and a note that it is "Important according to our magic sauce."

Send Spam

Make closed-loop attacks
easy and pervasive

The screenshot shows an email inbox with one message. The message is from the user to "postmaster@[REDACTED].edu". The subject is "hello". The message body contains the text "from: [REDACTED]<[REDACTED]@gmail.com>", "to: postmaster@[REDACTED].edu", "date: Mon, Apr 18, 2016 at 3:55 PM", "subject: hello", "mailed-by: [REDACTED].edu", "signed-by: gmail.com", and "encryption: Standard (TLS) [Learn more](#)". A note at the bottom left says "0.13 GB (0%) of 15 GB used" and "Manage".

Receive Reply
from Victims



Threat Analysis

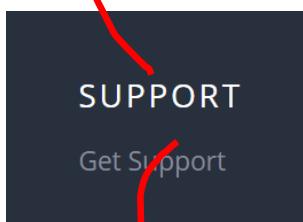
-- Scamming & Phishing

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



email.netcombo.com.br

payment.statista.com

shop.lsale.com

jobs.zdbb.net

www.mediafire.com/help/



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

Microsoft | Learn Documentation Training Certifications Q&A Code Samples Shows Events

Google dangling dns

Azure Product documentation Architecture Learn Azure Develop Resources

ABOUT FEATURES RESOURCES PRICING BLOG CONTACT US SIGN IN

Prevent cloud security subdomain takeover

Article • 03/16/2022 • 10

This article describes th

What is a subdomain takeover?

Subdomain takeovers involve malicious actors intercepting traffic intended for your organization's subdomains. A subdomain is a part of a domain name, such as DNS records for www.example.com. Subdomain takeovers can occur when a malicious actor performs a DNS poisoning attack or takes over a legitimate subdomain registration.

A common scenario for subdomain takeovers is when an attacker creates a new subdomain (e.g., blog.example.com) and points it to their own server, bypassing the organization's official website. This can lead to various security issues, such as phishing attacks or data theft.

1. CREATION:

- You provision a new subdomain, such as `001.azurewebsites.net`.
- You assign a CNAME record to your Azure resources.

2. DEPROVISIONING:

- The Azure resource is deleted.

At this point, the IP address associated with the record isn't longer valid, as the definition of a record is now pointing to a different IP address.

22 4 info It is the current search behavior optimized for best filter results. To change modes go to settings.

Record name	Type	Routing policy	Value/Route traffic to
argos-dev.io	NS	Simple	ns-877.awsdns-45.net. ns-1903.awsdns-45.co.uk. ns-161.awsdns-20.com. ns-1418.awsdns-49.org.
argos-dev.io	SOA	Simple	ns-877.awsdns-45.net.awsdns-hostmaster.amazon.com. 17200 900 1209600 86400
blog.argos-dev.io	A	Simple	8.8.8
test.argos-dev.io	A	Simple	192.168.2.1

AWS, CLOUD SECURITY, CSPM, AWS, CLOUD, CLOUD SECURITY, DNS, SECURITY

How to Detect Potentially Dangerous Dangling DNS on AWS

Dangling DNS records are a real security issue and without going into too much detail as to why this is, here is a quick overview of what "dangling DNS" means in the context of AWS.

If you do want to know more about the in-depth problem of dangling DNS we can highly recommend [this paper](#) by the University of Delaware and College of William and Mary.

What is a Dangling DNS Record

In the context of AWS a dangling DNS record means that a Route53 DNS entry (Resource Record) that pointed at an IP address in your cloud exists, but the IP address is not "owned" by you anymore.

As mentioned in our [cloud security paper](#) all Cloud Providers make use of well-known IP address ranges and DNS is often publicly enumerable, by design.

Technically this means that anybody can enumerate one's DNS zone and look for entries that do not successfully resolve anymore. These are usually of the following types:

- PROTECTION FROM DANGLING DELEGATION RECORDS
- Identity and access management

<https://nabeeley.medium.com/dangling-dns-records-a...>

Dangling DNS Records are a Real Vulnerability - Medium

Jan 2, 2017 — A resource may be authenticated for the first time, but later on the resource is not used or abandoned. If a DNS record is pointing to an ...



Real-World Attacks



ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE FORUMS SUBSCRIBE

SEARCH SIGN IN ▾

WHEN 1,000 EYES AREN'T ENOUGH —

When a network intel provider's domain serves fraudulent content, something is wrong

“

This was a stale DNS record from decommissioned infrastructure that was pointing to an IP address that we no longer use. The hosting provider re-used that IP address, and someone hosted those PDFs using that IP address. Since the stale DNS record was still pointing at that IP address, it appeared to be part of our domain. There was no compromise of our hosting, DNS, website or systems and no exposure of any of our or customer data. As soon as we saw the problem, our operations team was able to fix it and reported the issue to the hosting provider.



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

Thank You!

Questions?

