From Dangling DNS to Cloud Takeover

`and what to do about it…`

$ whoami

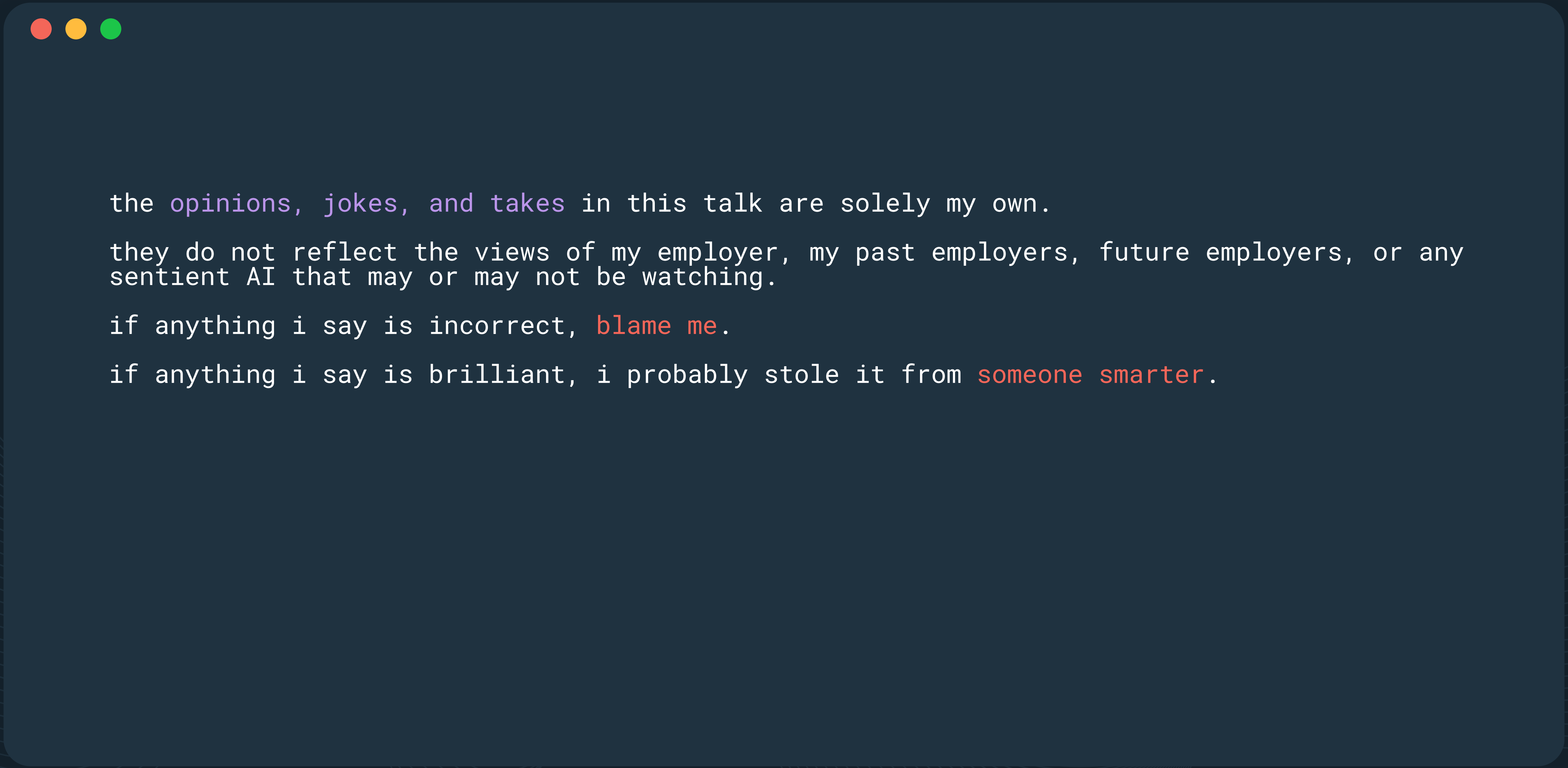
nathan getty.

security engineer @ menlo security

nategetty on discord

getsec on github

```
$ uptime

  -   cloud security    @ skip (jet)
  -   security analyst @ wawanesa
  -   service desk      @ wawanesa
  -   rrc ccna/ccnp
```



the opinions, jokes, and takes in this talk are solely my own.

they do not reflect the views of my employer, my past employers, future employers, or any sentient AI that may or may not be watching.

if anything i say is incorrect, blame me.

if anything i say is brilliant, i probably stole it from someone smarter.

toc...

01

the problem

02

who it affects most

03

what can you do

04

what we did

05

demo

06

questions/comments

glossary and terms

cloud stuffs

- route53
- lambda
- ec2
- alb/elb
- acm
- iam

general stuffs

- dns
- iac
- terraform
- grc
- “dangling dns”

01 The Problem

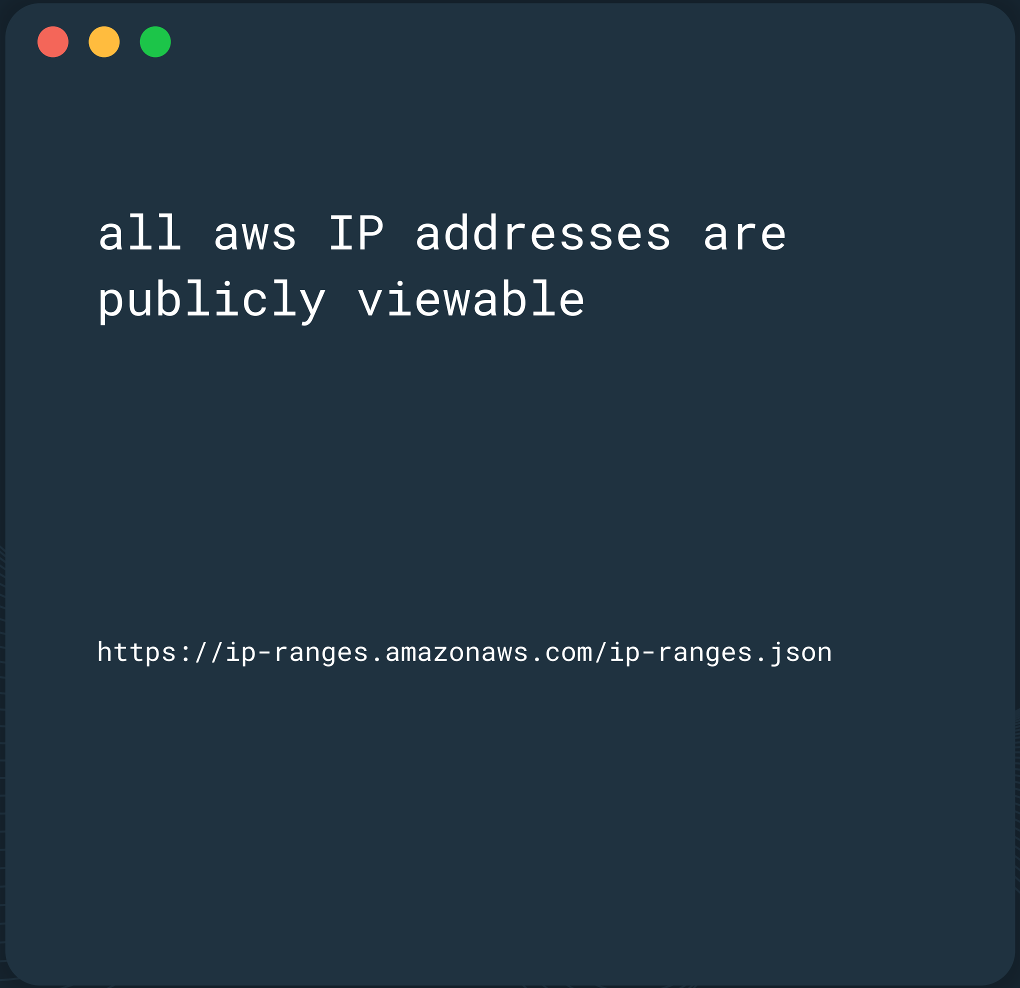
“Over the past year, a 20% increase was seen in domain takeovers. Out of the assets scanned – which includes apex domains and subdomains – 25% more vulnerabilities were seen in 2021 than in 2020.”

- helpnetsecurity.com, circa 2022

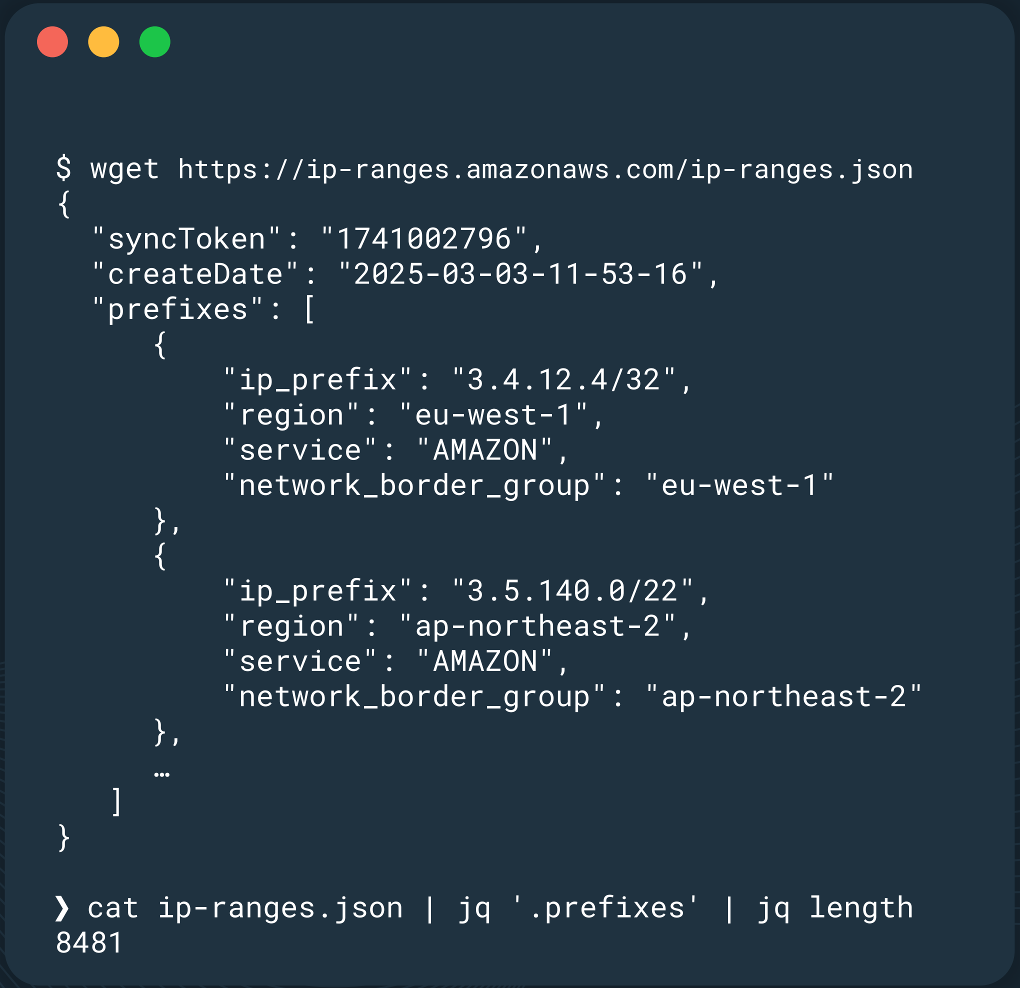
wtf is a subdomain takeover

your dns records pointing to hacker controlled resources

wait, resources out of my control...?

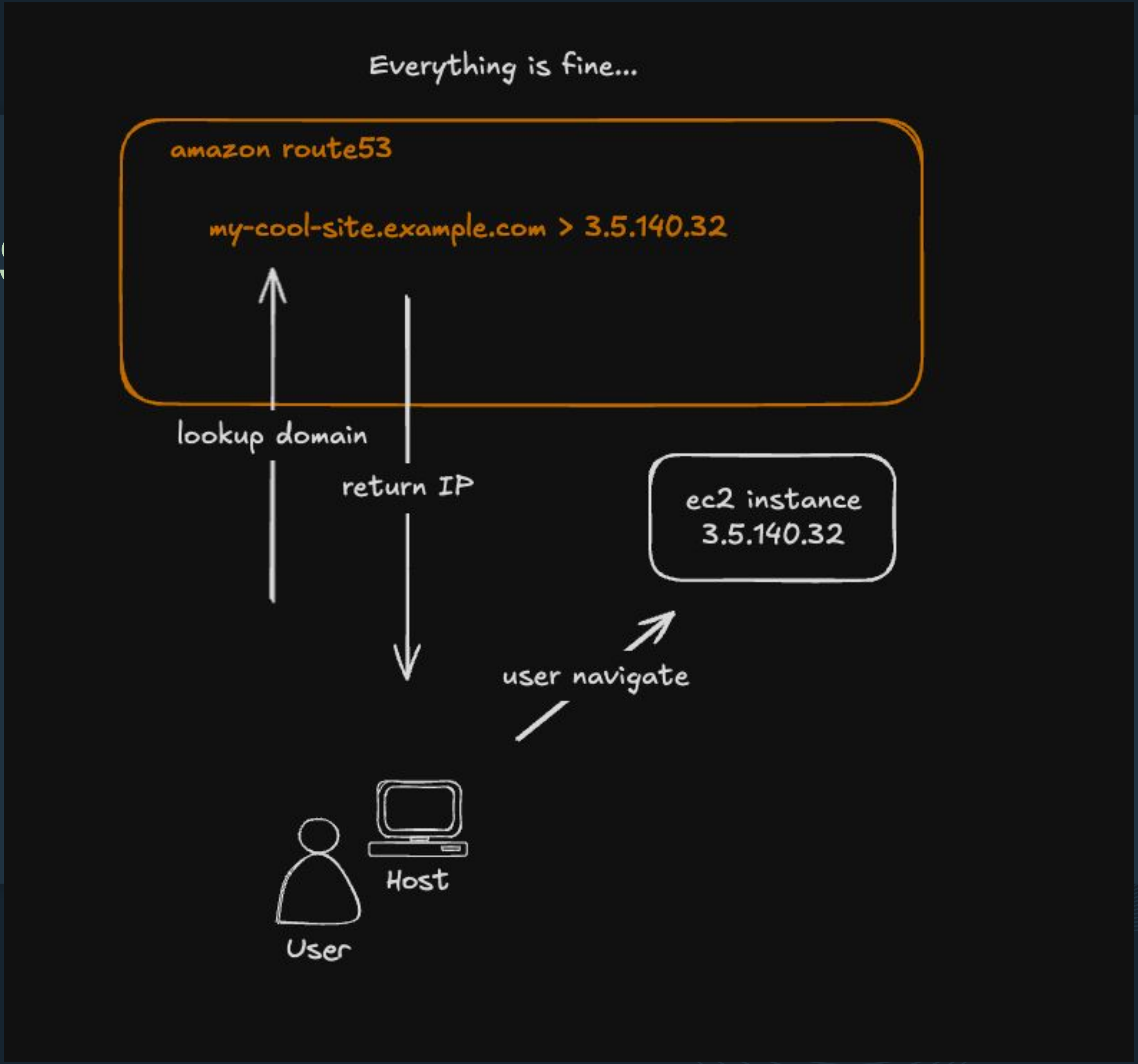


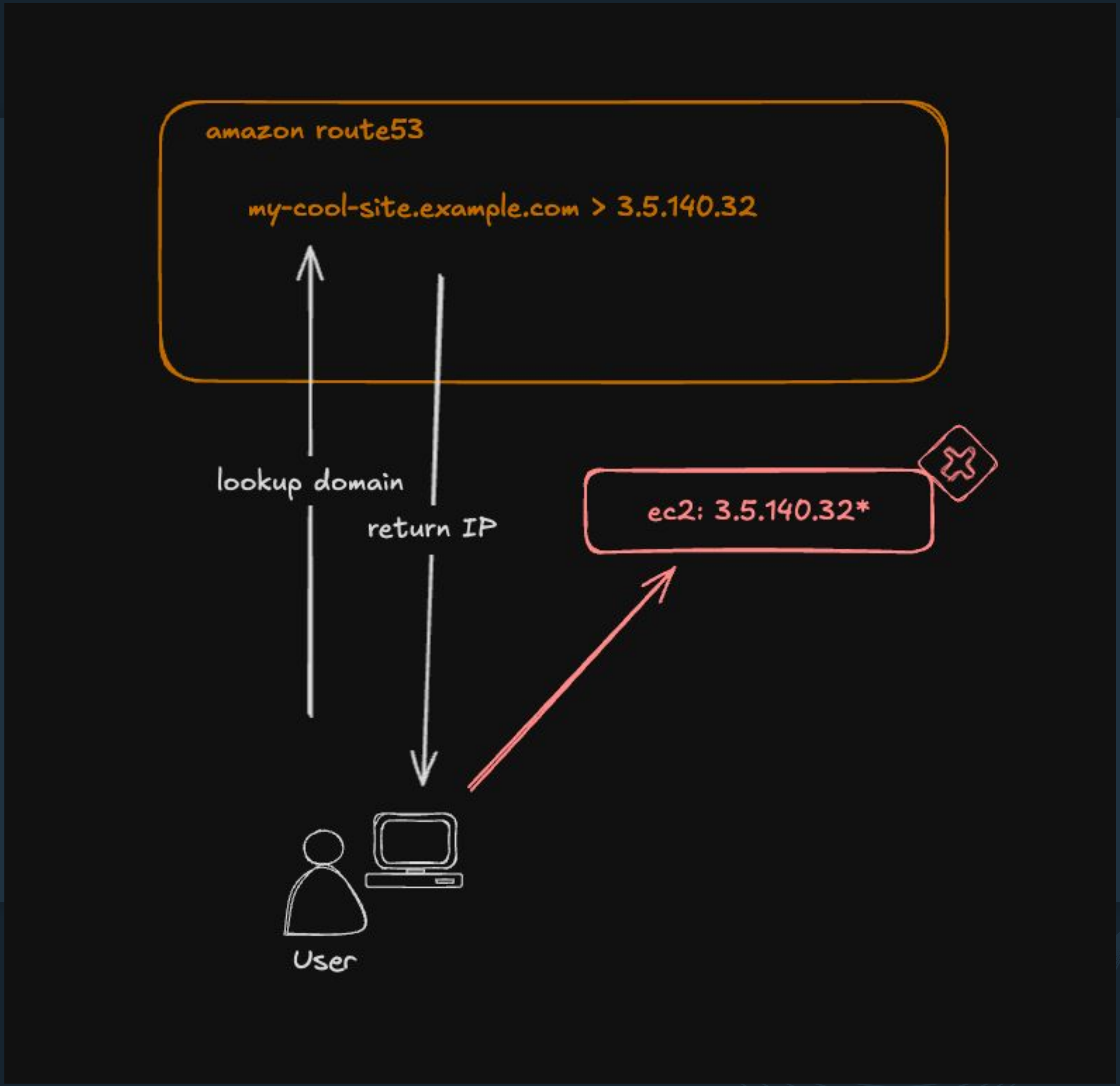
```
all aws IP addresses are
publicly viewable



https://ip-ranges.amazonaws.com/ip-ranges.json
```

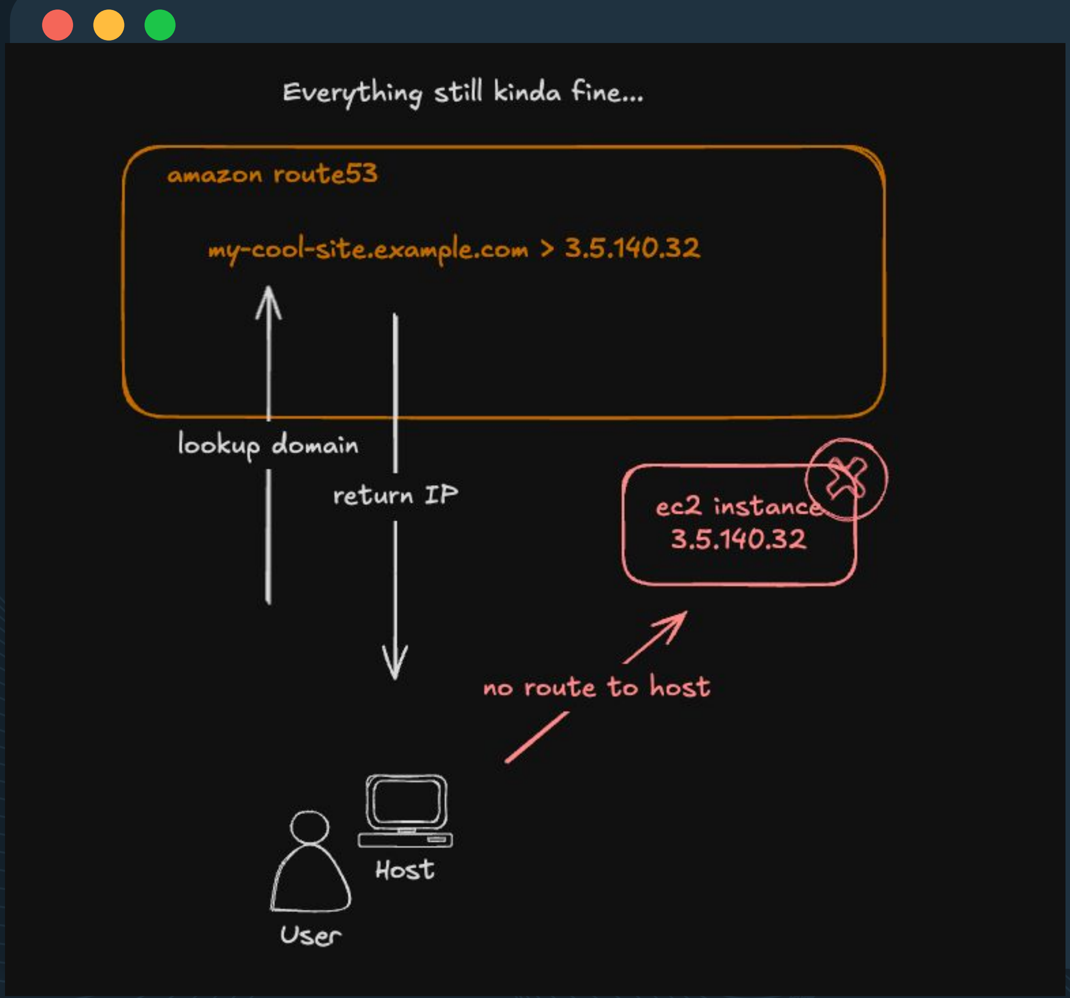


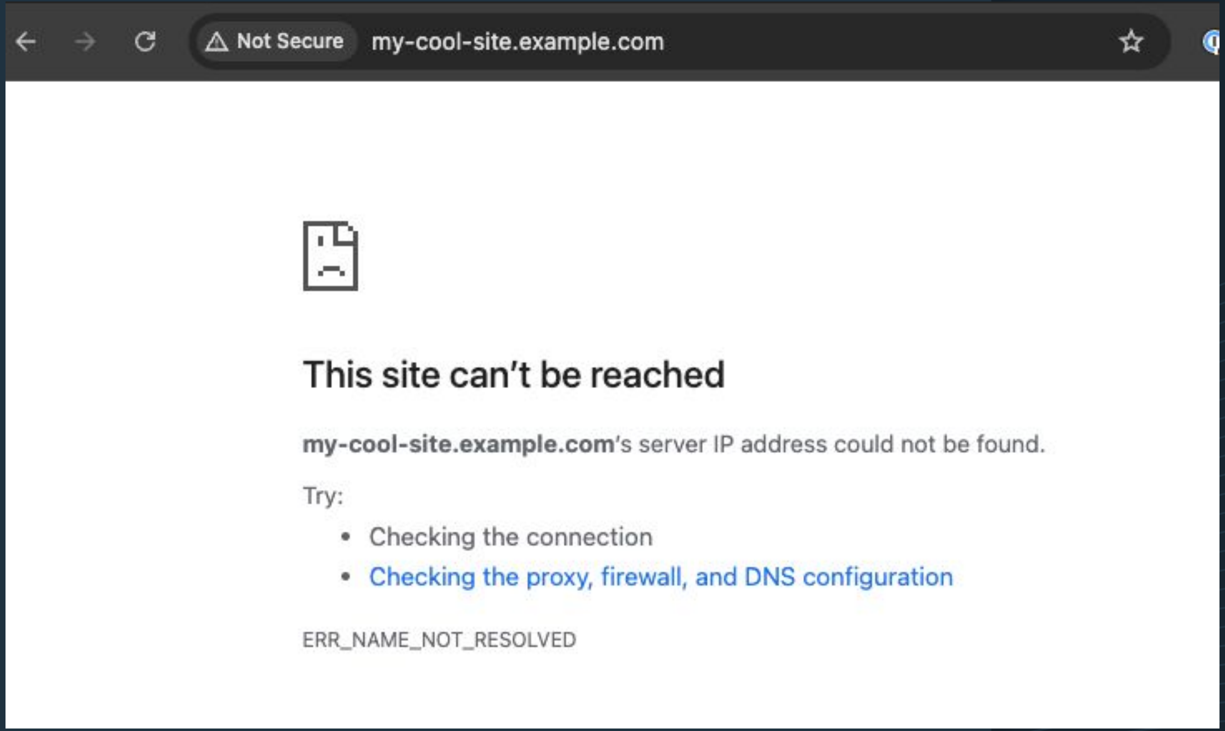
```
$ wget https://ip-ranges.amazonaws.com/ip-ranges.json
{
  "syncToken": "1741002796",
  "createDate": "2025-03-03-11-53-16",
  "prefixes": [
      {
          "ip_prefix": "3.4.12.4/32",
          "region": "eu-west-1",
          "service": "AMAZON",
          "network_border_group": "eu-west-1"
      },
      {
          "ip_prefix": "3.5.140.0/22",
          "region": "ap-northeast-2",
          "service": "AMAZON",
          "network_border_group": "ap-northeast-2"
      },
      …
   ]
}

❯ cat ip-ranges.json | jq '.prefixes' | jq length
8481
```

wtf i


Everything is fine...
amazon route53
my-cool-site.example.com > 3.5.140.32
lookup domain
return IP
ec2 instance
3.5.140.32
user navigate
Host
User


amazon route53
my-cool-site.example.com > 3.5.140.32
lookup domain
return IP
ec2: 3.5.140.32*
User





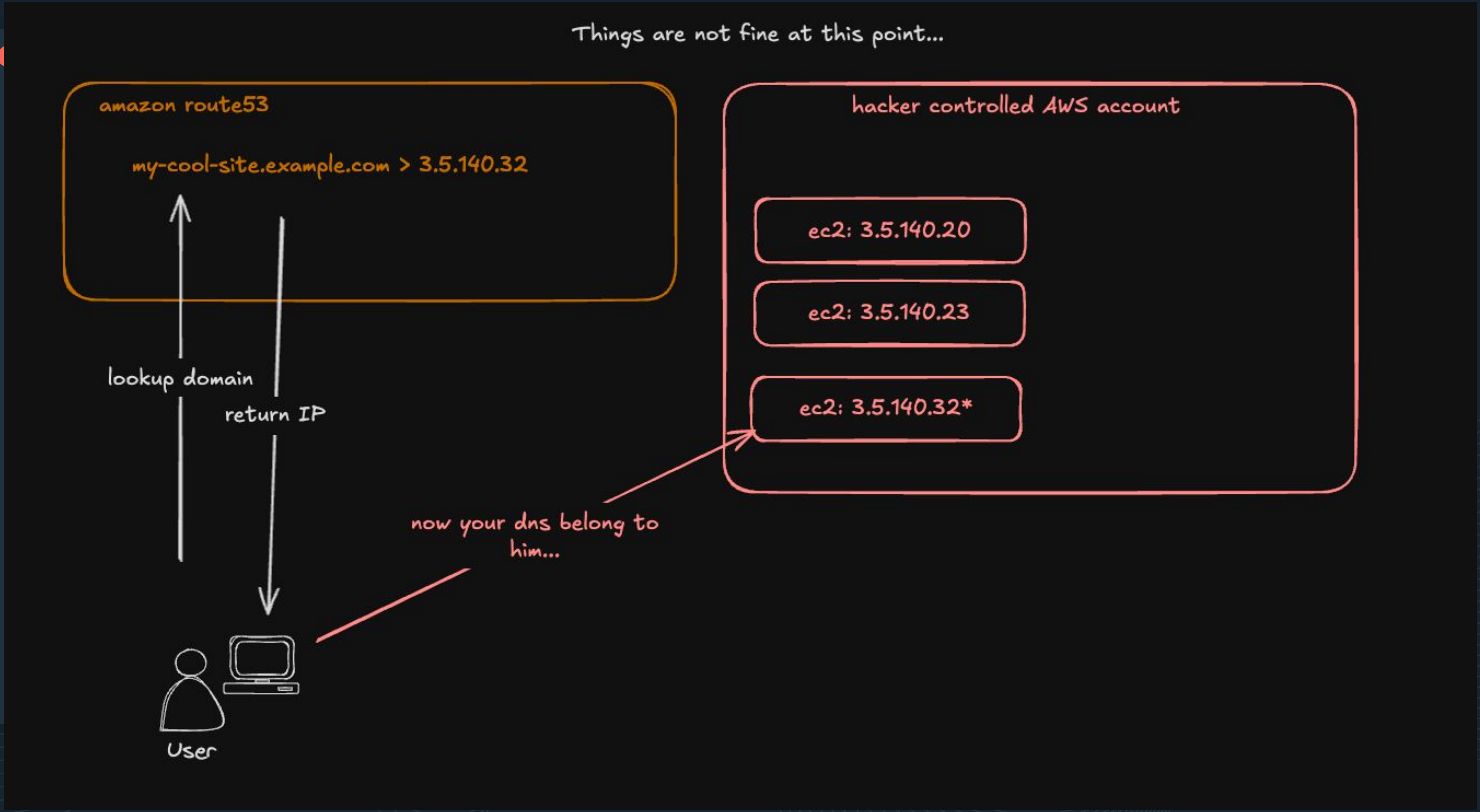
This site can’t be reached

my-cool-site.example.com’s server IP address could not be found.

Try:

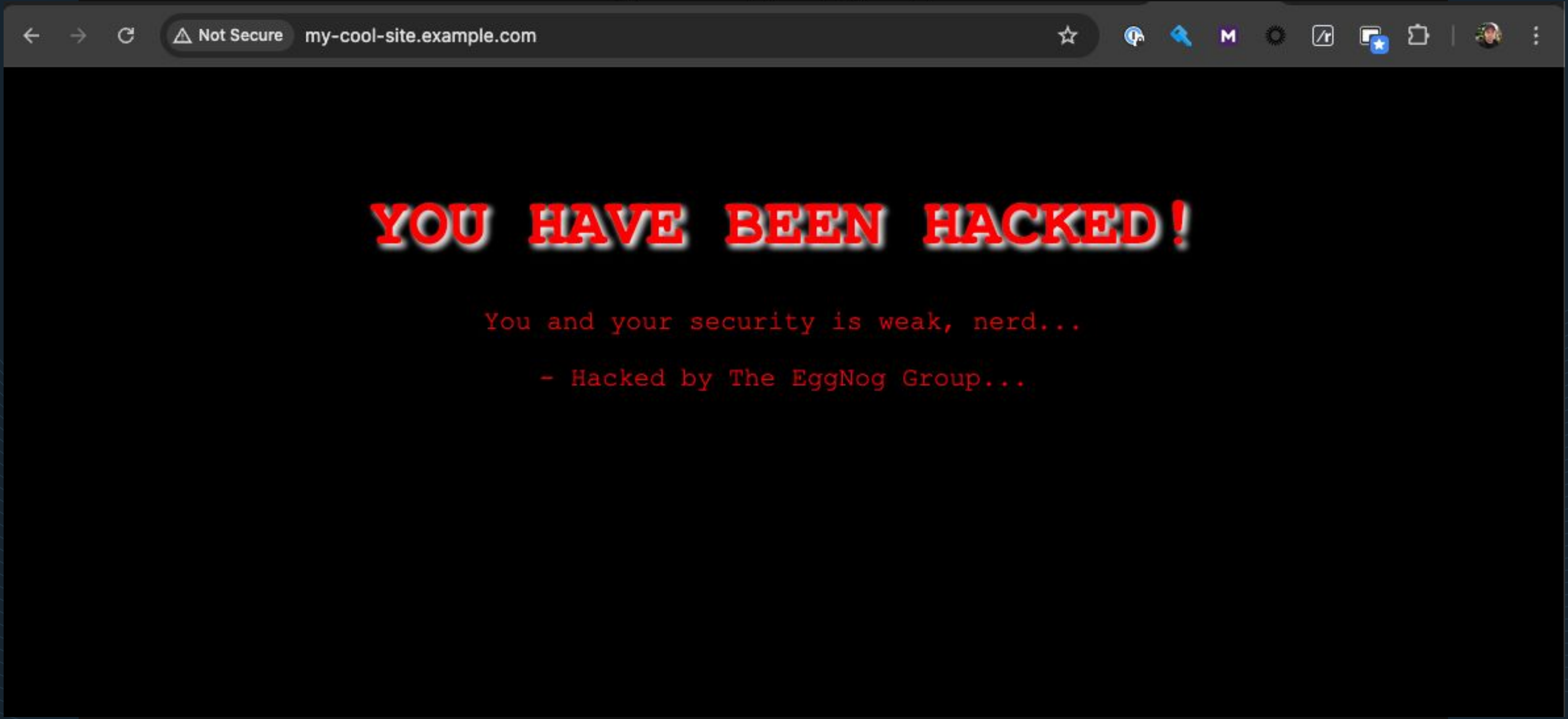
- Checking the connection
- Checking the proxy, firewall, and DNS configuration

ERR_NAME_NOT_RESOLVED



Things are not fine at this point...

amazon route53
my-cool-site.example.com > 3.5.140.32
lookup domain
return IP
User
now your dns belong to him...
hacker controlled AWS account
ec2: 3.5.140.20
ec2: 3.5.140.23
ec2: 3.5.140.32*

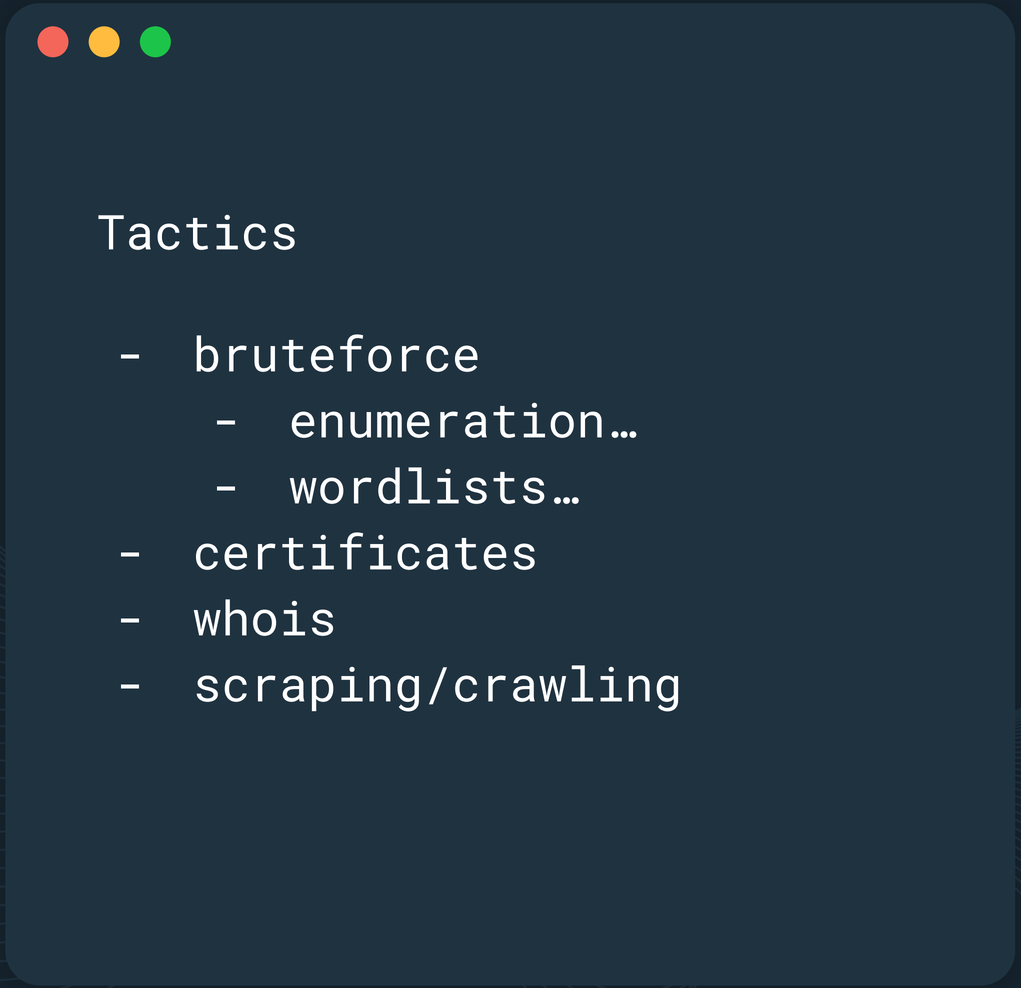


YOU HAVE BEEN HACKED!

You and your security is weak, nerd...

- Hacked by The EggNog Group...

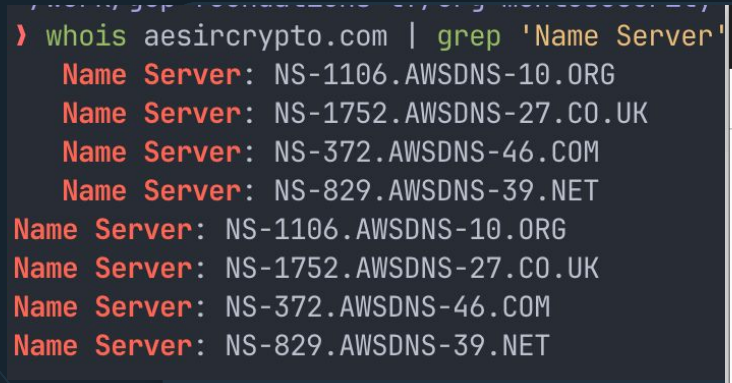
how to do this stuff…



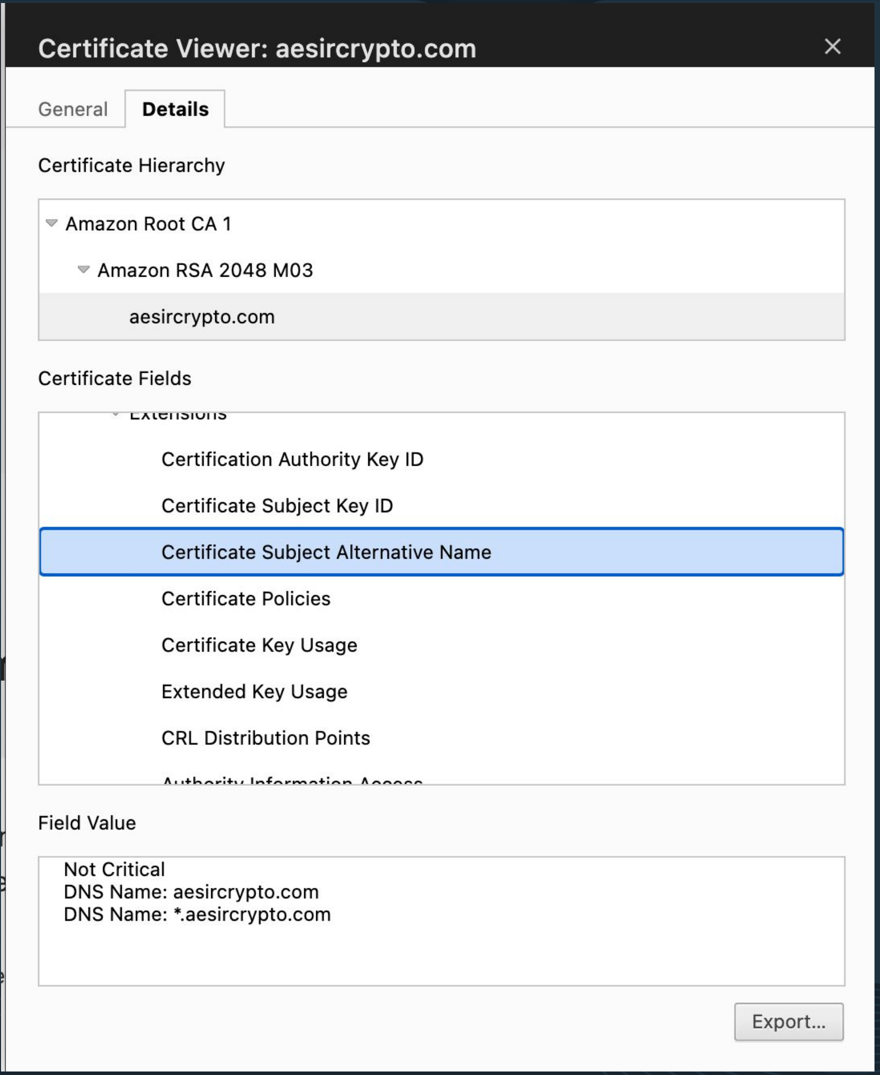
```
Tactics

 -  bruteforce
     -  enumeration…
     -  wordlists…
 -  certificates
 -  whois
 -  scraping/crawling
```

```
free tools
 -  owasp-amass/amass
 -  projectdiscovery/subfinder
 -  Josue87/gotator
 -  d3mondev/puredns
 -  initstring/cloud_enum

paid services
 -  shodan.io
 -  censys
 -  google attack surface management
    (prev. virus total / mandiant)
```

identification



```
❯ whois aesircrypto.com | grep 'Name Server'
   Name Server: NS-1106.AWSDNS-10.ORG
   Name Server: NS-1752.AWSDNS-27.CO.UK
   Name Server: NS-372.AWSDNS-46.COM
   Name Server: NS-829.AWSDNS-39.NET
Name Server: NS-1106.AWSDNS-10.ORG
Name Server: NS-1752.AWSDNS-27.CO.UK
Name Server: NS-372.AWSDNS-46.COM
Name Server: NS-829.AWSDNS-39.NET
```



Certificate Viewer: aesircrypto.com

Certificate Hierarchy

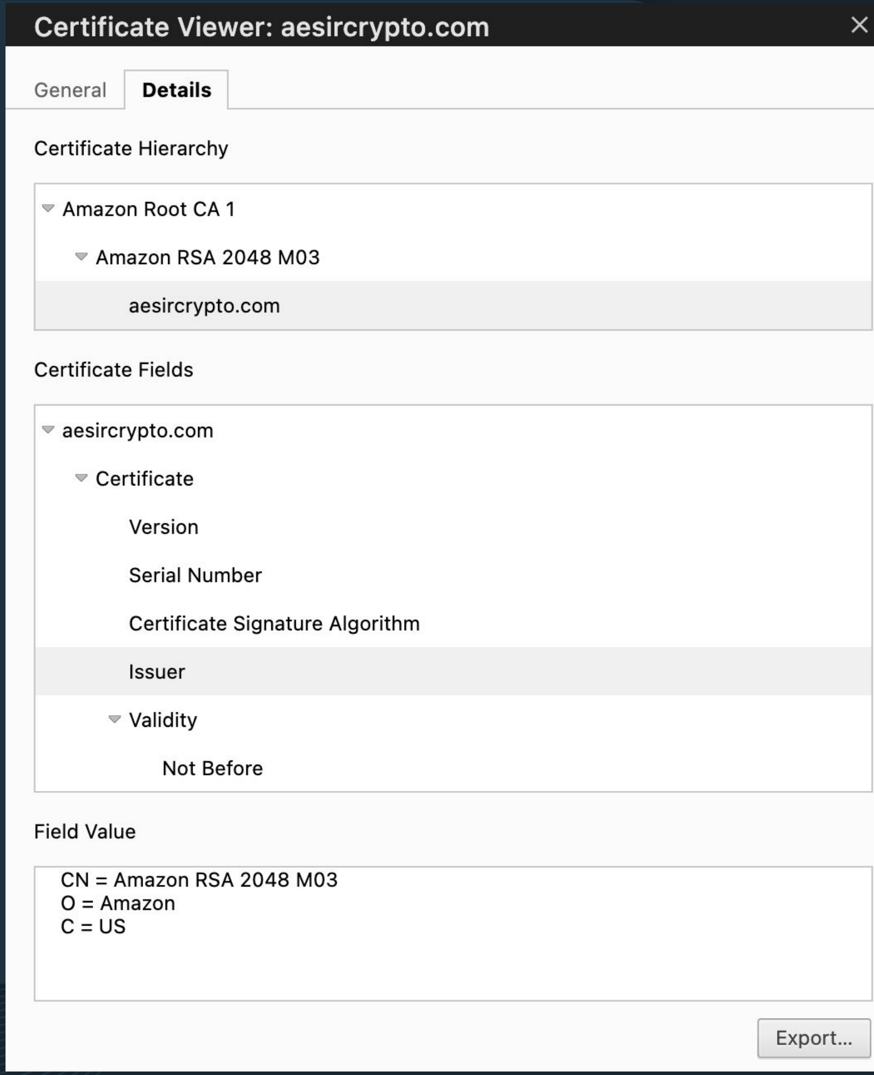
- Amazon Root CA 1
  - Amazon RSA 2048 M03
    - aesircrypto.com

Certificate Fields

- Extensions
  - Certification Authority Key ID
  - Certificate Subject Key ID
  - Certificate Subject Alternative Name
  - Certificate Policies
  - Certificate Key Usage
  - Extended Key Usage
  - CRL Distribution Points
  - Authority Information Access

Field Value

Not Critical
DNS Name: aesircrypto.com
DNS Name: *.aesircrypto.com



Certificate Viewer: aesircrypto.com

Certificate Hierarchy

- Amazon Root CA 1
  - Amazon RSA 2048 M03
    - aesircrypto.com

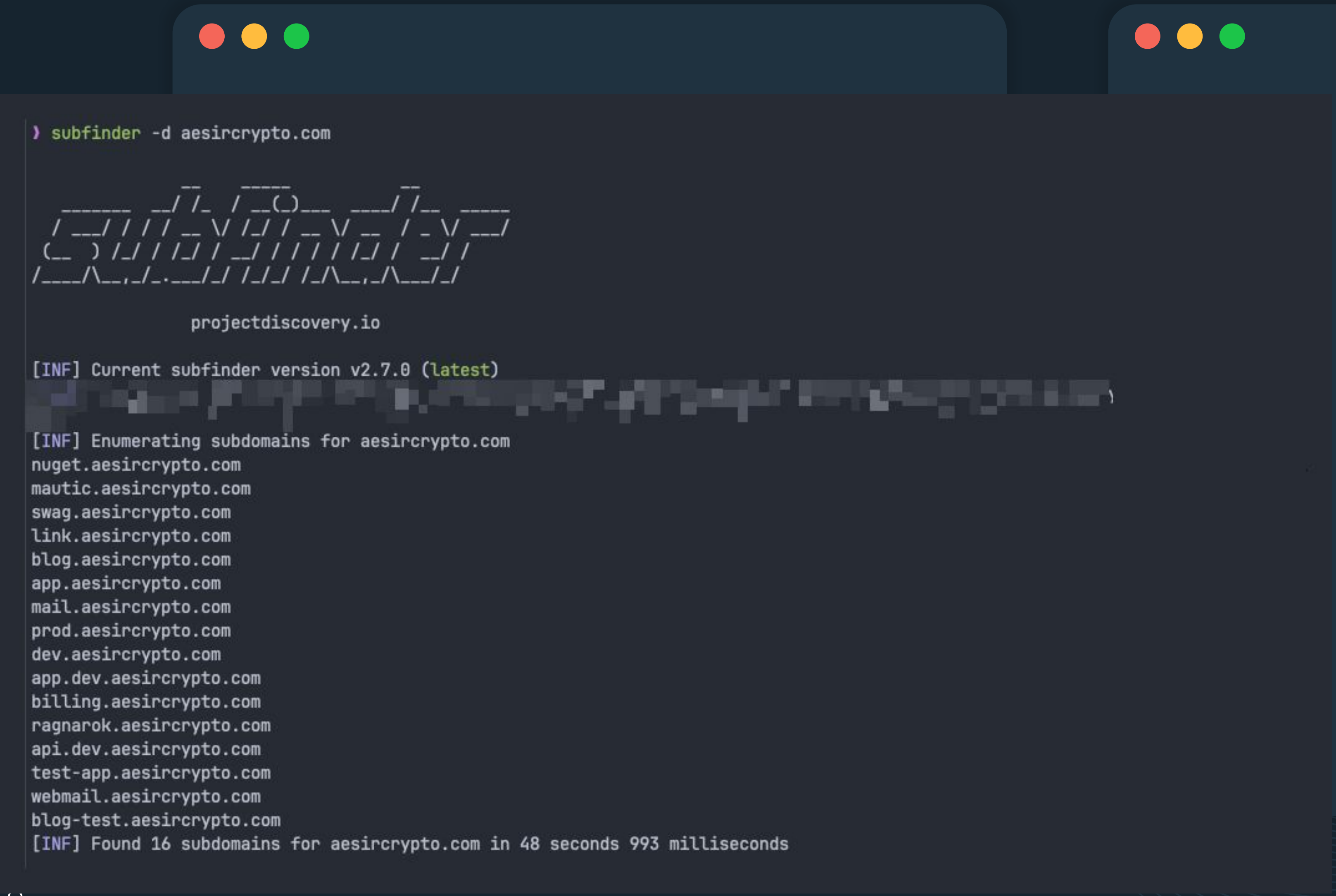
Certificate Fields

- aesircrypto.com
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before

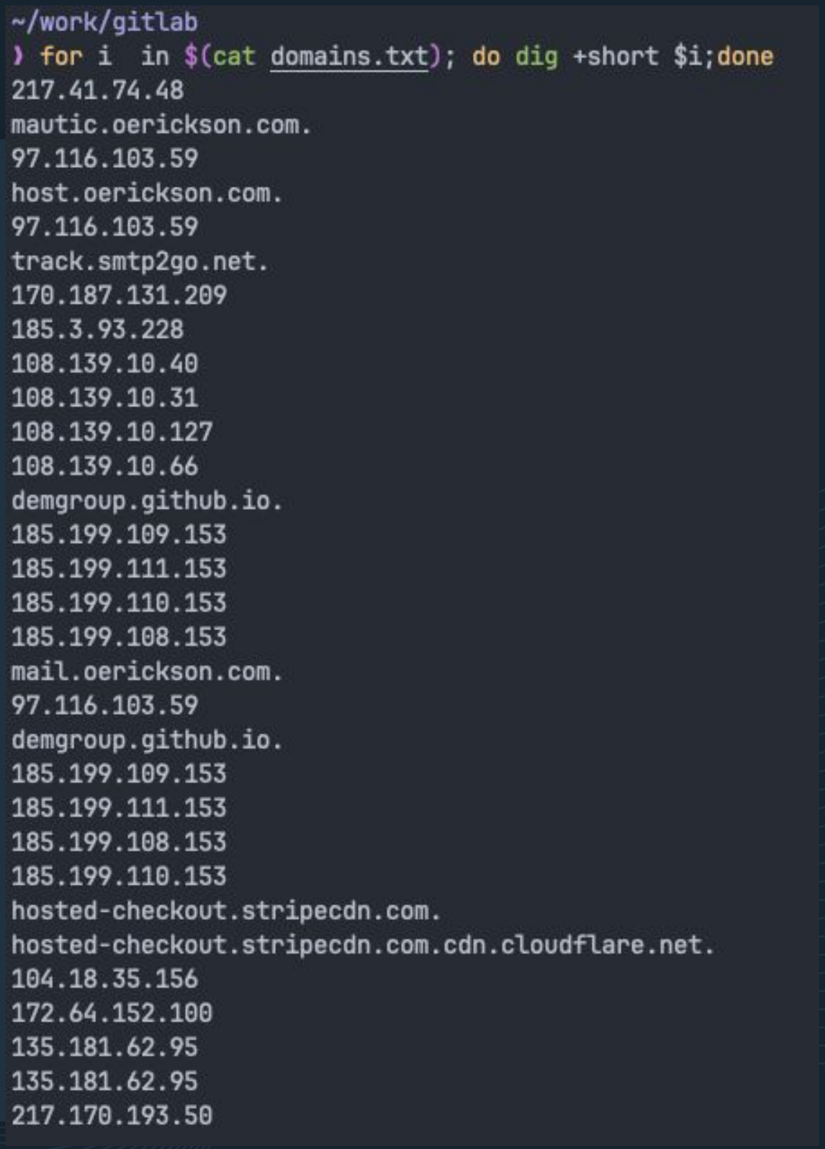
Field Value

CN = Amazon RSA 2048 M03
O = Amazon
C = US

identification



```
❯ subfinder -d aesircrypto.com

               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.7.0 (latest)
[redacted]
[INF] Enumerating subdomains for aesircrypto.com
nuget.aesircrypto.com
mautic.aesircrypto.com
swag.aesircrypto.com
link.aesircrypto.com
blog.aesircrypto.com
app.aesircrypto.com
mail.aesircrypto.com
prod.aesircrypto.com
dev.aesircrypto.com
app.dev.aesircrypto.com
billing.aesircrypto.com
ragnarok.aesircrypto.com
api.dev.aesircrypto.com
test-app.aesircrypto.com
webmail.aesircrypto.com
blog-test.aesircrypto.com
[INF] Found 16 subdomains for aesircrypto.com in 48 seconds 993 milliseconds
```



```
~/work/gitlab
❯ for i  in $(cat domains.txt); do dig +short $i;done
217.41.74.48
mautic.oerickson.com.
97.116.103.59
host.oerickson.com.
97.116.103.59
track.smtp2go.net.
170.187.131.209
185.3.93.228
108.139.10.40
108.139.10.31
108.139.10.127
108.139.10.66
demgroup.github.io.
185.199.109.153
185.199.111.153
185.199.110.153
185.199.108.153
mail.oerickson.com.
97.116.103.59
demgroup.github.io.
185.199.109.153
185.199.111.153
185.199.108.153
185.199.110.153
hosted-checkout.stripecdn.com.
hosted-checkout.stripecdn.com.cdn.cloudflare.net.
104.18.35.156
172.64.152.100
135.181.62.95
135.181.62.95
217.170.193.50
```

chaining it together

building the attack

1. identified dangling record
2. identified address in known prefixes
3. start ripping ec2 instances
4. get a match…
5. profit…?

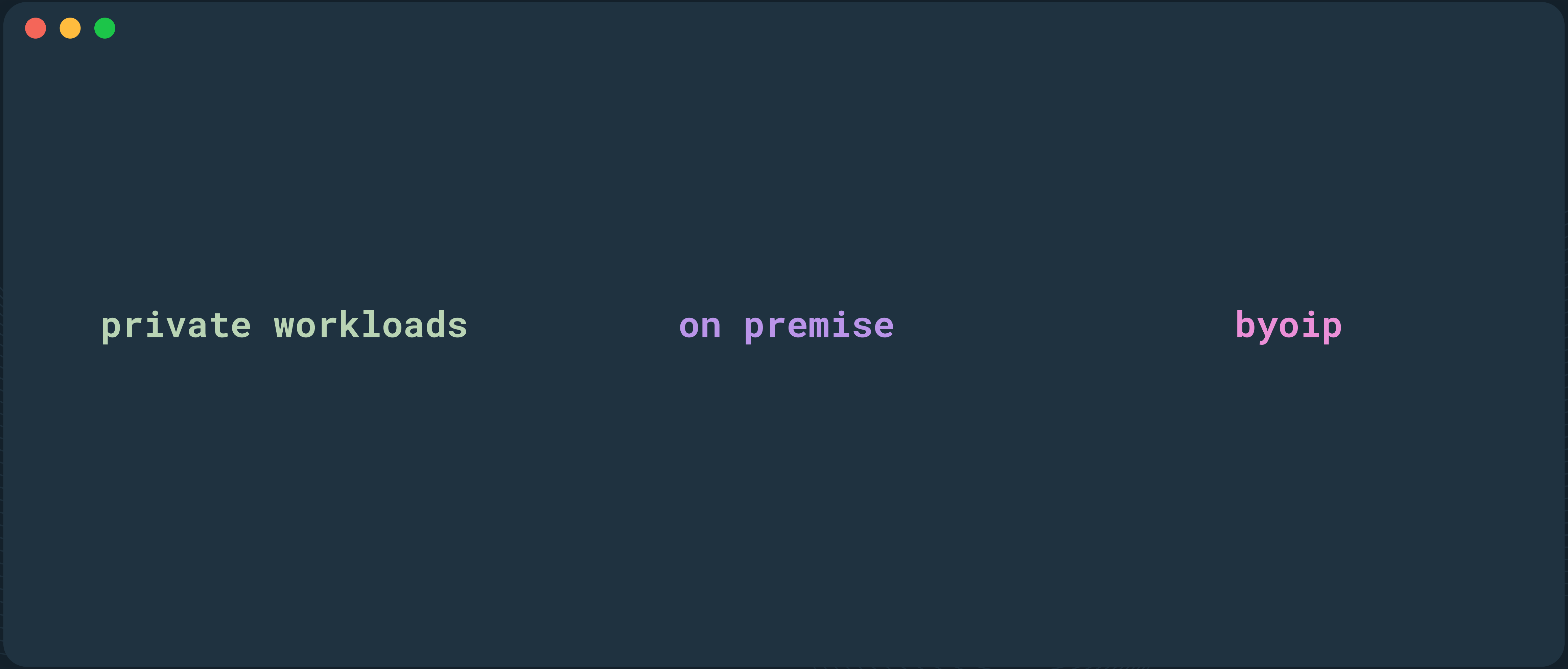
02 who does this affect most

you use the cloud

you run public workloads, or workloads with public addresses

you have bad governance over dns

who is less affected



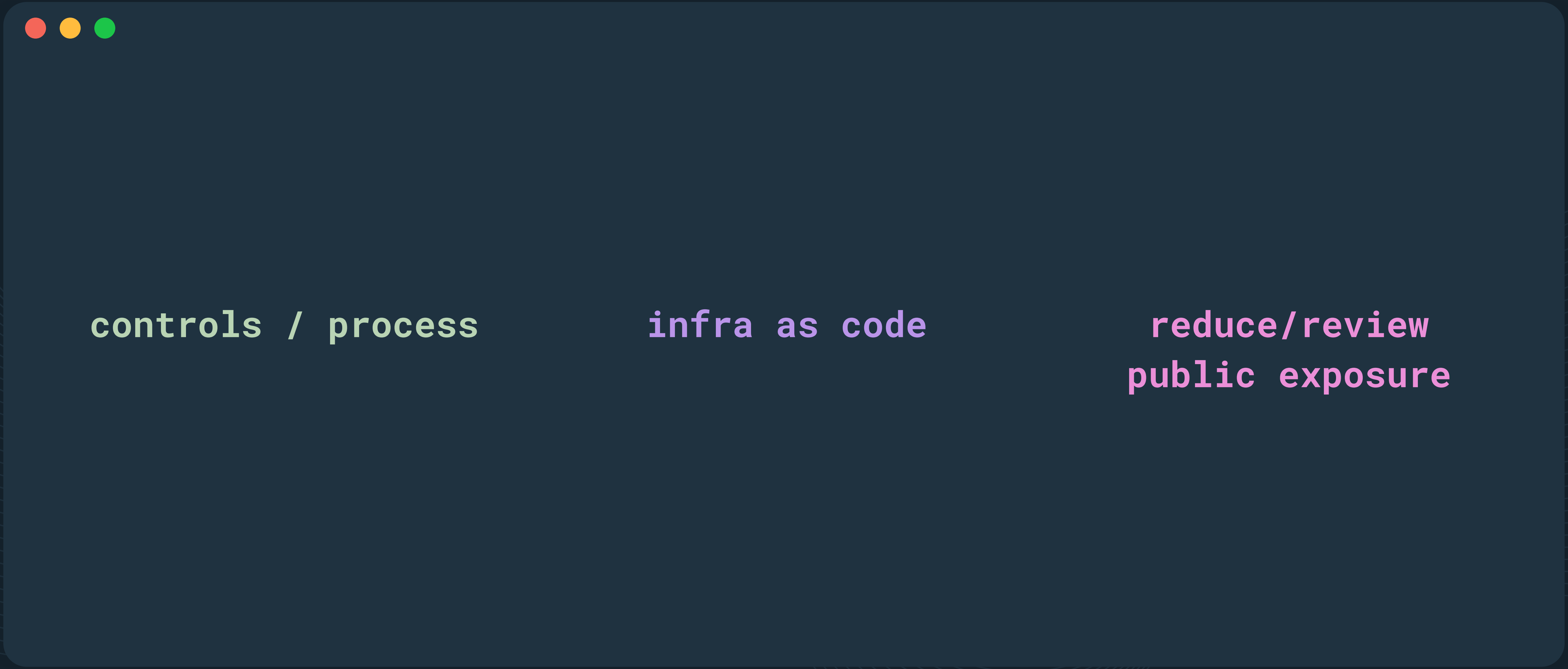
private workloads

on premise

byoip

03 what can i do ☺

what can i do



controls / process

infra as code

reduce/review
public exposure

04 what we did

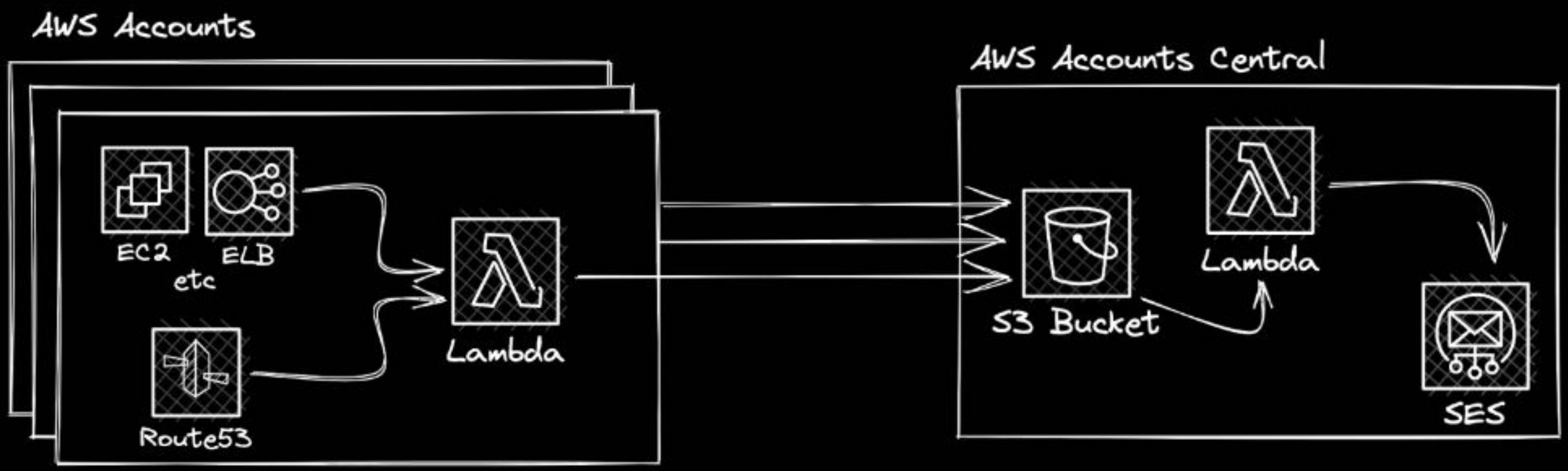
what we did

application lifecycle

review/reduce public exposure

develop controls & processes

Dangling DNS Monitoring

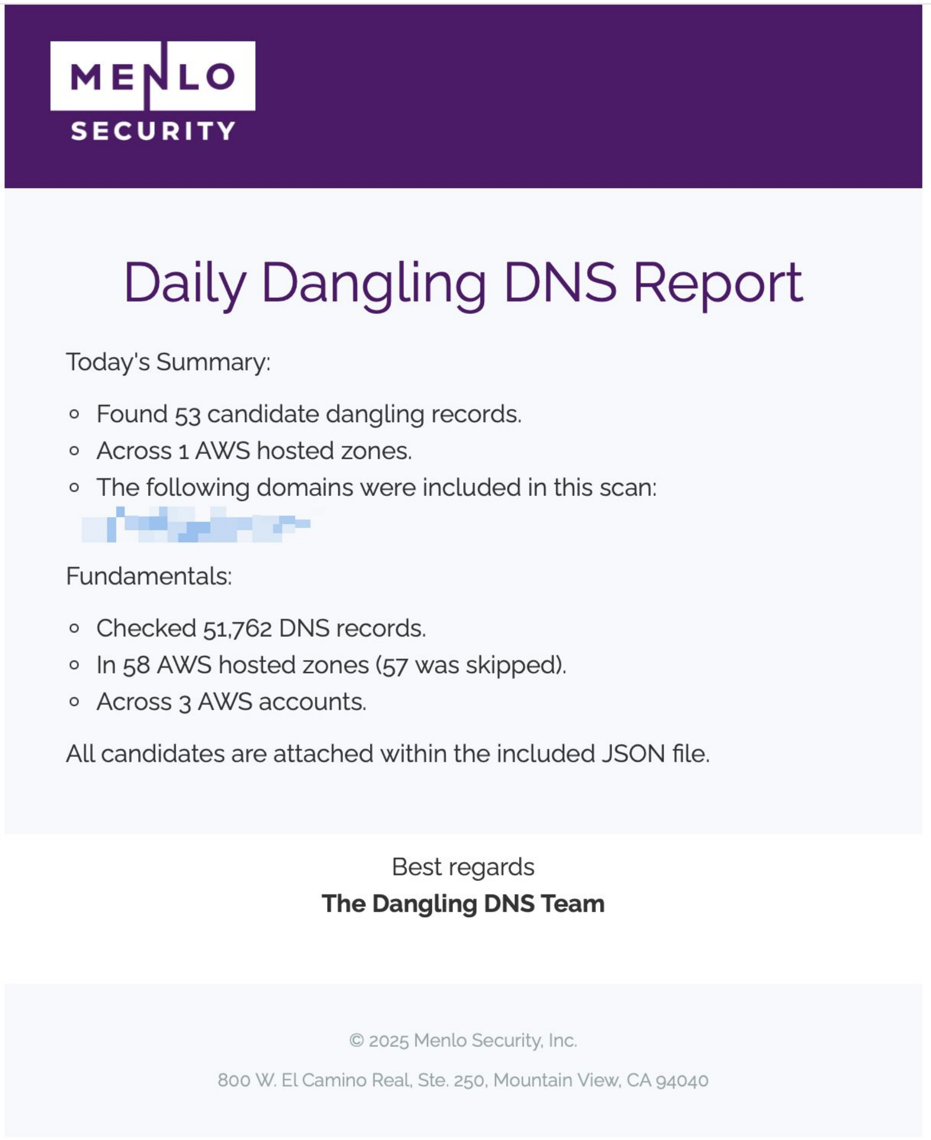


A Lambda within each account fetches all Network Interfaces and Route53 records within an account, publishing it to a central S3 bucket.

A central Lambda reads all interfaces data and Route53 records and computes candidate dangling records.

The resultant analysis is then emailed over SES to interested parties.

what we did



MENLO SECURITY

Daily Dangling DNS Report

Today's Summary:

- Found 53 candidate dangling records.
- Across 1 AWS hosted zones.
- The following domains were included in this scan: [redacted]

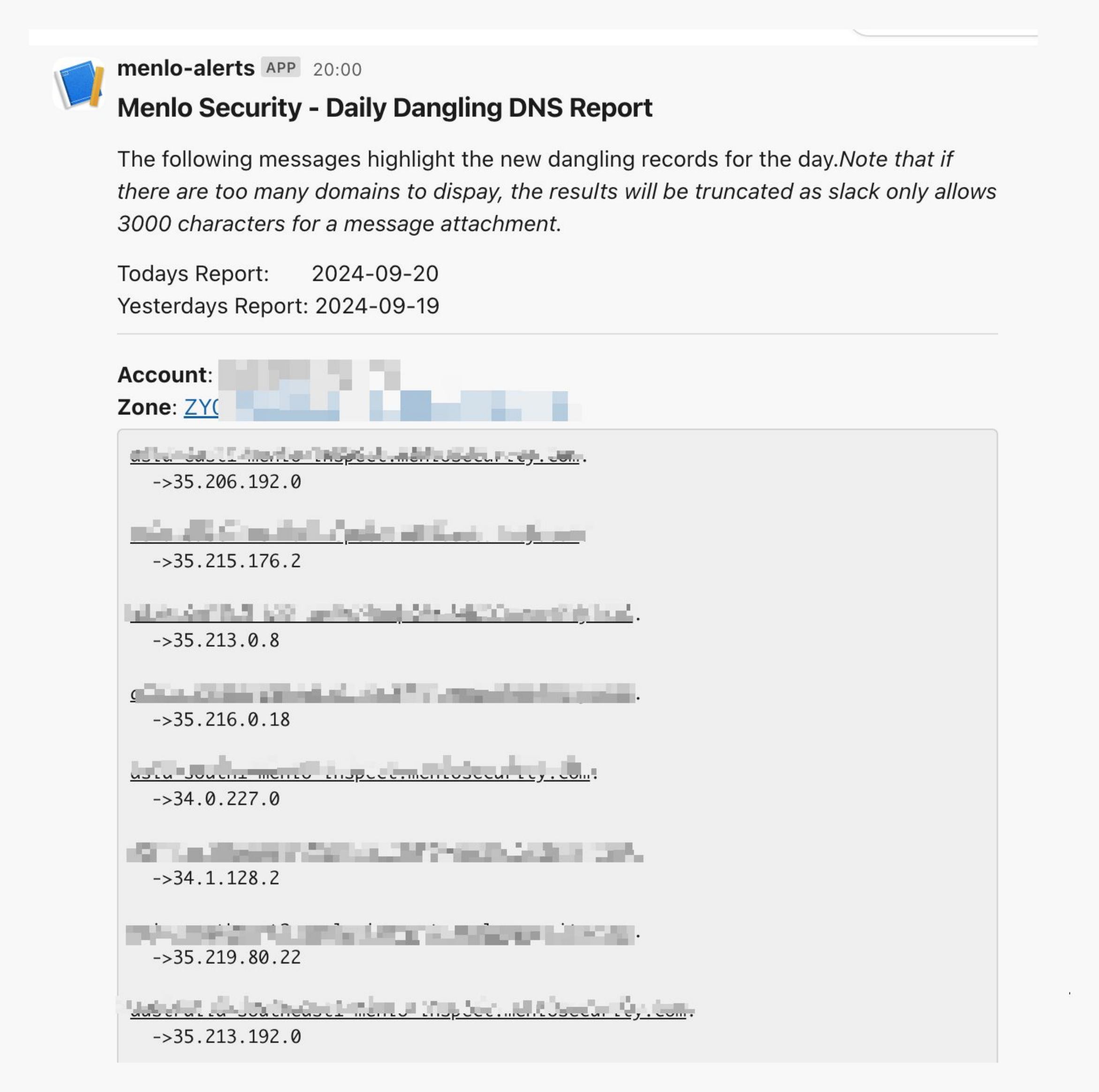
Fundamentals:

- Checked 51,762 DNS records.
- In 58 AWS hosted zones (57 was skipped).
- Across 3 AWS accounts.

All candidates are attached within the included JSON file.

Best regards
The Dangling DNS Team

800 W. El Camino Real, Ste. 250, Mountain View, CA 94040



menlo-alerts APP 20:00

Menlo Security - Daily Dangling DNS Report

The following messages highlight the new dangling records for the day.*Note that if there are too many domains to dispay, the results will be truncated as slack only allows 3000 characters for a message attachment.*

Todays Report: 2024-09-20
Yesterdays Report: 2024-09-19

Account: [redacted]
Zone: ZY([redacted]

```
[redacted]
  ->35.206.192.0

[redacted]
  ->35.215.176.2

[redacted]
  ->35.213.0.8

[redacted]
  ->35.216.0.18

[redacted]
  ->34.0.227.0

[redacted]
  ->34.1.128.2

[redacted]
  ->35.219.80.22

[redacted]
  ->35.213.192.0
```

demo time...

review of what can be done

application lifecycle

governance

review and reduce exposure

threat modelling

application development / scripting

buy expensive shit