



Subdomain Hijacking:

why DevOps is making us more vulnerable

Simon
Gurney

#>whoami

Co-Founder – Punk Security

- DevSecOps consultant
- Python Developer
- Security guy
- Geek



The agenda for this evening

How does DNS work?

2 methods to attack subdomains

Why should you care?

How you can defend your org

An intro to DNS

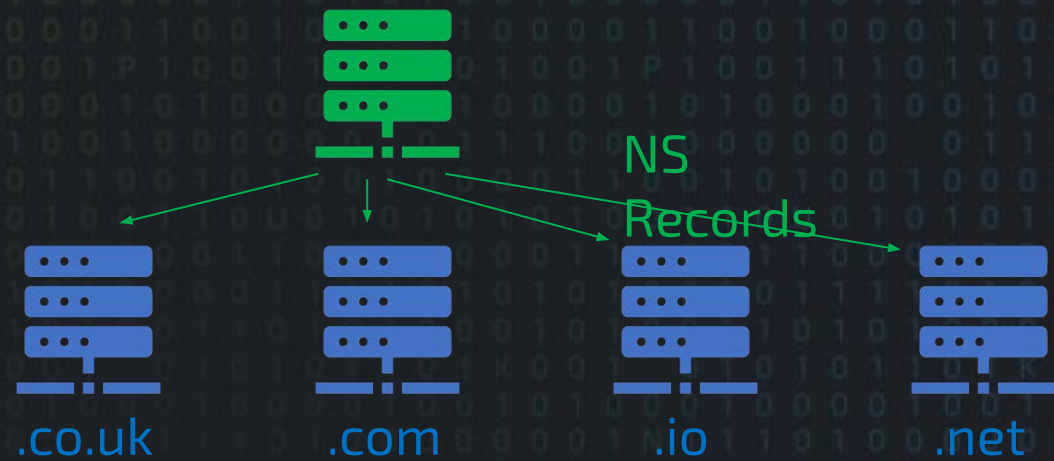
An intro to DNS

root hint servers



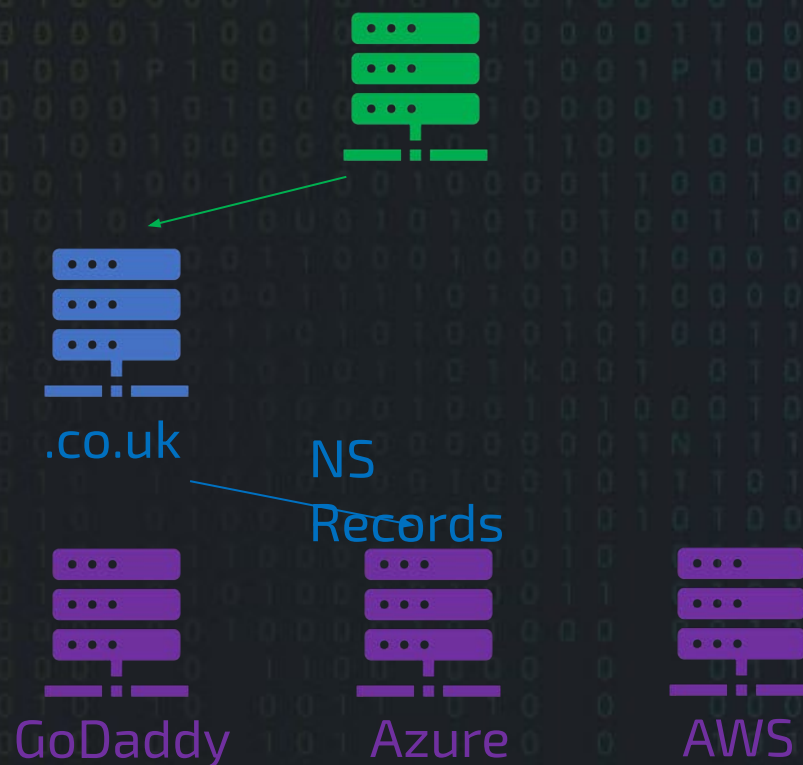
An intro to DNS

TLD servers

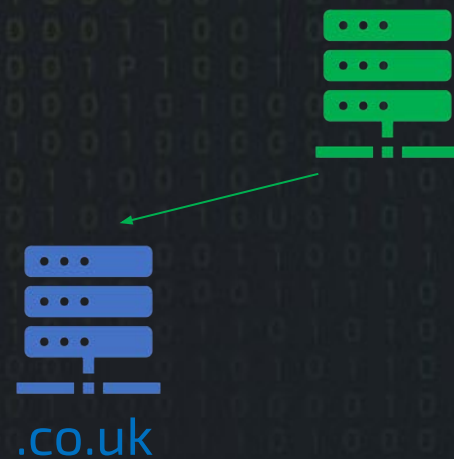


An intro to DNS

DNS Hosts



An intro to DNS



RECORDS:

- A
- AAAA
- CNAM
- E
- NS

An intro to DNS



NO ACCESS



.co.uk

CONFIGURE VIA REGISTRAR

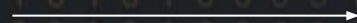


Azure

CONFIGURABLE

An intro to DNS

www.punksecurity.co.uk



BT

An intro to DNS

www.punksecurity.co.uk



BT

Where is .co.uk?

NS RECORD



An intro to DNS

www.punksecurity.co.uk



Where is
punksecurity.co.uk?

NS RECORD



An intro to DNS

www.punksecurity.co.uk



BT

Where is
www.punksecurity.co.uk

?

A: 104.26.8.175



Azure

An intro to DNS

www.punksecurity.co.uk



A: 104.26.8.175



BT

what are subdomains?

punksecurity.co.uk

www.punksecurity.co.uk

blog.punksecurity.co.uk

docs.punksecurity.co.uk


what are subdomains takeovers?

punksecurity.co.uk

www.punksecurity.co.uk

blog.punksecurity.co.uk

docs.punksecurity.co.uk



CNAME
punksecurity-docs.github.io

Scenario #1

Github pages takeover

```
C:\Users\SimonGurney>ping punksecurity-docs.punksecurity.co.uk
```

```
Pinging punksecurity-docs.punksecurity.co.uk [185.199.110.153] with 32 bytes of data:
```

```
Reply from 185.199.110.153: bytes=32 time=14ms TTL=58
```

```
Reply from 185.199.110.153: bytes=32 time=10ms TTL=58
```

```
Reply from 185.199.110.153: bytes=32 time=11ms TTL=58
```

```
Reply from 185.199.110.153: bytes=32 time=15ms TTL=58
```

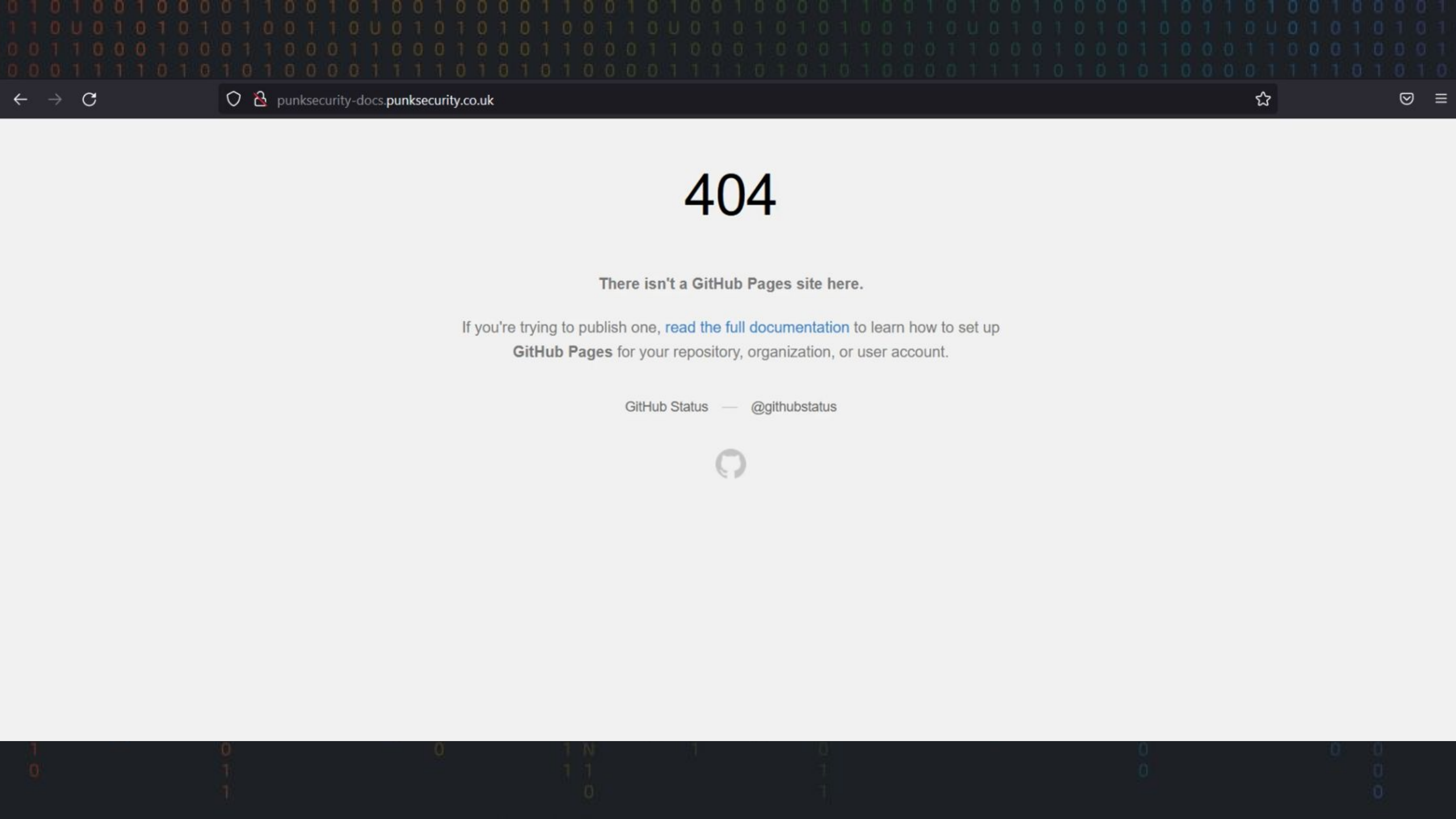
```
Ping statistics for 185.199.110.153:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 10ms, Maximum = 15ms, Average = 12ms
```

```
C:\Users\SimonGurney>
```

404

There isn't a GitHub Pages site here.

If you're trying to publish one, [read the full documentation](#) to learn how to set up **GitHub Pages** for your repository, organization, or user account.

GitHub Status — @githubstatus



SimonGurney Update index.md ✓ Latest commit 2700479 2 minutes ago History

1 contributor

This domain has been taken over

How is DevOps making it worse?

Core vs Context

Gene Kim / Geoffrey Moore

Ticketing systems

What is NS delegation

punksecurity.co.uk

www.punksecurity.co.uk

↑
Main DNS Server

NS delegation

punksecurity.co.uk

www.punksecurity.co.uk

dev.punksecurity.co.uk

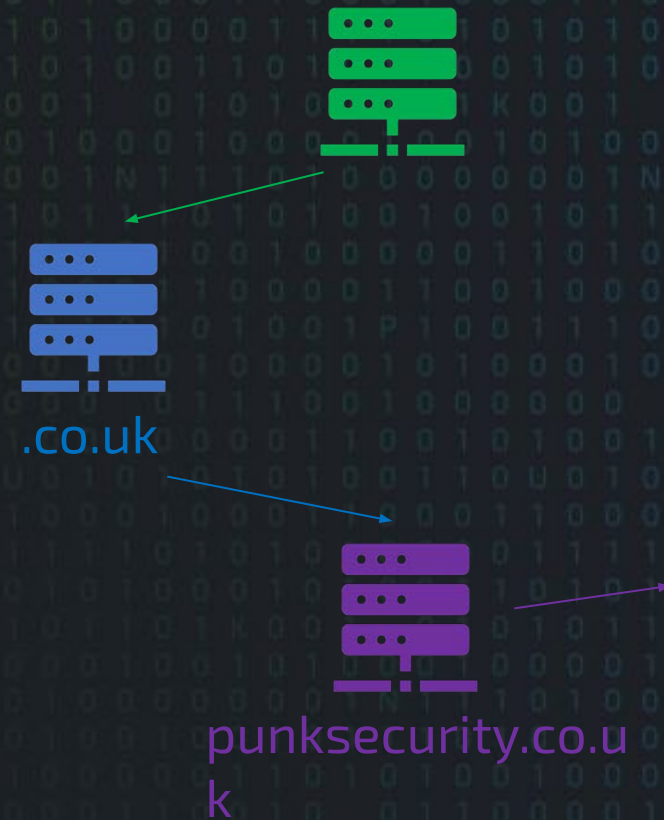
Main DNS Server

NS Record to Developers DNS Server

www.dev.punksecurity.co.uk

Developers
DNS Server

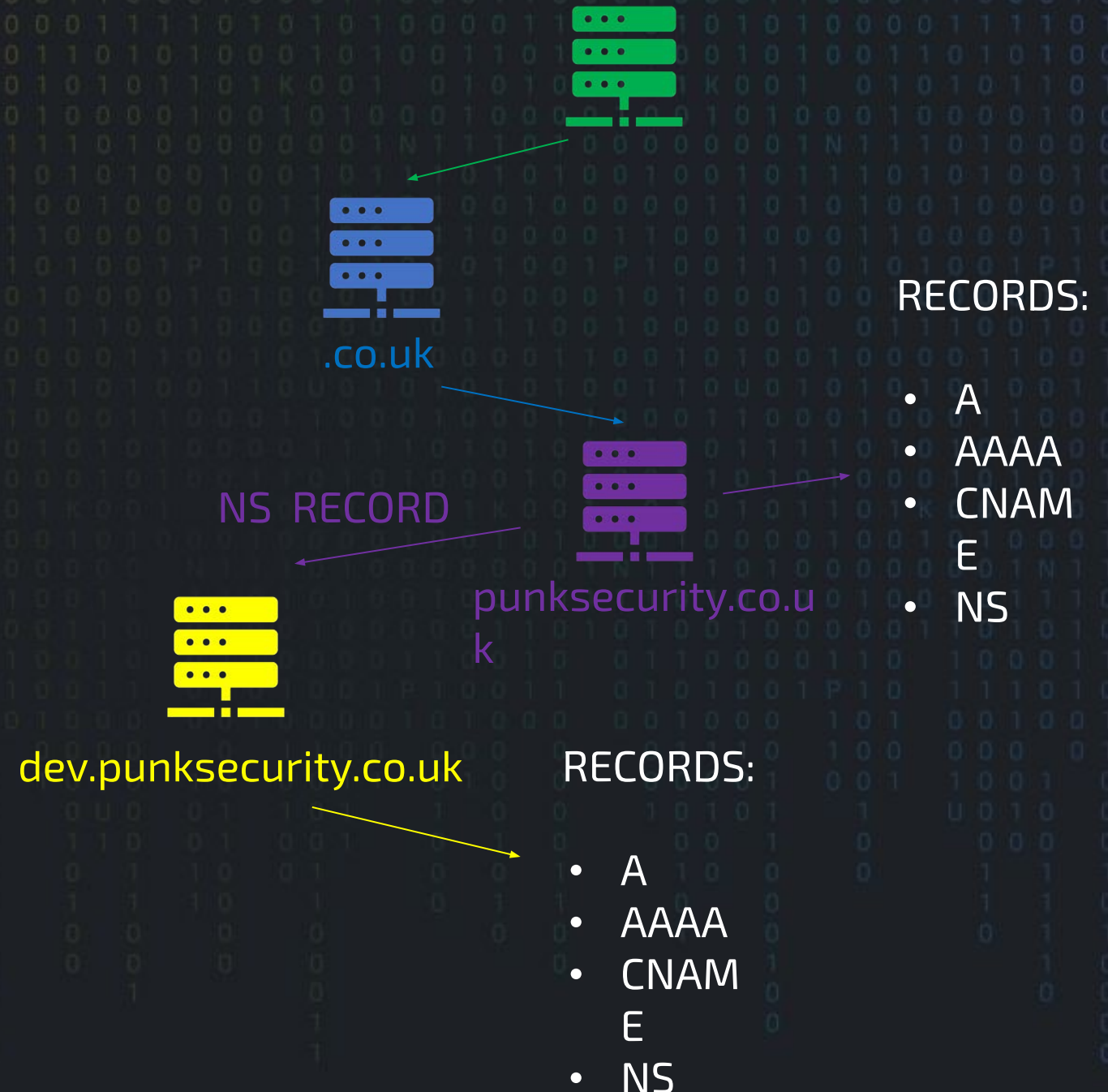
NS delegation



RECORDS:

- A
- AAAA
- CNAM
- E
- NS

NS delegation



What is an NS takeover

punksecurity.co.uk

www.punksecurity.co.uk

dev.punksecurity.co.uk

uat.punksecurity.co.uk

Main DNS Server

NS Record to Developers DNS Server

Incorrect NS Record

Scenario #2

AWS Route53 NS Takeover

Route 53 Console Hosted Zones

https://us-east-1.console.aws.amazon.com/route53/v2/hostedzones#

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Global AWSAdministratorAccess/admin.simon@punksecurity.co.uk

Route 53

Dashboard

Hosted zones

Health checks

▼ IP-based routing

CIDR collections

▼ Traffic flow

Traffic policies

Policy records

▼ Domains

Registered domains

Pending requests

▼ Resolver

VPCs

Inbound endpoints

Outbound endpoints

Rules

Query logging

▼ DNS Firewall

Route 53 > Hosted zones

Hosted zones (1)

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

↻

View details

Edit

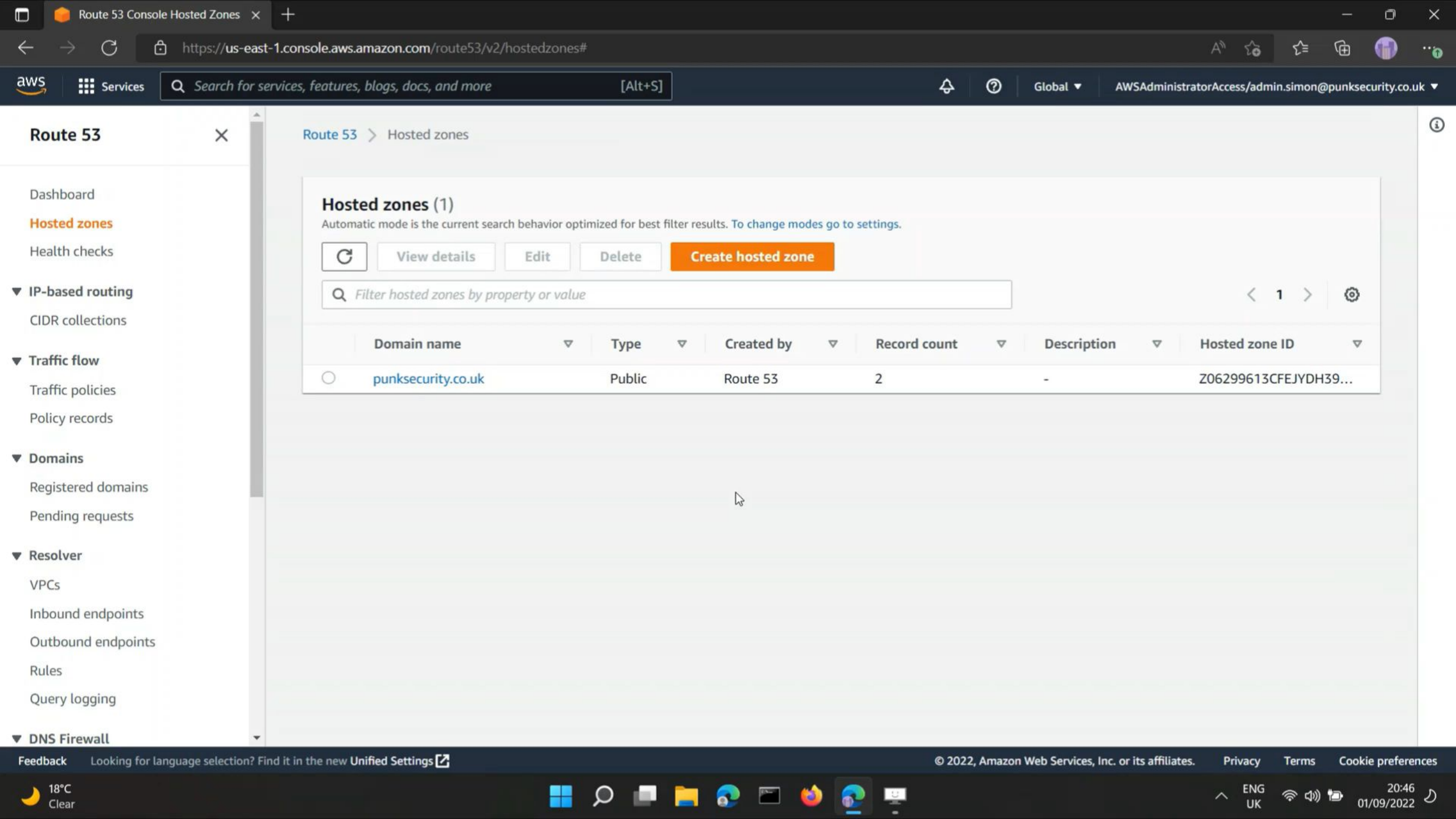
Delete

Create hosted zone

🔍 Filter hosted zones by property or value

< 1 > ⚙️

	Domain name	Type	Created by	Record count	Description	Hosted zone ID
○	punksecurity.co.uk	Public	Route 53	2	-	Z06299613CFEJYDH39...



- Route 53
- ×
- Dashboard
- Hosted zones
- Health checks
- ▼ IP-based routing
- CIDR collections
- ▼ Traffic flow
- Traffic policies
- Policy records
- ▼ Domains
- Registered domains
- Pending requests
- ▼ Resolver
- VPCs
- Inbound endpoints
- Outbound endpoints
- Rules
- Query logging
- ▼ DNS Firewall

Route 53 > Hosted zones

Hosted zones (1)

Automatic mode is the current search behavior optimized for best filter results. [To change modes go to settings.](#)



View details

Edit

Delete

Create hosted zone

Filter hosted zones by property or value

< 1 > ⚙

	Domain name	Type	Created by	Record count	Description	Hosted zone ID
<input type="radio"/>	punksecurity.co.uk	Public	Route 53	2	-	Z06299613CFEJYDH39...

How can we exploit this?

TARGET:

ns-766.awsdns-31.net

ns-1819.awsdns-35.co.uk

ns-1507.awsdns.co.uk

ns-99.awsdns-12.com



ns-300.awsdns-31.net

ns-200.awsdns-35.co.uk

ns-100.awsdns.co.uk

ns-400.awsdns-12.com

How can we exploit this?

TARGET:

ns-766.awsdns-31.net
ns-1819.awsdns-35.co.uk
ns-1507.awsdns.co.uk
ns-99.awsdns-12.com



ns-300...-31.net
ns-...-...co.uk
ns-1...awsdns...uk
ns-400.awsdns-12.com

How can we exploit this?

TARGET:

ns-766.awsdns-31.net
ns-1819.awsdns-35.co.uk
ns-1507.awsdns.co.uk
ns-99.awsdns-12.com



ns-300.awsdns-31.net
ns-766.awsdns-35.co.uk
ns-1507.awsdns.co.uk
ns-400.awsdns-12.com



ns-300.awsdns-31.net
ns-200.awsdns-35.co.uk
ns-1507.awsdns.co.uk
ns-99.awsdns-12.com

How can we exploit this?

TARGET:

ns-766.awsdns-31.net
ns-1819.awsdns-35.co.uk
ns-1507.awsdns.co.uk
ns-99.awsdns-12.com



ns-300.awsdns-31.net
ns-200.awsdns-35.co.uk
ns-100.awsdns.co.uk
ns-400.awsdns-12.com



ns-300.awsdns-31.net
ns-200.awsdns-35.co.uk
ns-1507.awsdns.co.uk
ns-99.awsdns-12.com



ns-766.awsdns-31.net
ns-1819.awsdns-35.co.uk
ns-100.awsdns.co.uk
ns-400.awsdns-12.com

How is DevOps making it worse?

- IaC and good old copy and pasting
- Delegation is more rife than ever

so what?

Credible phishing links

support.invisionpower.com

new.rubyonrails.org

signup.uber.com

so what?

Credible email addresses

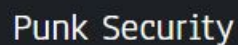
info@support.invisionpower.com

support@new.rubyonrails.org

help@signup.uber.com

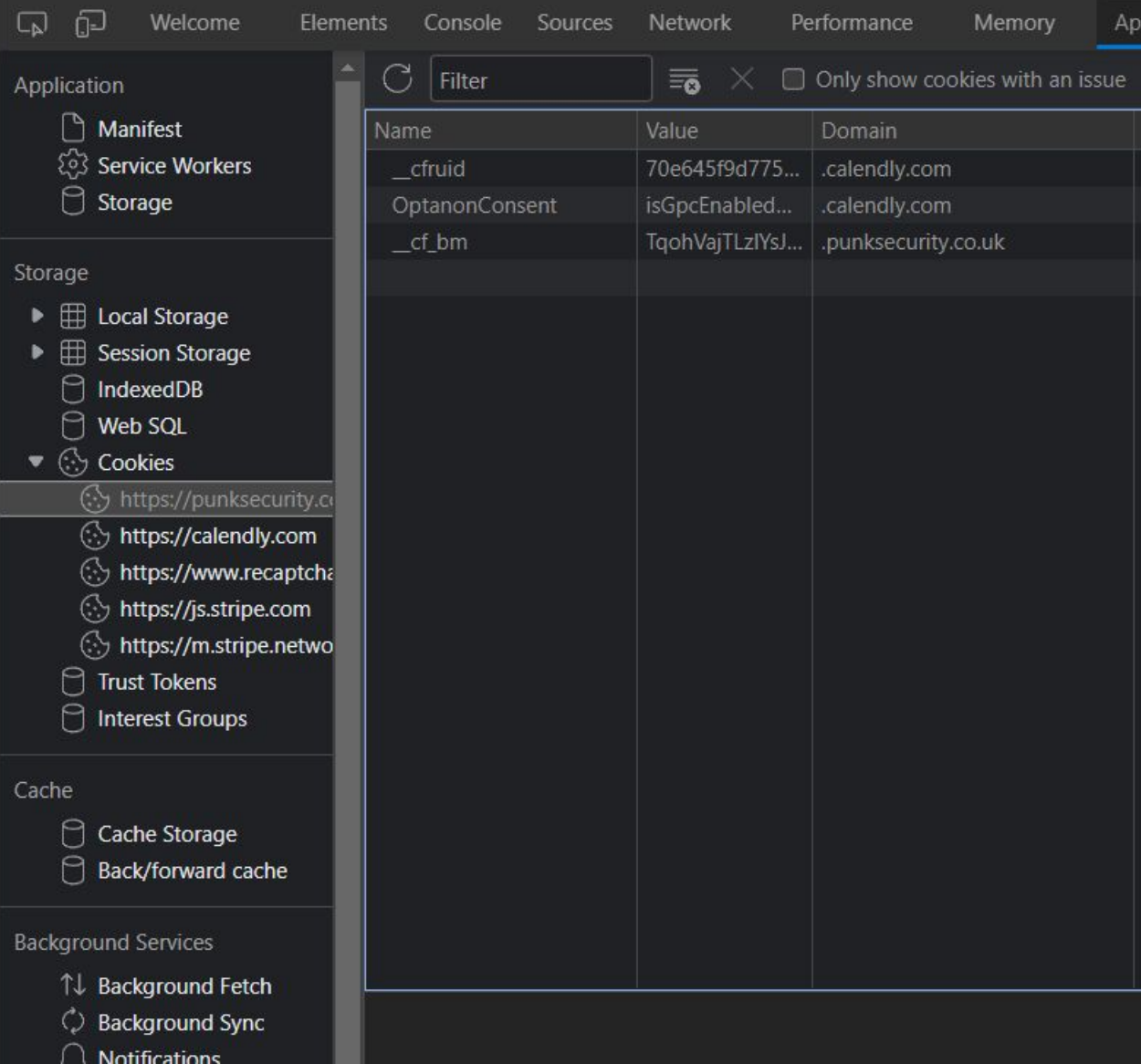
so what?

Loosely scoped cookies



We are specialists in integrating security in to DevOps pipelines, enabling rapid and secure development.

Our managed services enable our customers to release **secure code** through managed security **pipelines** that automatically analyse their applications with **industry leading tools**, whilst our analysts reduce the burden to developers.



so what?

Loosely scoped cookies

punksecurity.co.uk

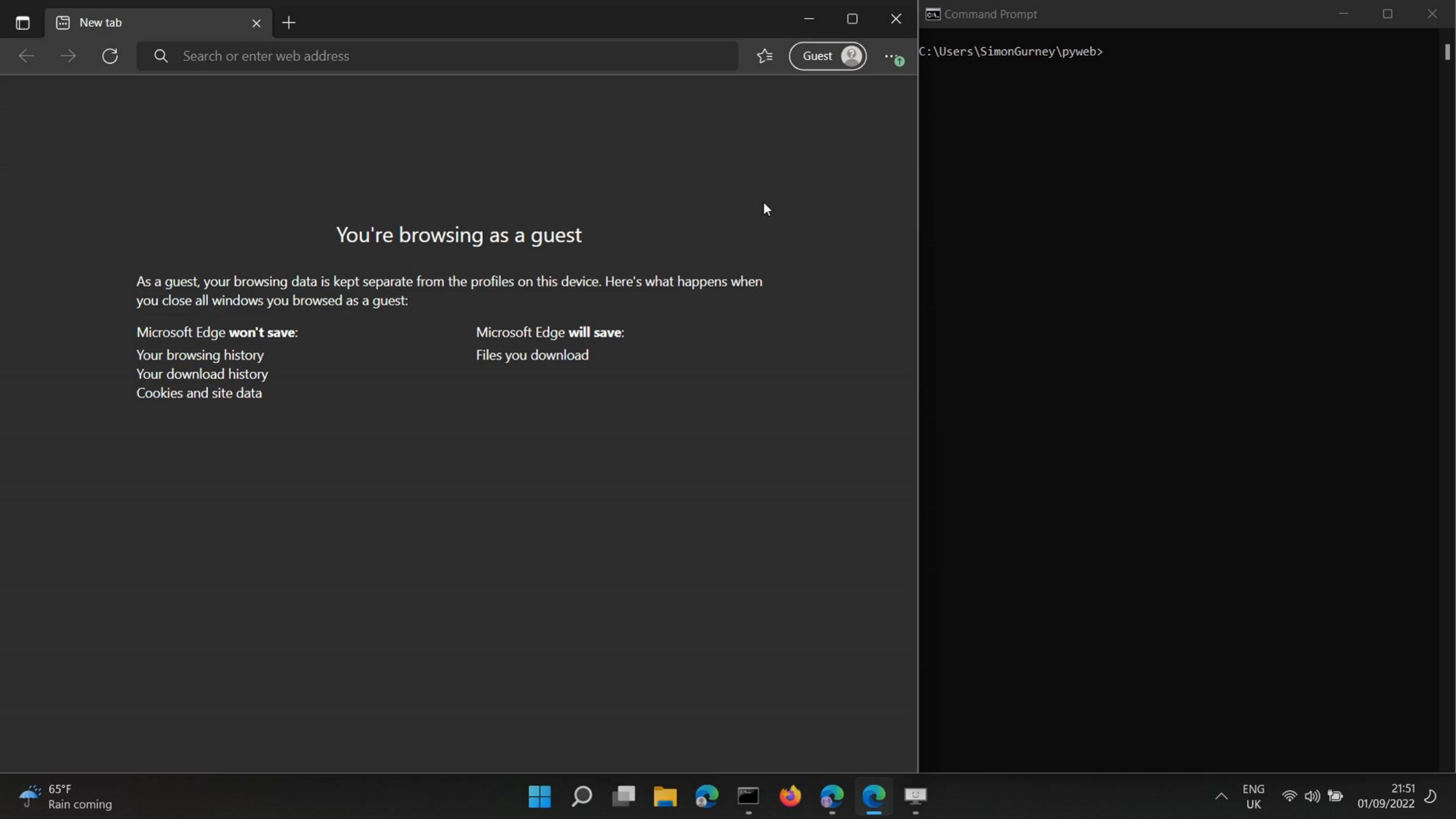
www.punksecurity.co.uk

blog.punksecurity.co.uk

docs.punksecurity.co.uk

DEMO #3

Stealing loosely scoped cookies



New tab



Search or enter web address



Guest



You're browsing as a guest

As a guest, your browsing data is kept separate from the profiles on this device. Here's what happens when you close all windows you browsed as a guest:

Microsoft Edge **won't save:**

- Your browsing history
- Your download history
- Cookies and site data

Microsoft Edge **will save:**

- Files you download

Command Prompt

C:\Users\SimonGurney\pyweb>



65°F
Rain coming



ENG
UK



21:51
01/09/2022



how do we defend?

Periodic audits / DNS hygiene

Bug bounty programs

Extend our pen testing scopes

dnsReaper

#> docker run punksecurity/dnsReaper

Give it domains, or have it fetch them

#> docker run punksecurity/dnsReaper

Give it domains, or have it fetch them

Tests all domains with nearly 60 signatures

- ❑ Pattern match the record
- ❑ Pattern match the web response

#> docker run punksecurity/dnsReaper

Give it domains, or have it fetch them

Tests all domains with nearly 60 signatures

- Pattern match the record
- Pattern match the web response

Reports to screen, csv and json

use cases

Audit a DNS configuration

Scan for bounties \$ \$ \$

Prevent bad deployments

dnsReaper

```
PS C:\Users\SimonGurney> docker run punksecurity/dnsreaper
```

```
✗ error: the following arguments are required: provider
```



DNS Reaper ☠

Scan all your DNS records for subdomain takeovers!

usage:

```
docker run punksecurity/dnsreaper -- provider [options]
```

output:

findings output to screen and (by default) results.csv

help:

```
docker run punksecurity/dnsreaper -- --help
```

providers:

- > zonetransfer - Scan multiple domains by fetching records via DNS zone transfer
- > file - Read domains from a file (or folder of files), one per line
- > cloudflare - Scan multiple domains by fetching them from Cloudflare
- > aws - Scan multiple domains by fetching them from AWS Route53
- > single - Scan a single domain by providing a domain on the commandline
- > azure - Scan multiple domains by fetching them from Azure DNS services
- > bind - Read domains from a dns BIND zone file, or path to multiple
- > digitalocean - Scan multiple domains by fetching them from Digital Ocean

```
PS C:\Users\SimonGurney> |
```



```
PS C:\Users\SimonGurney> docker run punksecurity/dnsreaper aws --aws-access-key-id AKIAUIG46DC3VB7C4SHA --aws-access-key-secret rHrhuWmFLPiSxBSYj0oJ5IzLYp06ToHdNvBHI02D
```



DNS Reaper 🦋

Scan all your DNS records for subdomain takeovers!

```
Got 3 records from aws
Testing with 59 signatures
```

We found 2 takeovers 🦋

```
-- DOMAIN 'developers.punksecurity.co.uk' :: SIGNATURE '_generic_zone_missing_on_ns' :: CONFIDENCE 'POTENTIAL'
```

```
NS: ns-766.awsdns-31.net,ns-1819.awsdns-35.co.uk,ns-1507.awsdns-60.org,ns-99.awsdns-12.com
```

```
-- DOMAIN 'developers.punksecurity.co.uk' :: SIGNATURE 'aws_ns' :: CONFIDENCE 'CONFIRMED'
```

```
NS: ns-766.awsdns-31.net,ns-1819.awsdns-35.co.uk,ns-1507.awsdns-60.org,ns-99.awsdns-12.com
```

🦋 We completed in 1.68 seconds

...Thats all folks!

```
PS C:\Users\SimonGurney> |
```



Search or jump to...



[Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)



[punk-security](#) / [dnsReaper](#)

Public



Edit Pins



Watch

13



Fork

108



Starred

1.5k



[Code](#)



Issues

11



Pull requests

5



Discussions



Actions



Security



Insights



Settings



main



4 branches



11 tags

[Go to file](#)



Add file



Code



About



[SimonGurney](#) fix: explicitly close pool [#118](#) ([#121](#))



57b9a4d

on Sep 8



184 commits



.github/workflows

feat: add docker builds

3 months ago



dev

feat: Support DNS zone transfer provider ([#103](#))

2 months ago



docs

feat: Add support for DigitalOcean provider ([#115](#))

last month



providers

enhancement: Handle AWS provider API errors gracefully ([#119](#))

last month



signatures

feat: cargo collective signature ([#111](#))

last month



tests

fix: remove false positives caused by whois rate limiting [#74](#) ([#75](#))

2 months ago



.gitignore

feat: Support DNS zone transfer provider ([#103](#))

2 months ago



Dockerfile

feat: Support DNS zone transfer provider ([#103](#))

2 months ago



LICENSE

chore: add license

2 months ago



README.md

feat: Add support for DigitalOcean provider ([#115](#))

last month

dnsReaper - subdomain takeover tool for attackers, bug bounty hunters and the blue team!

[Readme](#)

[AGPL-3.0 license](#)

[1.5k stars](#)

[13 watching](#)

[108 forks](#)

[Releases](#) 5



1.6.1

Latest

on Sep 8

[+ 4 releases](#)

dnsReaper/aws.md at main · punk-security/dnsReaper

← → ↺ https://github.com/punk-security/dnsReaper/blob/main/docs/aws.md A ☆ Guest

47 lines (38 sloc) 1.41 KB <> Raw Blame

Requirements

As a minimum you need:

- `GetHostedZone`
- `ListHostedZones`
- `ListResourceRecordSets`

A suggested inline policy for the account would be:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets"
      ],
      "Resource": "*"
    }
  ]
}
```

Fancy a DevSecOps CTF?

punksecurity.co.uk/ctf

Fancy a DevSecOps CTF?

Subdomain takeovers

Abusing SaaS services

Attacking aws and kubernetes

Cracking JWTs and Ansible vaults

punksecurity.co.uk/ctf

Punk Security

Automating quality
and security checks