Internal Domain Name Collision 2.0

Philippe Caturegli

*"A **name collision** occurs when an attempt to resolve a name used in a **private name space** (e.g., short, unqualified name) results in a query to the **public Domain Name System** (DNS).*

*When the administrative boundaries of **private** and **public** namespaces **overlap**, name resolution may yield **unintended** or **harmful** results."*

ICANN, 2013

Outline

1. Introduction
2. Definitions & Context
3. Research Methodology
4. Findings Examples

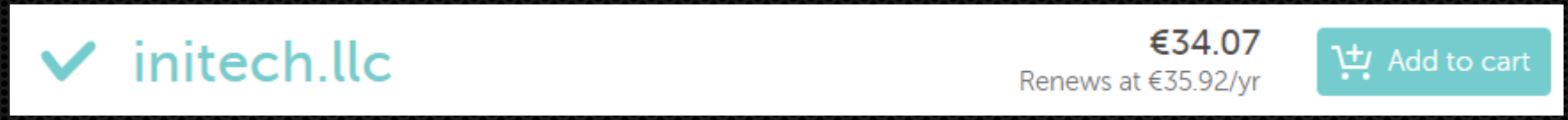
Introduction

- Hired to perform a RedTeam engagement for an IT Services Company

- ~300 Employees (with strong IT background)
- Limited external footprint
  - Hosted WordPress
  - Client Portal (.NET)
  - Exchange Server
  - VPN (SonicWall)

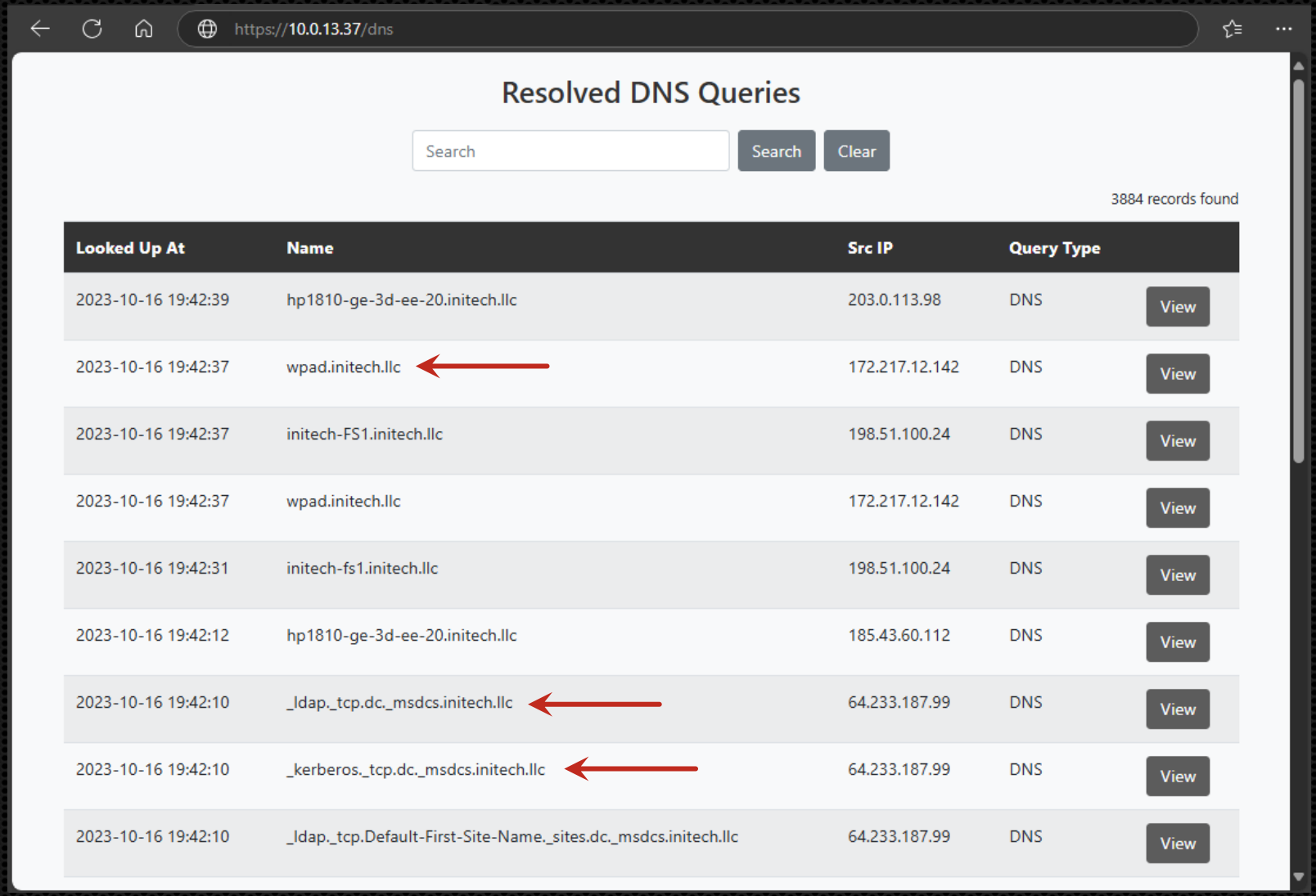
Introduction

```
└─# telnet exch01.initech.com 25
Trying exch01.initech.com...
Connected to exchange.initech.com.
Escape character is '^]'.
220 mail.initech.com Microsoft ESMTP MAIL Service ready at Mon, 16 Oct 2023 17:08:49 +0200
ehlo hack.lu
250-exch01.initech.com Hello [211.219.156.149]
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-AUTH NTLM
250-8BITMIME
250 BINARYMIME
```




```
└─# nmap -p 25 --script smtp-ntlm-info exch01.initech.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-10-16 17:18 EDT
Nmap scan report for exch01.initech.com (211.219.156.149)
Host is up (0.013s latency).

PORT    STATE    SERVICE
25/tcp  open     smtp
| smtp-ntlm-info:
|   Target_Name: INITECH
|   NetBIOS_Domain_Name: INITECH
|   NetBIOS_Computer_Name: EXCH01
|   DNS_Domain_Name: initech.llc
|   DNS_Computer_Name: EXCH01.initech.llc
|   DNS_Tree_Name: initech.llc
|_  Product_Version: 10.0.14393
```

Introduction



https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/7fcdce70-5205-44d6-9c3a-260e616a2f04

Introduction

- Responder

```
[CLDAP] Sent CLDAP pong to 172.217.12.142.
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[Proxy-Auth] NTLMv2 Client   : 198.51.100.24
[Proxy-Auth] NTLMv2 Username : INITECH\m.bolton
[Proxy-Auth] NTLMv2 Hash     : m.bolton::INITECH:6b5265915a608ae4:EC46F943ED35702C59A2D4EC4D0C0F31:01010000000000F344679DF7B3D43F4AAB
01A4EE0A8E2A836E41000000000200080053004F0044005A0001001E00570049004E002D0058004200340034004600460035004900390036005300040014005300 4F0
044005A002E004C004F00430041004C0003003400570049004E002D0058004200340034004600460035004900390036005300 2E0053004F0044005A002E004C004F00
430041004C000500140053004F0044005A002E004C004F00430041004C0008003000300000000000000000000000000020000055552299C7444122816C56B3B4A057C50
31E1A00FD89FF7BD035F3AAD321356C0A001000000000000000000000000000000000000000900240048005400540050002F00390034002E00320033002E003100350035
002E00320031003700000000000000000000
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[CLDAP] Sent CLDAP pong to 151.101.1.69.
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[Proxy-Auth] User-Agent       : Microsoft NCSI
[Proxy-Auth] User-Agent       : Microsoft NCSI
[CLDAP] Sent CLDAP pong to 64.233.187.99.
[Proxy-Auth] NTLMv2 Client   : 37.48.95.144
[Proxy-Auth] NTLMv2 Username : INITECH\s.nagheenanajar
[Proxy-Auth] NTLMv2 Hash     : s.nagheenanajar::INITECH:1631c5efeb18e928:B87F8A79DF4B3755E57917178B65204D:01010000000001681FEC895087
02E004C004F00430041004C0003003400570049004E002D0058004200340034004600460035004900390036005300 2E0053004F0044005A002E004C004F0043004100
4C000500140053004F0044005A002E004C004F00430041004C0008003000300000000000000000000000000020000 0B7EBC86DCA1 0DECC09EAB8DF6D8D3E09346C86AB
71735F500E7E88BDDA2E93E0A001000000000000000000000000000000000000000900 2E0048005400540050002F00390034002E00320033002E003100350035002E0032
00310037003A003300310032003800000000000000000
[Proxy-Auth] User-Agent       : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Sa
fari/537.36 Edg/129.0.0.0
```

Introduction

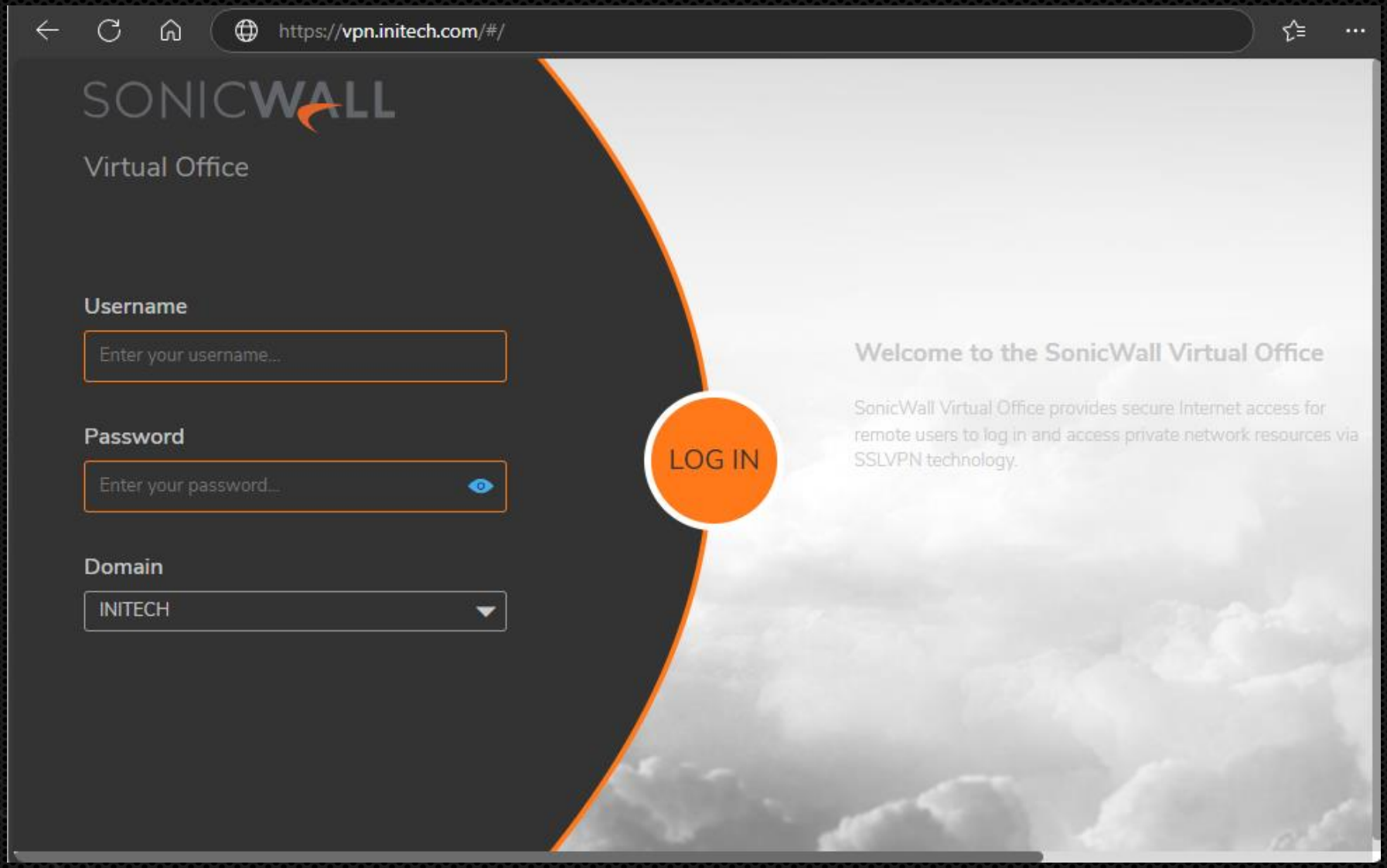
- Responder

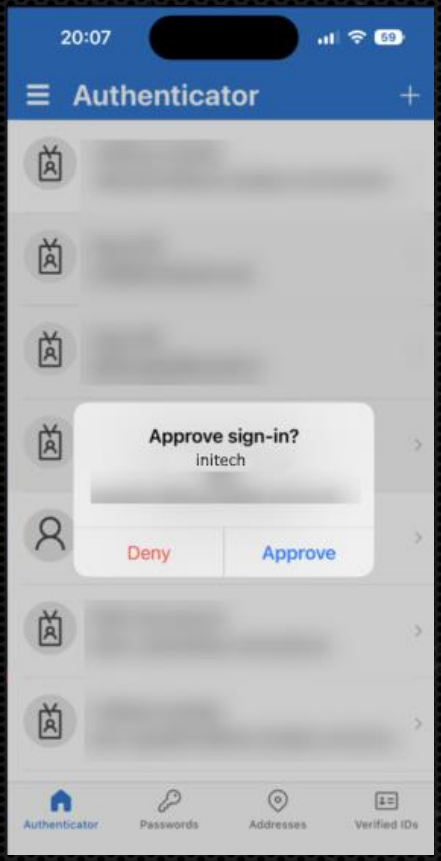
```
[CLDAP] Sent CLDAP pong to 172.217.12.142.
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[Proxy-Auth] NTLMv2 Client   : 198.51.100.24
[Proxy-Auth] NTLMv2 Username : INITECH\m.bolton
[Proxy-Auth] NTLMv2 Hash     : m.bolton::INITECH:6b5265915a608ae4:EC46F943ED35702C59A2D4EC4D0C0F31:01010000000000F344679DF7B3D43F4AAB
01A4EE0A8E2A836E41000000000200080053004F0044005A0001001E00570049004E002D0058004200340034004600460035004900390036005300040014005300 4F0
044005A002E004C004F00430041004C0003003400570049004E002D0058004200340034004600460035004900390036005300 2E0053004F0044005A002E004C004F00
430041004C000500140053004F0044005A002E004C004F00430041004C0008003000300000000000000000000000000020000055552299C7444122816C56B3B4A057C50
31E1A00FD89FF7BD035F3AAD321356C0A001000000000000000000000000000000000000900240048005400540050002F00390034002E00320033002E003100350035
002E00320031003700000000000000000
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[CLDAP] Sent CLDAP pong to 151.101.1.69.
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[Proxy-Auth] User-Agent        : Microsoft NCSI
[Proxy-Auth] User-Agent        : Microsoft NCSI
```

- Hashcat

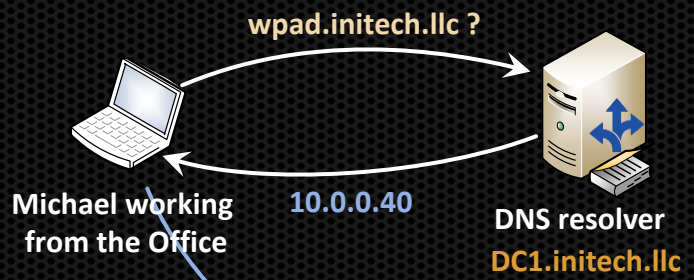
```
m.bolton::INITECH:6b5265915a608ae4:EC46F943ED35702C59A2D4EC4D0C0F31:01010000000000F344679DF7B3D43F4AAB01A4EE0A8E2A836E41000000000200080053004F0044005A0001001E00570049004E002D0058004200340034004600460035004900390036005300040014005300 4F0044005A002E004C004F00430041004C00030034005700 49004E002D0058004200340034004600460035004900390036005300040014005300 4F0044005A002E004C004F00430041004C000500140053004F0044005A002E004C004F004300 41004C0008003000300000000000000000000000000020000055552299C7444122816C56B3B4A057C5031E1A00FD89FF7BD035F3AAD321356C0A001000000000000000000000000000000000000900240048005400540050002F00390034002E00320033002E003100350035002E00320031003700000000000000000:TPSreport2023!

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: m.bolton::INITECH:6b5265915a608ae4:ec46f943ed35702...000000
Time.Started.....: Wed Nov 22 15:42:54 2023 (0 secs)
Time.Estimated...: Wed Nov 22 15:42:54 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/officespace.dict)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 1928.3 MH/s (0.71ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/2 (50.00%) Digests (total), 1/2 (50.00%) Digests (new)
Progress.........: 432056/14344386 (0.01%)
Rejected.........: 0/432056 (0.00%)
Restore.Point....: 0/14344386 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: TPSreport2023! -> queen
Hardware.Mon.#1..: Temp: 49c Fan: 32% Util: 72% Core:2805MHz Mem:10802MHz Bus:16

Started: Wed Nov 22 15:42:52 2024
Stopped: Wed Nov 22 15:42:55 2024
```

Introduction

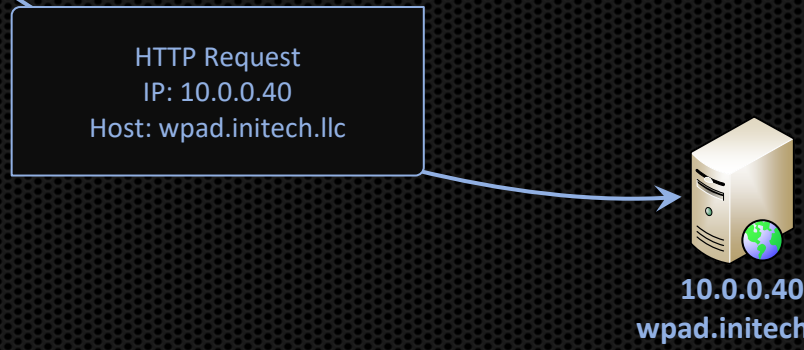




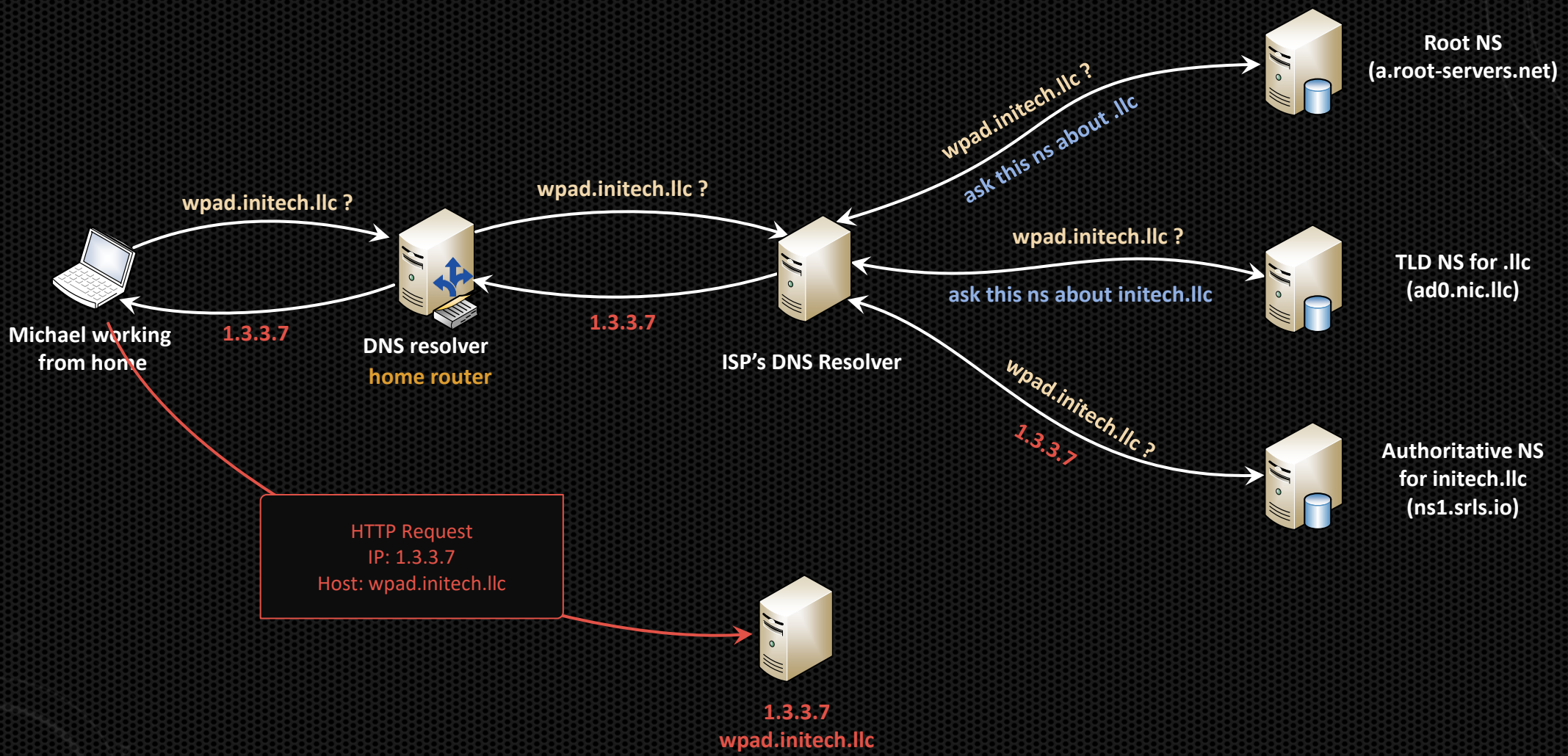
What happened ?



DNS Zone initech.llc		
Name	Type	Data
intranet.	A	10.0.0.41
wpad.	A	10.0.0.40
DC1.		10.0.0.10
__ldap._tcp.dc._msdcs.	SRV	[0][100][DC1.initech.llc]



What happened ?



Definitions

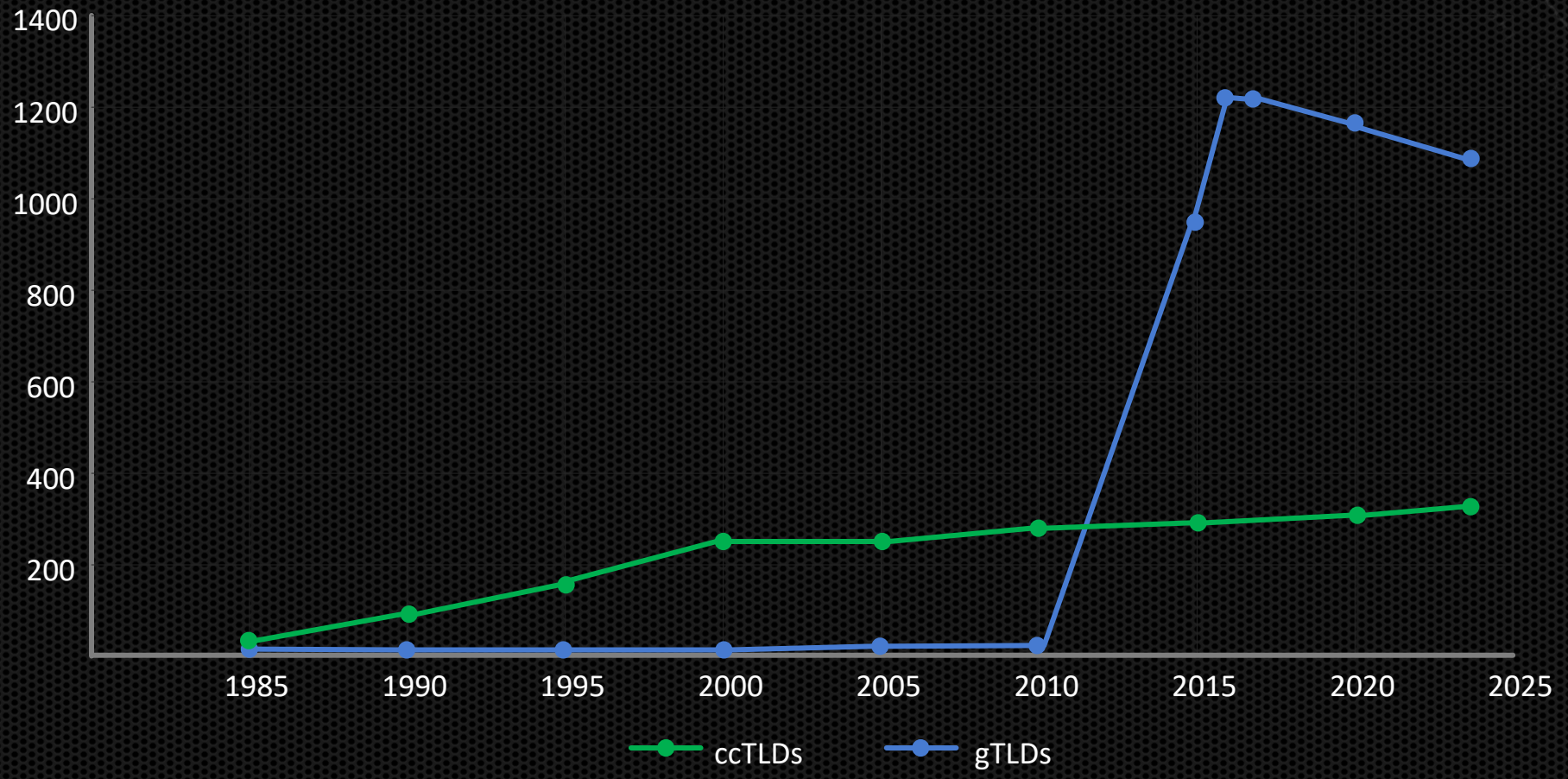
Top Level Domains (TLDs)

There are several categories of TLDs, each serving different purposes.

- **Generic Top-Level Domains** (gTLDs)
  - .com, .net, .org, .llc, etc.
- **Country Code Top-Level Domains** (ccTLDs)
  - .us, .fr, .de, .it, etc.
- **Sponsored Top-Level Domains** (sTLDs)
  - .edu, .gov, .mil, .int, etc.

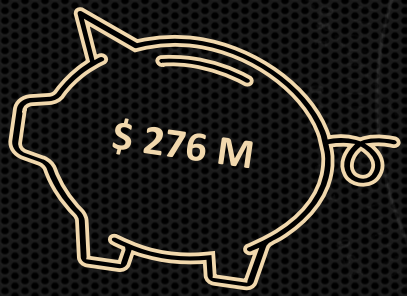
New gTLDs

- Up until 2013, there were 8 gTLDs (.com, .net, .org, .biz, .info, .name, .pro, .mobi)
- In 2013, ICANN launched a program to allow new gTLDs to be added the Internet's root zone
- Between 2013 and 2016, over **1200** new gTLDs were introduced.



ICANN Revenue

- **One time revenue from new gTLD applicants**
  - New gTLDs application fee: **$227,000** (non-refundable)
  - New gTLDs contention resolution (e.g., auctions for contested TLDs)
    - .shop – acquired by GMO Registry for **$41.5 million**
    - .app – acquired by Google for **$25 million**
    - .tech – acquired by Radix for **$6.76 million**
    - .store – acquired by Radix for **$5.1 million**



- **Recuring revenue from gTLD registry operators** (1,131 registry operators)
  - Annual registry fee: **$25,000** per year
  - Transcation fee: **$0.25** per transcation (i.e., registrations, renewals, or transfers) after the first 50,000 transactions/ quarter

- **Recuring revenue from Registrar** (~2800 accredited registrars)
  - Application fee: **$3,500** (non-refundable)
  - Annual accreditation fee: **$4,000** per year
  - Variable accreditation fee: **$3.42 million** in 2024 (distributed among all registrar based on their market share)
  - Transaction-based fee : **$0.18** per domain per year

https://www.icann.org/en/system/files/files/icann-financial-report-fye-30jun24-en.pdf

Registry Operator Revenue

- First sale (often discounted because it is a competitive market)
- Renewal = Recuring revenue
  - .com – **154 million domains** @ $9.59 = **~$ 1,476 million**
  - .shop – **3,4 million domains** @ $30.00 = **~$ 102 million**
  - .app – **730k domains** @$15.00 = **~$10.95 million**
  - .tech – **470k domains** @$45.00 = **~$21.15 million**
  - .store – **1,6 millions domains** @35.00 = **~$56 million**

Problems introduced by new gTLDs

Unintended consequences

- **Brand protection**
  - Defensive registrations became costly for companies.
- **User confusion & trust issues**
  - Similar-looking domains increase phishing/social engineering risks.
- **Internal naming collisions**
  - Many enterprises had already deployed internal domains that now conflict with these new gTLDs.
  - Can’t rename an Active Directory.

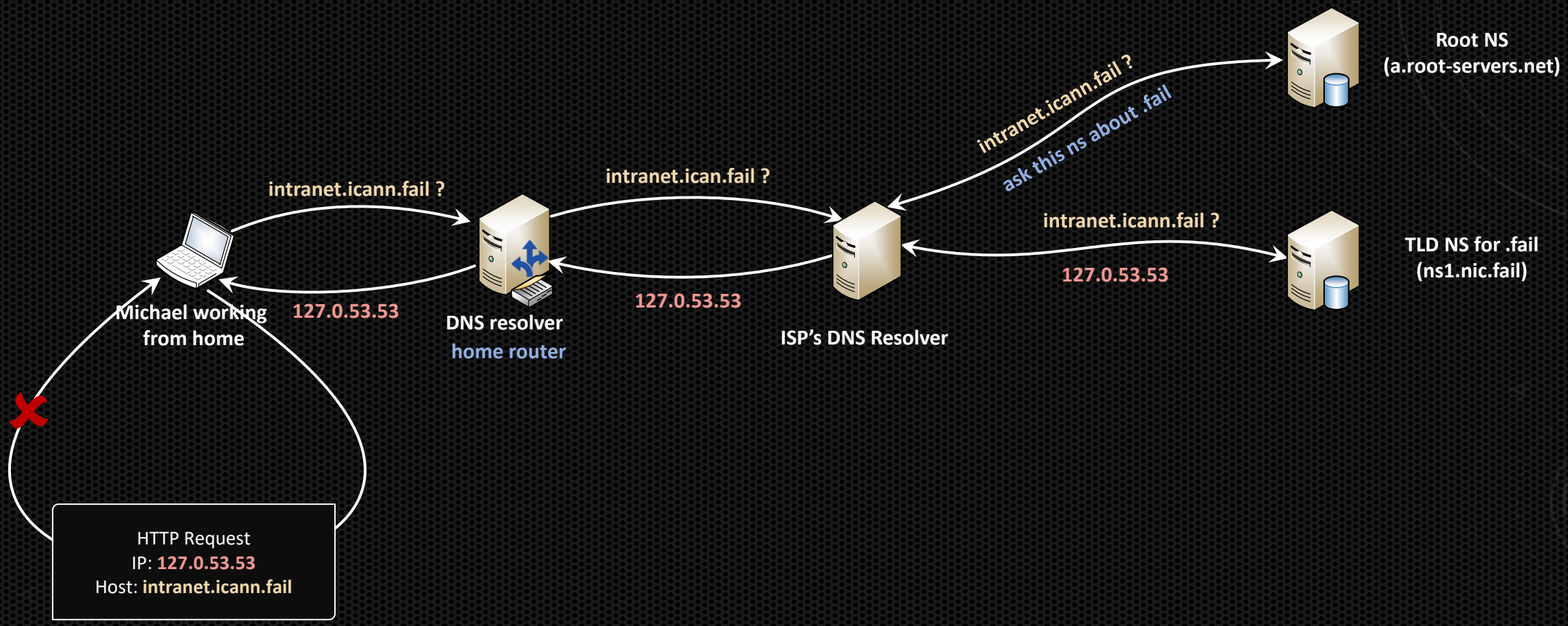
ICANN's effort to prevent name collision

"Name collision occurrence management framework" (© JAS Global Advisors)

- Restrict "high-risk" strings (e.g., **.home**, **.corp**, **.mail**)
  - but string like .homes, .llc, .inc or .email are "safe"
- **Controlled interruption** for a continuous period of no less than **90 days**.
- **Emergency rollback**, if high collision rate is detected.
- Registry operators must respond to ICANN's name collision reports within **24 hours**.

https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf

Controlled interruption



Controlled interruption

ot NS
servers.net)

S for .fail
.nic.fail)

Michael wo
from ho

HTTP Requ
IP: 127.0.5
Host: intranet.i

Methodology

Methodology

- **Objective #1**: Find internal domain names **leaked externally**
- **Objective #2**: Find internal domain names that **match a valid FQDN** (i.e., SLD.TLD)
- **Objective #3**: Find internal domain with public FQDN that are **not registered**

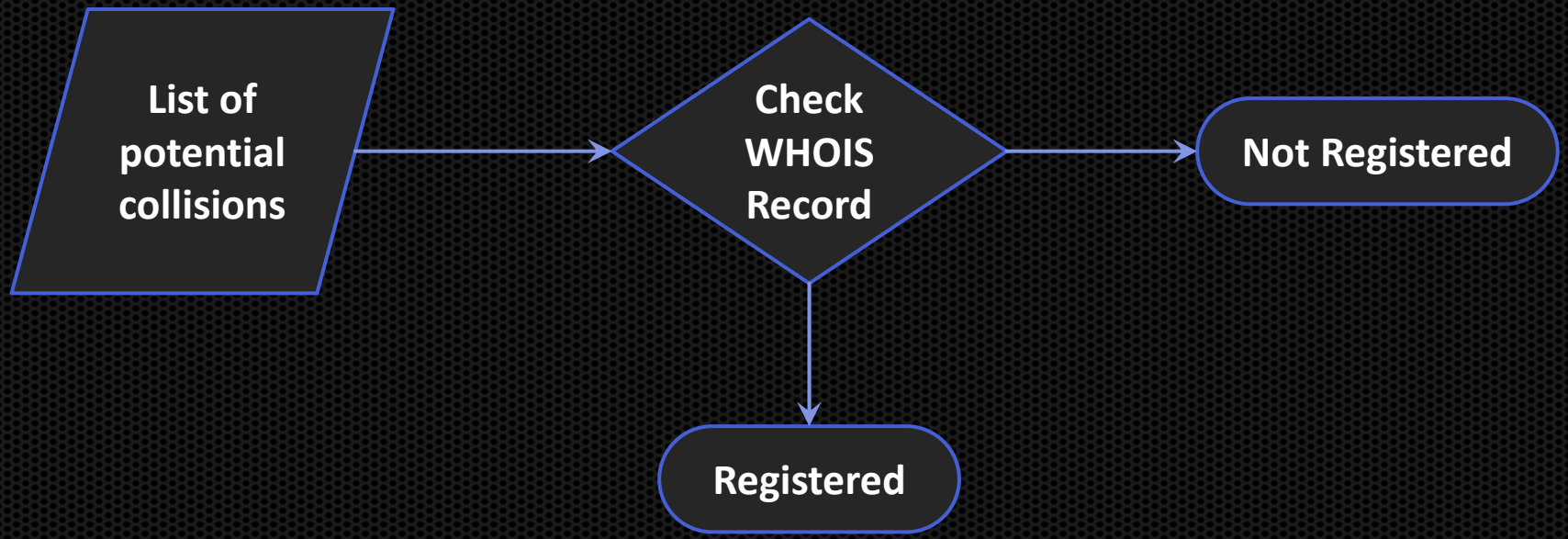
Objective #1 – Leaks of internal domain names

- Banner (e.g., Telnet, FTP, SMTP)
- SSL Self-Signed Cert
- CRL in SSL Certs
- Email Headers (e.g. Received, Message-ID)
- Content Security Policy
- NTLM Authentication
  - HTTP/HTTPS, SMTP, RDP, SQL, etc.
- TLS Services
  - RDP, SMTPS, IMAPs, FTPS, etc.

Objective #2 - TLDs prone to ~~confusion~~ collision

- ccTLDs
  - **.ad** = Active Directory (Andorra)
  - **.ms** = Microsoft (Montserrat)
  - **.io** = In/Out (British Indian Ocean Territory)
  - **.ai** = Artificial Intelligence (Anguilla)
  - **.ws** = Web Service (Western Samoa)
  - **.co** = Company (Colombia)
- gTLDs
  - **Generic business terms** (.company, .group, .tech, .global, .services)
  - **Common legal entities** (.inc, .llc, .ltd, .plc, .gmbh, .limited, .srl, .sarl)
  - **Ambiguous / Common technical terms** (.host, .email, .zone, .site, .dev, .box, .cloud)

Objective #3 – Check registration status



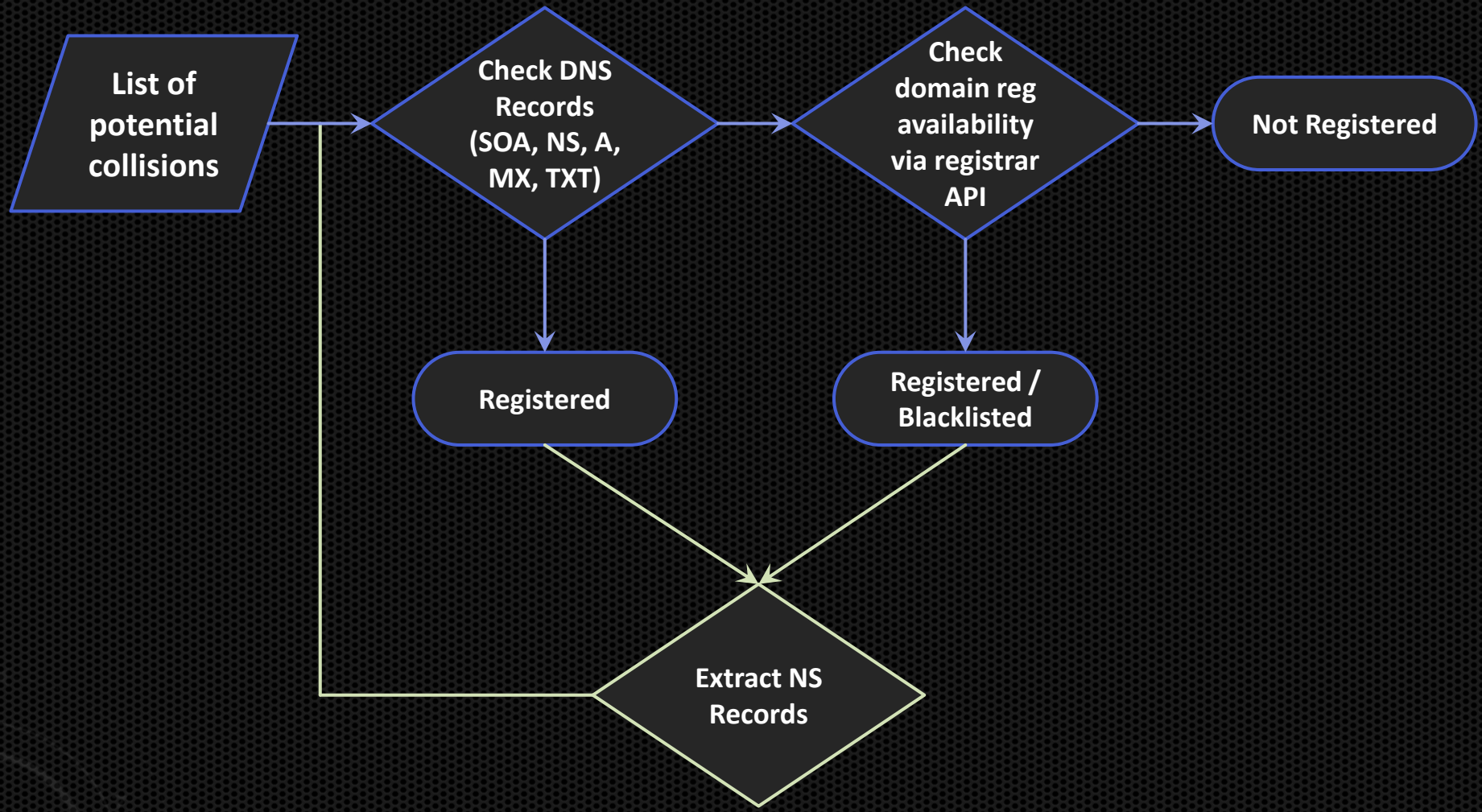

```
% WHOIS dns.lu
%% Excessive querying, grace period of      90 days
```

Objective #3 – Check registration status


```
% WHOIS dns.lu
%% Excessive querying, grace period of
```

90 days

Objective #3 – Check registration status



Examples

Examples - memrtcc.ad

censys | Certificates | names: "*.memrtcc.ad" | Search | PC

Results | Report | Docs

Certificate Filters

For all fields, see Data Definitions

Label:

3,076
3,076
3,075
3,074
2

Issuer:

1 Uns

Certificates

Results: 3,076 Time: 6.04s

AVAILABLE

memrtcc.ad

Domains include: EMAIL DNS SSL

Duration 2 years

€69.00/year

Domain info

I=MPD-

CN=P5139.memrtcc.ad

P5139.memrtcc.ad

2023-05-28 — 2023-11-27

P5139.memrtcc.ad

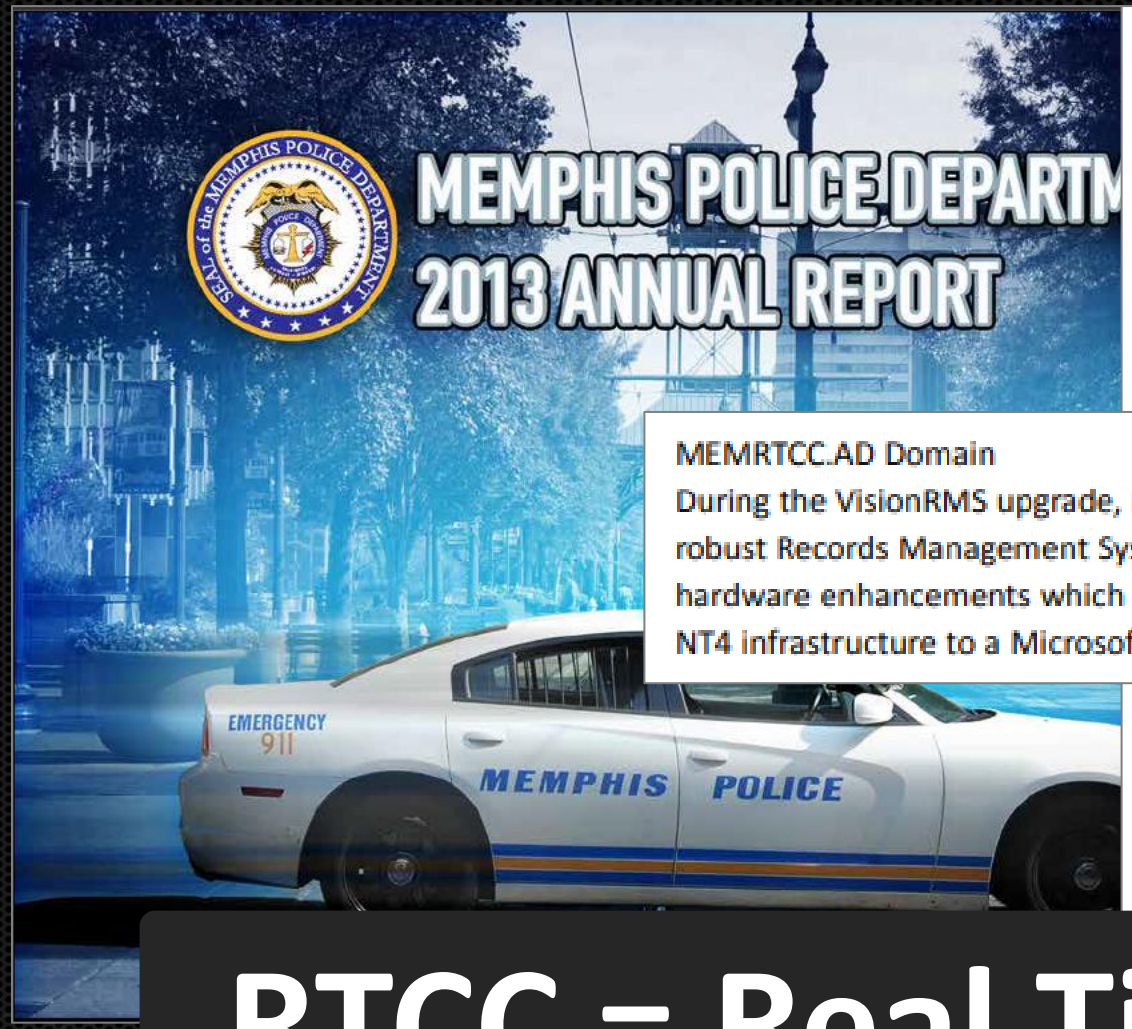
CN=P9566.memrtcc.ad

P9566.memrtcc.ad

2023-05-28 — 2023-11-27

P9566.memrtcc.ad

Examples - memrtcc.ad



Information Systems

Mission Statement

The mission of MPD's Information Technology Division is to optimize the Department's ability to protect and serve the citizens of Memphis through the efficient and innovative use of the most advanced Information Technology (IT) available. Challenges include identifying which technologies should be incorporated to achieve the greatest public safety benefit. Responsibilities include planning, developing, implementing, and

agency's compliance to the CJIS Security Policy and the Management Control Agreement.

Accomplishments for 2013

During fiscal year 2013, we made significant progress on a number of key initiatives designed to enhance services and increase operational efficiencies. Most notable were:
VisionRMS Upgrade
The IT Division of the Memphis Police Department worked with TriTech Software Systems to upgrade our 13 year old Records Management System, VisionRMS 3 TN Metro release, to Inform RMS 4.5.

MEMRTCC.AD Domain
During the VisionRMS upgrade, MPD IT enhanced its IT infrastructure to support a more robust Records Management System. Through strategic planning we were able to leverage hardware enhancements which allowed us to start migrating from an outdated Windows NT4 infrastructure to a Microsoft Windows Server Active Directory environment.

2014 Information Systems Goals

- Information Systems plans to migrate all MPD users from the antiquated, NT4 Memphis Police domain to a more robust Active Directory domain (MEM RTCC domain).
- Update the paperless Watson reporting suite from a Windows PC platform to the Android platform that allows for greater functionality.
- Complete the Vision RMS upgrade that will result in a more efficient RMS with greater functionality & storage capacity.

lans are in place for the implementation of the new yberwatch program, electronic FTO program and an lectronic bid program.

nstitute the (ACES) Automated Case Examination Service nvestigative protocol.

dd cameras to the Greater Memphis Greenline.

nhancements to our Port Security program.

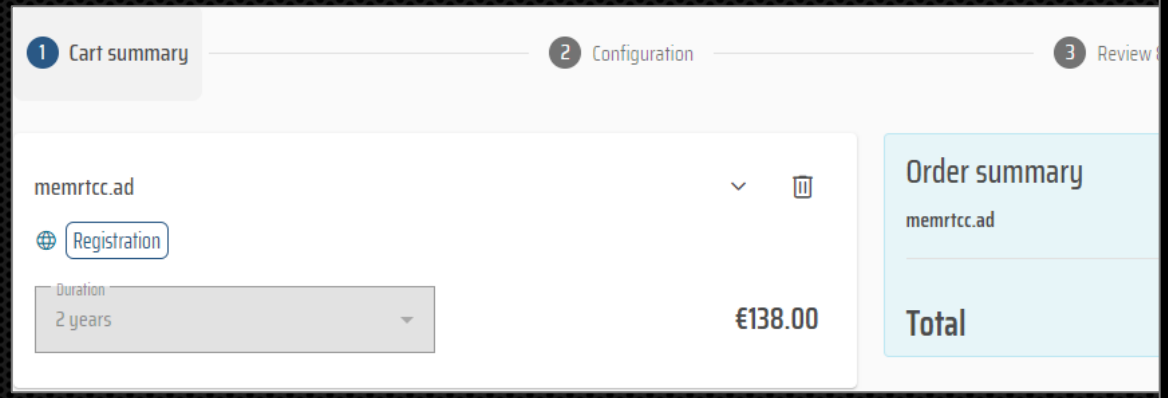
dditional SkyCop & SkyWatch surveillance platforms.

MEMRTCC.AD Domain
During the VisionRMS upgrade, MPD IT enhanced its IT infrastructure to support a more robust Records Management System. Through strategic planning we were able to leverage hardware enhancements which allowed us to start migrating from an outdated Windows NT4 infrastructure to a Microsoft Windows Server Active Directory environment.

RTCC = Real Time Crime Center

Examples - memrtcc.ad

Examples - memrtcc.ad



Dear customer,

We inform you that to proceed with the registration of an "ad" domain, the owner **must possess a local trademark in Andorra** that must be the **same as the requested domain name** or be the owner of a commercial name registered in Andorra and present the document "Register of Commerce".

Regards,
DNS Registrar

Dear Mr. Caturegli,

Thank you for contacting us.

We have a special price to **file a trademark for domain**: **320,10 €** (official fees 170,10 € + agent's fees 150,00 €).

It takes **more or less 2 weeks** to get the registration certificate and the authorization.

To file the trademark, we will need the **trademark and owner's details**, and a **power of attorney** signed in the name of the trademark's owner.

Once the authorisation is obtained, we will file the primary and secondary DNS servers at the domain.ad management (nic.ad).

Regards,
Trademark attorney
Andorra

Examples - memrtcc.ad

Dear customer,

We inform you that to proce
an "ad" domain, the owner **n**
trademark in Andorra that m
requested domain name or b
commercial name registered
the document "Register of Co

Regards,
DNS Regist

OFICINA DE MARQUES
I PATENTS D'ANDORRA

CERTIFICAT DE REGISTRE

1 NÚMERO DEL REGISTRE DE MARCA

(NÚMERO DEL REGISTRO DE MARCA / TRADEMARK REGISTRATION NUMBER / NUMÉRO D'ENREGISTREMENT)

46172

2 REPRODUCCIÓ DE LA MARCA

(REPRODUCCIÓN DE LA MARCA / REPRODUCTION OF TRADEMARK / REPRODUCTION DE LA MARQUE)

memrtcc

3 DATA DE REGISTRE

(FECHA DE REGISTRO / DATE OF REGISTRATION / DATE D'ENREGISTREMENT)

19-01-2024 12:40

4 DATA DE VENCIMENT DEL REGISTRE

(FECHA DE VENCIMIENTO DEL REGISTRO / DATE OF EXPIRATION OF REGISTRATION / DATE D'ÉCHÉANCE DE L'ENREGISTREMENT)

19-01-2034

5 NOM DEL TITULAR

(NOMBRE DEL TITULAR / NAME OF OWNER / NOM DU TITULAIRE)

Denominació social *(Denominación social / Name of company / Dénomination officielle complète)*
SERALYS
Forma jurídica *(Forma jurídica / Legal form of constitution / Forme juridique)*
SÀRL

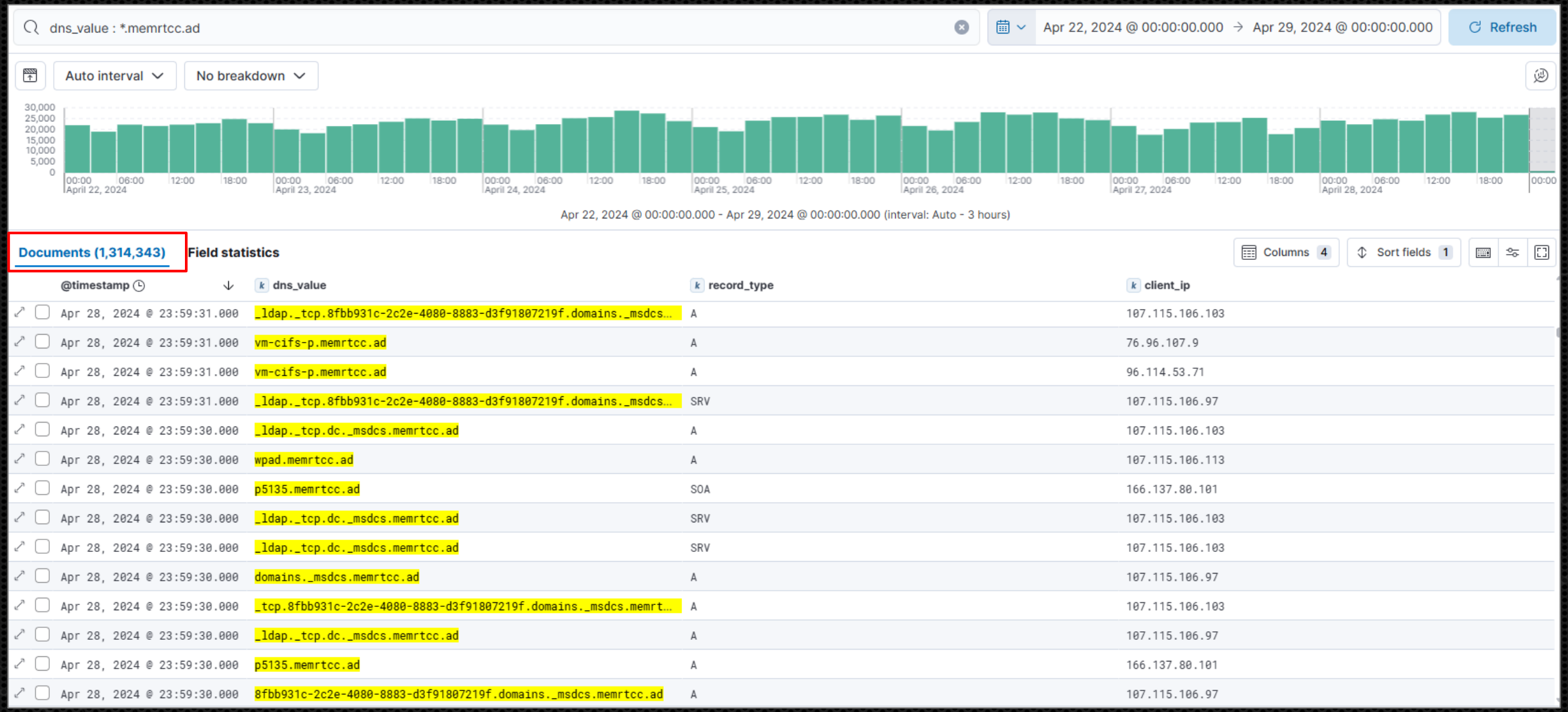
ark for domain:
s fees 150,00 €).

registration

trademark and
ey signed in the

will file the primary
ain.ad management

Examples - memrtcc.ad



@timestamp	dns_value	record_type	client_ip
Apr 28, 2024 @ 23:59:31.000	_ldap._tcp.8fbb931c-2c2e-4080-8883-d3f91807219f.domains._msdcs...	A	107.115.106.103
Apr 28, 2024 @ 23:59:31.000	vm-cifs-p.memrtcc.ad	A	76.96.107.9
Apr 28, 2024 @ 23:59:31.000	vm-cifs-p.memrtcc.ad	A	96.114.53.71
Apr 28, 2024 @ 23:59:31.000	_ldap._tcp.8fbb931c-2c2e-4080-8883-d3f91807219f.domains._msdcs...	SRV	107.115.106.97
Apr 28, 2024 @ 23:59:30.000	_ldap._tcp.dc._msdcs.memrtcc.ad	A	107.115.106.103
Apr 28, 2024 @ 23:59:30.000	wpad.memrtcc.ad	A	107.115.106.113
Apr 28, 2024 @ 23:59:30.000	p5135.memrtcc.ad	SOA	166.137.80.101
Apr 28, 2024 @ 23:59:30.000	_ldap._tcp.dc._msdcs.memrtcc.ad	SRV	107.115.106.103
Apr 28, 2024 @ 23:59:30.000	_ldap._tcp.dc._msdcs.memrtcc.ad	SRV	107.115.106.103
Apr 28, 2024 @ 23:59:30.000	domains._msdcs.memrtcc.ad	A	107.115.106.97
Apr 28, 2024 @ 23:59:30.000	_tcp.8fbb931c-2c2e-4080-8883-d3f91807219f.domains._msdcs.memrt...	A	107.115.106.103
Apr 28, 2024 @ 23:59:30.000	_ldap._tcp.dc._msdcs.memrtcc.ad	A	107.115.106.97
Apr 28, 2024 @ 23:59:30.000	p5135.memrtcc.ad	A	166.137.80.101
Apr 28, 2024 @ 23:59:30.000	8fbb931c-2c2e-4080-8883-d3f91807219f.domains._msdcs.memrtcc.ad	A	107.115.106.97

Examples - memrtcc.ad

- Reported to Memphis Deputy CIO via email – (April 2nd)
- Reported to Memphis Deputy CIO via common connection – (April 3rd)
- Reported to CIO@memphistn.gov (April 17th)
- Reported to vulnerability.disclosure.prog@hq.dhs.gov (April 22nd)
- Reached out to fellow hacker in Memphis/DC901 (May 15th)
- Spoke with Memphis FBI Special Agent (June 17th)
- Spoke to Brian Krebs (August 5th)
- Memphis Information Security Manager finally reached out (Aug 13th)
- Brian Krebs published his article (August 23rd)

https://krebsonsecurity.com/2024/08/local-networks-go-global-when-domain-names-collide/

Examples - .ad

- **1,129 registered domain** in the .ad TLD
- **3,802 trusted SSL certificates** in Censys certificate database
- **25,689 self-signed certificates** in Censys certificate database
- **2,795 unique sld.tld** extracted
- **2,484 not registered** (89%)

Examples - local.ad / internal.ad

Examples - local.ad / internal.ad

OFICINA DE MARQUES
I PATENTS D'ANDORRA

1 NÚMERO DEL REGISTRE DE MARCA

(NÚMERO DEL REGISTRO DE MARCA / TRADEMARK REGISTRATION NUMBER / NUMÉRO D'ENREGISTREMENT)

46207

2 REPRODUCCIÓ DE LA MARCA

(REPRODUCCIÓN DE LA MARCA / REPRODUCTION OF TRADEMARK / REPRODUCTION DE LA MARQUE)

INTERNAL

3 DATA DE REGISTRE

(FECHA DE REGISTRO / DATE OF REGISTRATION / DATE D'ENREGISTREMENT)

26-01-2024 11:53

4 DATA DE VENCIMENT DEL REGISTRE

(FECHA DE VENCIMIENTO DEL REGISTRO / DATE OF EXPIRATION OF REGISTRATION / DATE D'ÉCHÉANCE DE L'ENREGISTREMENT)

26-01-2034

5 NOM DEL TITULAR

(NOMBRE DEL TITULAR / NAME OF OWNER / NOM DU TITULAIRE)

Denominació social *(Denominación social / Name of company / Dénomination officielle complète)*
SERALYS
Forma jurídica *(Forma jurídica / Legal form of constitution / Forme juridique)*
SÀRL

OFICINA DE MARQUES
I PATENTS D'ANDORRA

1 NÚMERO DEL REGISTRE DE MARCA

(NÚMERO DEL REGISTRO DE MARCA / TRADEMARK REGISTRATION NUMBER / NUMÉRO D'ENREGISTREMENT)

43965

2 REPRODUCCIÓ DE LA MARCA

(REPRODUCCIÓN DE LA MARCA / REPRODUCTION OF TRADEMARK / REPRODUCTION DE LA MARQUE)

local

3 DATA DE REGISTRE

(FECHA DE REGISTRO / DATE OF REGISTRATION / DATE D'ENREGISTREMENT)

09-03-2022 13:09

4 DATA DE VENCIMENT DEL REGISTRE

(FECHA DE VENCIMIENTO DEL REGISTRO / DATE OF EXPIRATION OF REGISTRATION / DATE D'ÉCHÉANCE DE L'ENREGISTREMENT)

09-03-2032

5 NOM DEL TITULAR

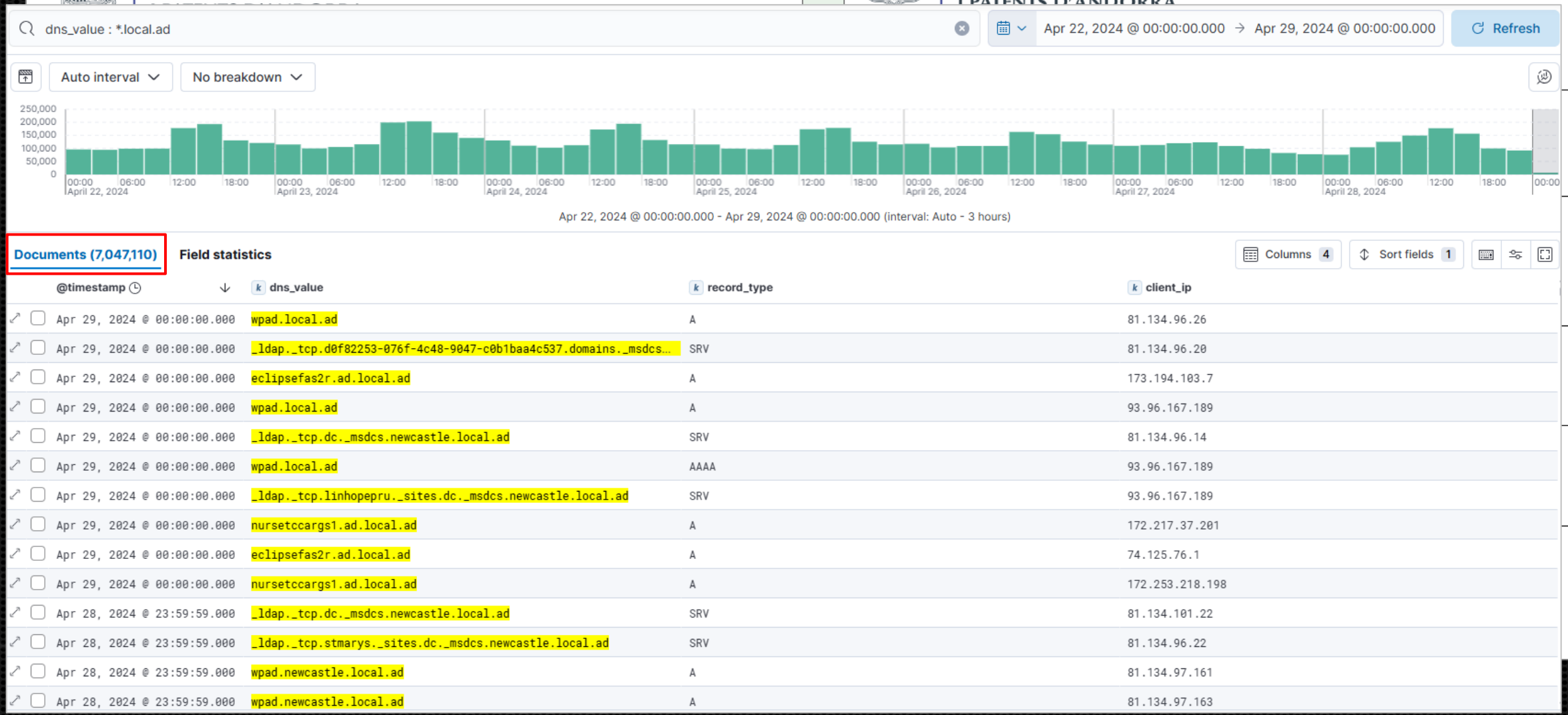
(NOMBRE DEL TITULAR / NAME OF OWNER / NOM DU TITULAIRE)

Denominació social *(Denominación social / Name of company / Dénomination officielle complète)*
SERALYS
Forma jurídica *(Forma jurídica / Legal form of constitution / Forme juridique)*
SÀRL

Examples - local.ad / internal.ad

OFICINA DE MARQUES

OFICINA DE MARQUES
I PATENTS D'ANDORRA



@timestamp	dns_value	record_type	client_ip
Apr 29, 2024 @ 00:00:00.000	wpad.local.ad	A	81.134.96.26
Apr 29, 2024 @ 00:00:00.000	_ldap._tcp.d0f82253-076f-4c48-9047-c0b1baa4c537.domains._msdcs…	SRV	81.134.96.20
Apr 29, 2024 @ 00:00:00.000	eclipsefas2r.ad.local.ad	A	173.194.103.7
Apr 29, 2024 @ 00:00:00.000	wpad.local.ad	A	93.96.167.189
Apr 29, 2024 @ 00:00:00.000	_ldap._tcp.dc._msdcs.newcastle.local.ad	SRV	81.134.96.14
Apr 29, 2024 @ 00:00:00.000	wpad.local.ad	AAAA	93.96.167.189
Apr 29, 2024 @ 00:00:00.000	_ldap._tcp.linhopepru._sites.dc._msdcs.newcastle.local.ad	SRV	93.96.167.189
Apr 29, 2024 @ 00:00:00.000	nursetccargs1.ad.local.ad	A	172.217.37.201
Apr 29, 2024 @ 00:00:00.000	eclipsefas2r.ad.local.ad	A	74.125.76.1
Apr 29, 2024 @ 00:00:00.000	nursetccargs1.ad.local.ad	A	172.253.218.198
Apr 28, 2024 @ 23:59:59.000	_ldap._tcp.dc._msdcs.newcastle.local.ad	SRV	81.134.101.22
Apr 28, 2024 @ 23:59:59.000	_ldap._tcp.stmarys._sites.dc._msdcs.newcastle.local.ad	SRV	81.134.96.22
Apr 28, 2024 @ 23:59:59.000	wpad.newcastle.local.ad	A	81.134.97.161
Apr 28, 2024 @ 23:59:59.000	wpad.newcastle.local.ad	A	81.134.97.163

Examples - local.ad / internal.ad

- Over **1,200 different domains / companies** colliding with these domains.
- In 2020, Microsoft purchased “corp.com” before the domain was put for auction.
- Reached out to Microsoft via MSRC, but didn’t even make the triage.
- Technical details relayed internally at Microsoft (thanks Dr. Nestori Syynimaa !).
- Microsoft corporate domains service group reached out.
- Reopened MSRC case and “bough” the domains from us.
- But...

Examples - local.ad / internal.ad

- Over **1,200 different domains / companies** colliding with these domains.
- In 2020, Microsoft purchased “corp.com” before the domain was put for auction.
- Reached out to Microsoft via MSRC, but didn’t even make the triage.
- Technical details relayed internally at Microsoft (thanks Dr. Nestori Syynimaa !).
- M
- Re
- Bu

Microsoft laying off about 9,000 employees in latest round of cuts

PUBLISHED WED, JUL 2 2025•9:07 AM EDT | UPDATED WED, JUL 2 2025•4:11 PM EDT

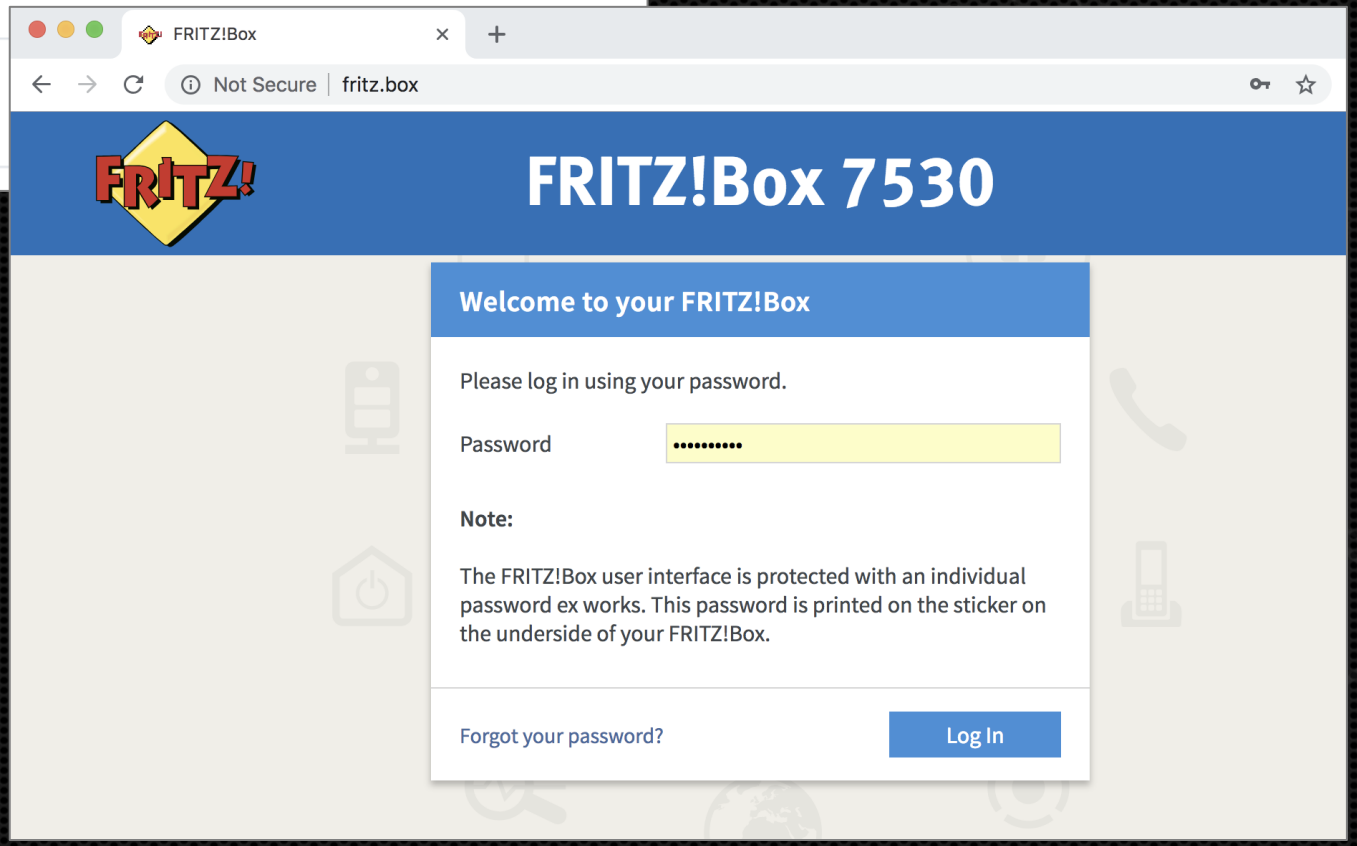
Jordan Novet
@IN/JORDANNOVET/

SHARE

Examples - .box

Introducing .box - The World's First Blockchain Native, DNS Routable Domain

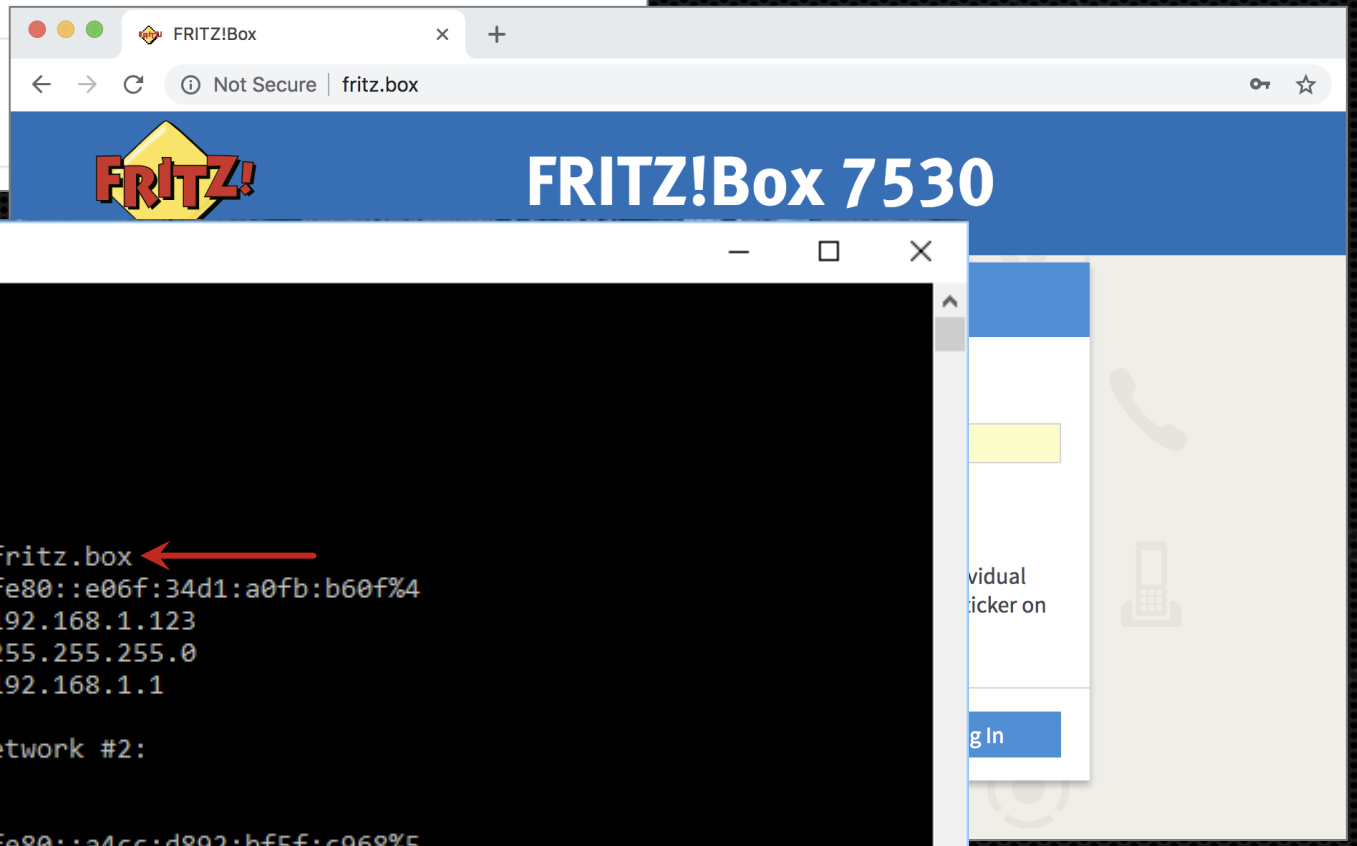
PR Newswire
Thu, Jan 18, 2024 • 3 min read



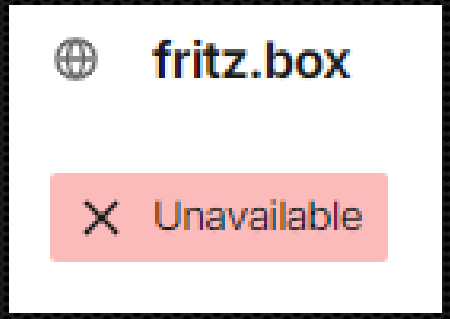
Examples - .box

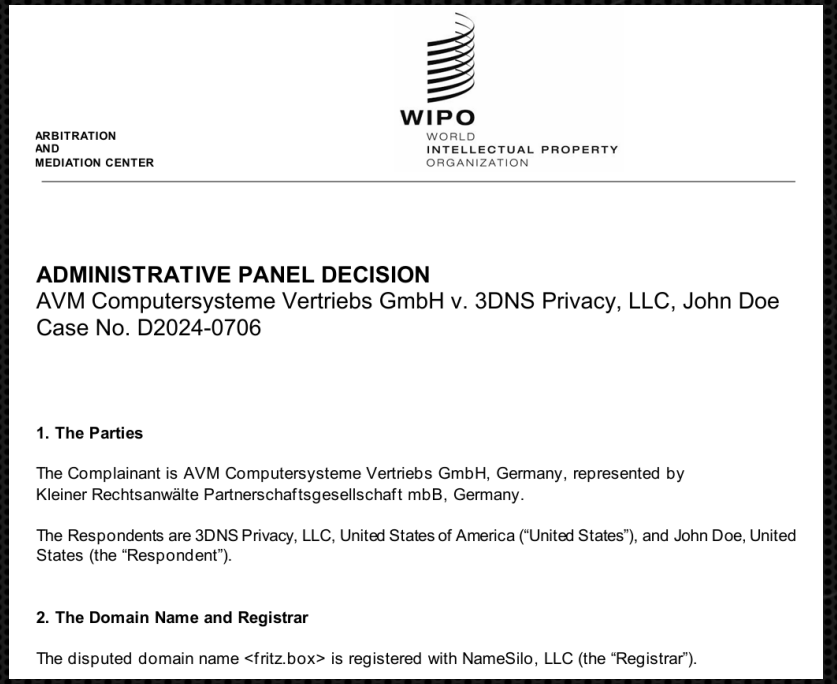
Introducing .box - The World's First Blockchain Native, DNS Routable Domain

PR Newswire
Thu, Jan 18, 2024 • 3 min read



Examples - .box





ARBITRATION AND MEDIATION CENTER

WIPO WORLD INTELLECTUAL PROPERTY ORGANIZATION

ADMINISTRATIVE PANEL DECISION
AVM Computersysteme Vertriebs GmbH v. 3DNS Privacy, LLC, John Doe
Case No. D2024-0706

1. The Parties

The Complainant is AVM Computersysteme Vertriebs GmbH, Germany, represented by Kleiner Rechtsanwälte Partnerschaftsgesellschaft mbB, Germany.

The Respondents are 3DNS Privacy, LLC, United States of America ("United States"), and John Doe, United States (the "Respondent").

2. The Domain Name and Registrar

The disputed domain name <fritz.box> is registered with NameSilo, LLC (the "Registrar").

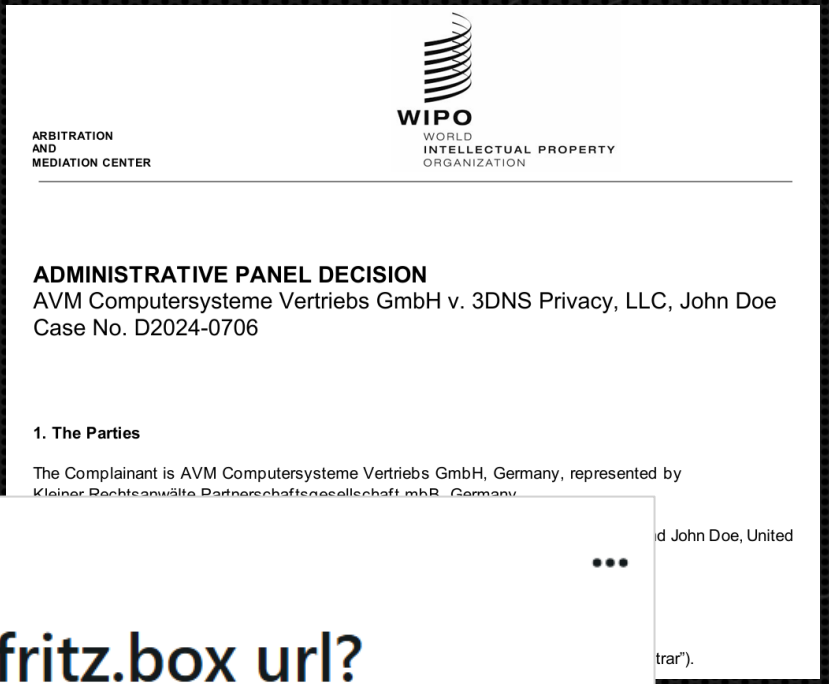
- **Jan 18, 2024** - .box gTLD **registration publicly opens**
- **Jan 22, 2024** - **.fritz.box**, o2.box and wpad.box registered by 0xDc8c[...]Fe8B
- **Jan 22, 2024** - domain fritz.box listed on opensea.io for **420 ETH** (~ $ 1 million)
- **Jan 29, 2024** - Domain fritz.box re-listed on opensea.io for **99 ETH** ($ 250,000)
- **Feb 15 , 2024** - AVM open **complaint with WIPO** (World Intellectual Property Organization)
- **Apr 12, 2024** - WIPO decided to **transfer the domain to AVM**

https://www.wipo.int/amc/en/domains/decisions/pdf/2024/d2024-0706.pdf

Examples - .box

fritz.box

Unavailable



ARBITRATION AND MEDIATION CENTER

WIPO WORLD INTELLECTUAL PROPERTY ORGANIZATION

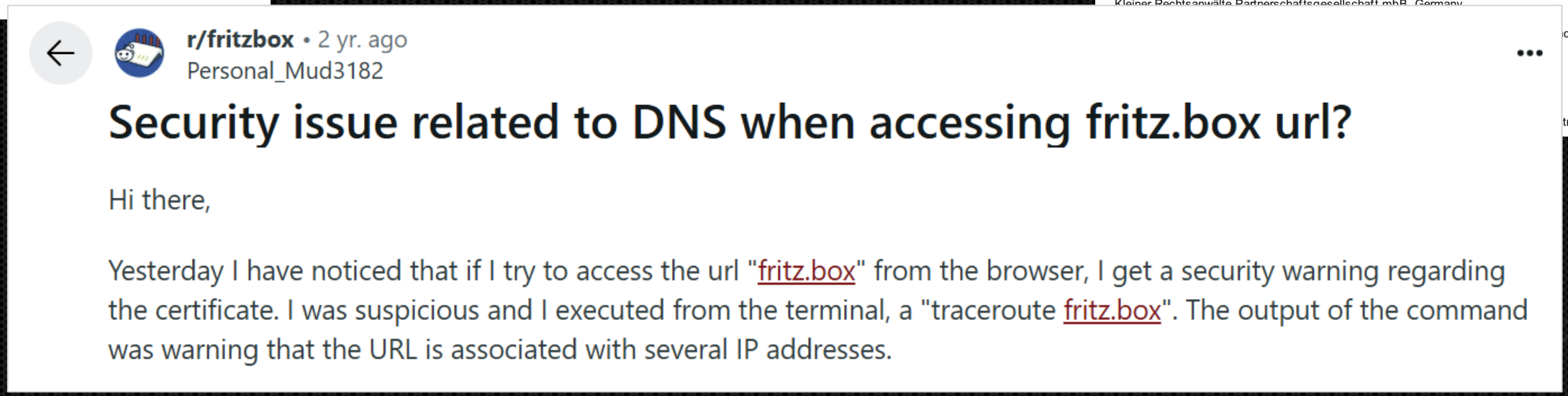
ADMINISTRATIVE PANEL DECISION
AVM Computersysteme Vertriebs GmbH v. 3DNS Privacy, LLC, John Doe
Case No. D2024-0706

1. The Parties

The Complainant is AVM Computersysteme Vertriebs GmbH, Germany, represented by

d John Doe, United

trar").



r/fritzbox • 2 yr. ago
Personal_Mud3182

Security issue related to DNS when accessing fritz.box url?

Hi there,

Yesterday I have noticed that if I try to access the url "fritz.box" from the browser, I get a security warning regarding the certificate. I was suspicious and I executed from the terminal, a "traceroute fritz.box". The output of the command was warning that the URL is associated with several IP addresses.

- **Apr 12, 2024** - WIPO decided to **transfer the domain to AVM**

https://www.wipo.int/amc/en/domains/decisions/pdf/2024/d2024-0706.pdf

Examples – zyxel.box / sphairon.box

censys | Certificates | names:"*sphairon.box" | Search | PC

Results | Report | Docs

Certificate Filters

For all fields, see Data Definitions

Label:

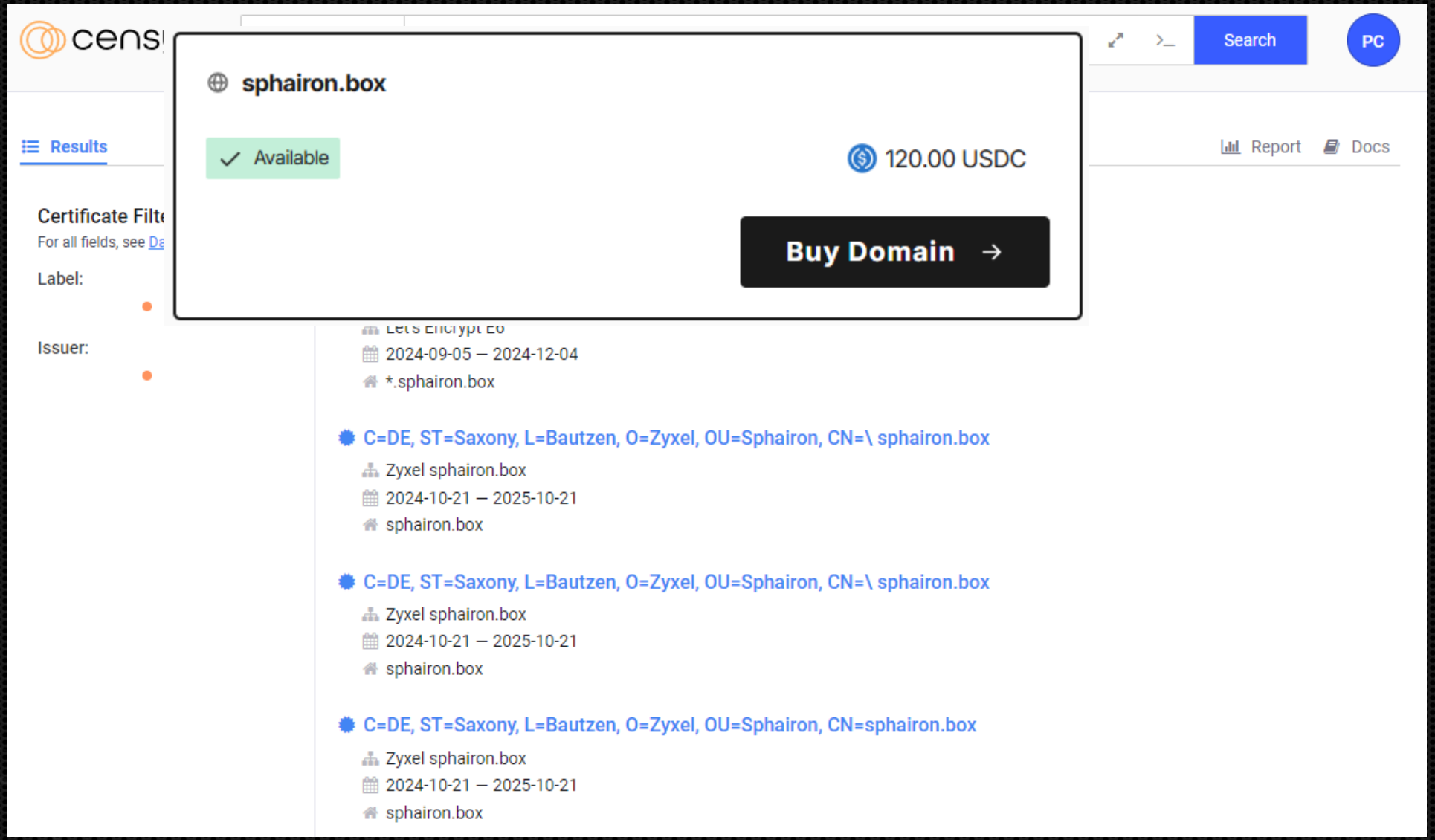
Issuer:

Certificates

Results: 49,794 Time: 16.55s

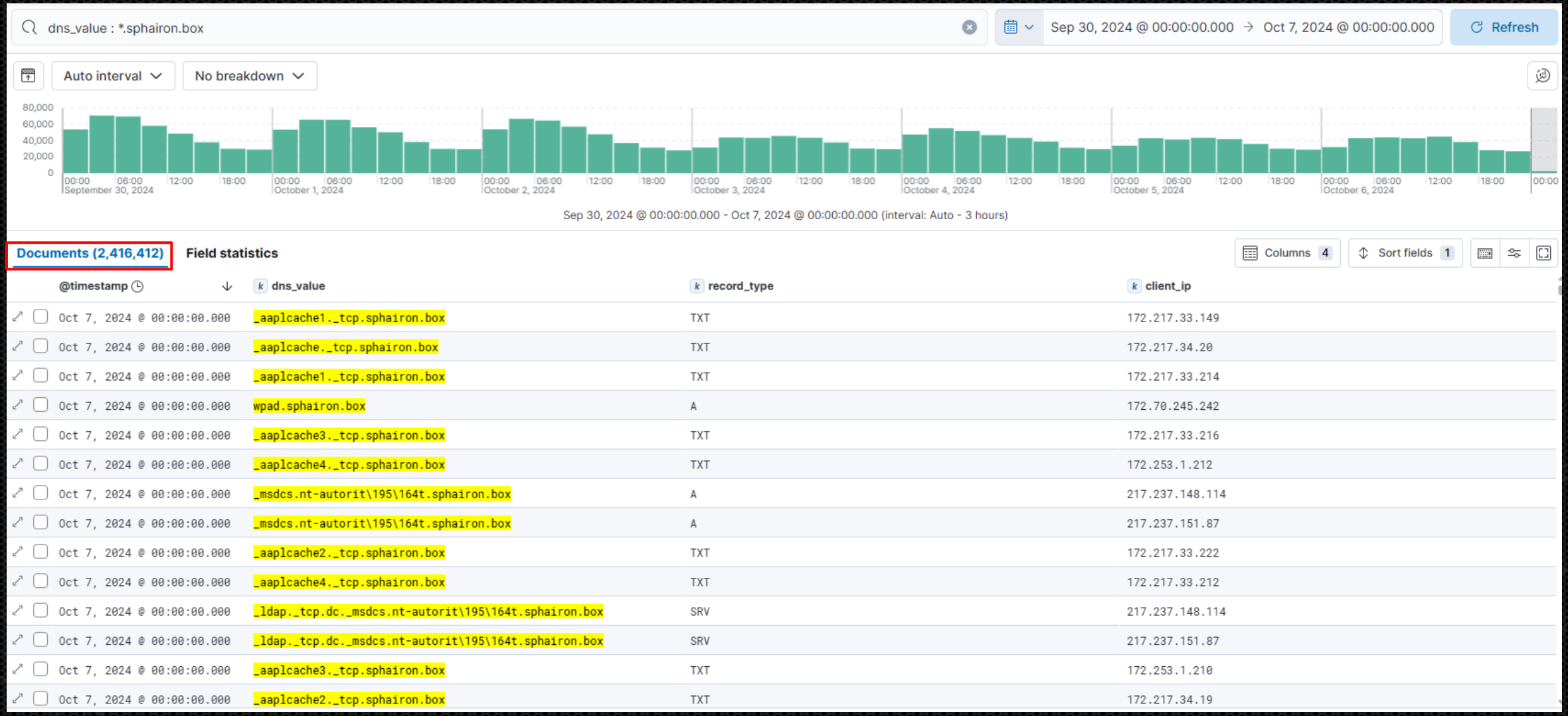
- CN=*.sphairon.box
  - Let's Encrypt E6
  - 2024-09-05 — 2024-12-04
  - *.sphairon.box
- C=DE, ST=Saxony, L=Bautzen, O=Zyxel, OU=Sphairon, CN=\ sphairon.box
  - Zyxel sphairon.box
  - 2024-10-21 — 2025-10-21
  - sphairon.box
- C=DE, ST=Saxony, L=Bautzen, O=Zyxel, OU=Sphairon, CN=\ sphairon.box
  - Zyxel sphairon.box
  - 2024-10-21 — 2025-10-21
  - sphairon.box
- C=DE, ST=Saxony, L=Bautzen, O=Zyxel, OU=Sphairon, CN=sphairon.box
  - Zyxel sphairon.box
  - 2024-10-21 — 2025-10-21
  - sphairon.box

Examples – zyxel.box / sphairon.box



Examples – zyxel.box / sphairon.box

Examples – zyxel.box / sphairon.box



@timestamp	dns_value	record_type	client_ip
Oct 7, 2024 @ 00:00:00.000	_aaplcache1._tcp.sphairon.box	TXT	172.217.33.149
Oct 7, 2024 @ 00:00:00.000	_aaplcache._tcp.sphairon.box	TXT	172.217.34.20
Oct 7, 2024 @ 00:00:00.000	_aaplcache1._tcp.sphairon.box	TXT	172.217.33.214
Oct 7, 2024 @ 00:00:00.000	wpad.sphairon.box	A	172.70.245.242
Oct 7, 2024 @ 00:00:00.000	_aaplcache3._tcp.sphairon.box	TXT	172.217.33.216
Oct 7, 2024 @ 00:00:00.000	_aaplcache4._tcp.sphairon.box	TXT	172.253.1.212
Oct 7, 2024 @ 00:00:00.000	_msdcs.nt-autorit\195\164t.sphairon.box	A	217.237.148.114
Oct 7, 2024 @ 00:00:00.000	_msdcs.nt-autorit\195\164t.sphairon.box	A	217.237.151.87
Oct 7, 2024 @ 00:00:00.000	_aaplcache2._tcp.sphairon.box	TXT	172.217.33.222
Oct 7, 2024 @ 00:00:00.000	_aaplcache4._tcp.sphairon.box	TXT	172.217.33.212
Oct 7, 2024 @ 00:00:00.000	_ldap._tcp.dc._msdcs.nt-autorit\195\164t.sphairon.box	SRV	217.237.148.114
Oct 7, 2024 @ 00:00:00.000	_ldap._tcp.dc._msdcs.nt-autorit\195\164t.sphairon.box	SRV	217.237.151.87
Oct 7, 2024 @ 00:00:00.000	_aaplcache3._tcp.sphairon.box	TXT	172.253.1.210
Oct 7, 2024 @ 00:00:00.000	_aaplcache2._tcp.sphairon.box	TXT	172.217.34.19

Examples – zyxel.box / sphairon.box

Hi Philippe,

Thanks for reaching out. Based on the IP list you provided, we observed that zyxel.box and sphairon.box were resolved from IP addresses located all over the world. **We believe that most of the sources are not from a LAN-based host behind a Zyxel CPE** since our devices using those two domains are only deployed in some regions in Europe. Although **the level of potential risk exposure is relatively low**.

Regards,
Zyxel PSIRT

Examples – zyxel.box / sphairon.box

Hi Philippe,

Thanks for reaching
provided, we observ
were resolved from
world. **We believe th**
from a LAN-based h
devices using those
some regions in Euro
risk exposure is relat

Regards,
Zyxel PSIRT

```
[HTTP] GET request from: ::ffff:217.91.154.236  URL: /wpad.dat
[HTTP] NTLMv2 Client    : 217          6
[HTTP] NTLMv2 Username  : DEN          eller
[HTTP] NTLMv2 Hash      : moeller::DENT01.DOM:c3be3a7463e43e5e:4A5EF50C8367FB1                908C8BA:01010000
500360032003300010001E00570049004E002D00470032005800500430031004200410048003200                1400350036003200
20058005A00430031004200410048003200330002E00350036003200330002E004C004F00430041                1400350036003200
0000020000034428 0E820D06A7A133827586FB76F50369BF82A9EA88E14A0F39DFDA55631DB0A                  0000000000000000
E00730070006800610069007200 6F006E002E0062006F00780000000000000000000000
[HTTP] WPAD (auth) file sent to 217.91.154.236
[HTTP] Sending NTLM authentication request to 79.192.32.204
[HTTP] Sending NTLM authentication request to 87.164.35.34
[HTTP] Sending NTLM authentication request to 91.60.202.8
[HTTP] Sending NTLM authentication request to 79.192.32.204
[HTTP] Sending NTLM authentication request to 93.241.71.209
[HTTP] GET request from: ::ffff:93.241.71.209  URL: /wpad.dat
[HTTP] Sending NTLM authentication request to 79.192.32.204
[HTTP] NTLMv2 Client    : 93           9
[HTTP] NTLMv2 Username  : RE           \Reservierung2
[HTTP] NTLMv2 Hash      : Re           2::RESERVIERUNG:ca25cf4c28766b70:5FE936F              3EBC89291B31CFE:
200080035003600320033000100 1E00570049004E002D00470032005800500430031004200410              3300040014003500
D00470032005800 5A00430031004200410048003200330002E00350036003200330002E004C004F              4C000500140035 00
0000100000000 2000002E762665F73A2B7F083442382691 18D665F8BBCDDF359A026F72CEB9B3              1000000000000000
10064002E007A00790078006500 6C002E0062006F00780000000000000000000000
[HTTP] WPAD (auth) file sent to 93.241.71.209
```

Examples – zyxel.box / sphairon.box

Hi Philippe,

Thanks for reaching …
provided, we observ…
were resolved fr…
world. **We believ…**
from a LAN-base…
devices using th…
some regions in …
risk exposure is …

Regards,
Zyxel PSIRT

```
[HTTP] GET request from: ::ffff:217.91.154.236  URL: /wpad.dat
[HTTP] NTLMv2 Client   : 217 [redacted] 6
[HTTP] NTLMv2 Username : DEN [redacted] eller
[HTTP] NTLMv2 Hash     : moeller::DENT01.DOM:c3be3a7463e43e5e:4A5EF50C8367FB1 [redacted] 908C8BA:01010000
500360032003300010010F00570049004F002D0047003200580058005A004300310042004100480032 [redacted] 1400350036003200
3002E004C004F00430041 [redacted] 1400350036003200
E14A0F39DFDA55631DB0A [redacted] 0000000000000000
000000000000
204
34
8
204
209
d.dat
204
5cf4c28766b70:5FE936F [redacted] 3EBC89291B31CFE:
8005A0043003100420041 [redacted] 3300040014003500
600320033002E004C004F [redacted] 4C00050014003500
BCDDF359A026F72CEB9B3 [redacted] 1000000000000000
0000000
```

Hi Philippe,

Thanks for providing the updated PoC. Based on the traffic you captured, we believe it **could result in potential risks** if the hosts behind a Zyxel CPE configured an external DNS server/resolver rather than the CPE itself. To prevent our customers' risk exposure, **we plan to register the domain names** used in the CPE.

How can we proceed?

Regards,
Zyxel PSIRT

Examples – zyxel.box / sphairon.box

Hi Philippe,

Thanks for reaching
provided, we observ
were resolved fr
world. **We believ**
from a LAN-base
devices using th
some regions in
risk exposure is

Regards,
Zyxel PSIRT

```
[HTTP] GE
[HTTP] NTI
[HTTP] NTI
[HTTP] NTI
5003600320
```

Hi Philippe,

Thanks for pr
traffic you ca
potential risk
configured a
the CPE itself
we plan to re

How can we

Regards,
Zyxel PSIRT


```
01010000
36003200
36003200
00000000
1B31CFE:
14003500
14003500
00000000
```

Examples – zyxel.box / sphairon.box

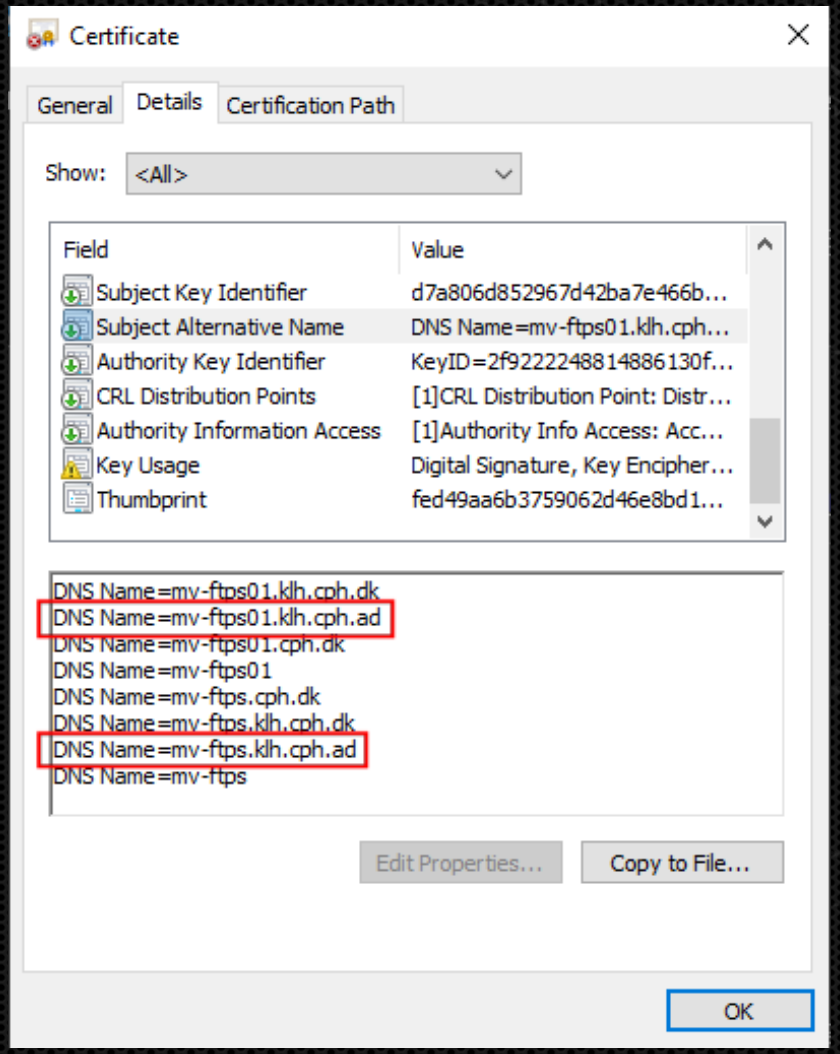
But...

```
└─$ dig @a.nic.box zyxel.box
;; BADCOOKIE, retrying.

; <<>> DiG 9.20.4-4-Debian <<>> @a.nic.box zyxel.box
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35154
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3e38eb2c0e81d32201000000683b6608de7ebb29b14f81d9 (good)
;; QUESTION SECTION:
;zyxel.box.                     IN      A

;; AUTHORITY SECTION:
zyxel.box.              3600    IN      NS      ns1.srls.io.
zyxel.box.              3600    IN      NS      ns2.srls.io.

;; Query time: 0 msec
;; SERVER: 194.169.218.139#53(a.nic.box) (UDP)
;; WHEN: Sat May 31 16:26:48 EDT 2025
;; MSG SIZE  rcvd: 109
```

```
└─$ dig @a.nic.box sphairon.box
;; BADCOOKIE, retrying.

; <<>> DiG 9.20.4-4-Debian <<>> @a.nic.box sphairon.box
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12677
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b693cd167868afcc01000000683b6684ac6b591990be0af6 (good)
;; QUESTION SECTION:
;sphairon.box.                  IN      A

;; AUTHORITY SECTION:
sphairon.box.           3600    IN      NS      ns1.srls.io.
sphairon.box.           3600    IN      NS      ns2.srls.io.

;; Query time: 0 msec
;; SERVER: 194.169.218.139#53(a.nic.box) (UDP)
;; WHEN: Sat May 31 16:28:52 EDT 2025
;; MSG SIZE  rcvd: 112
```

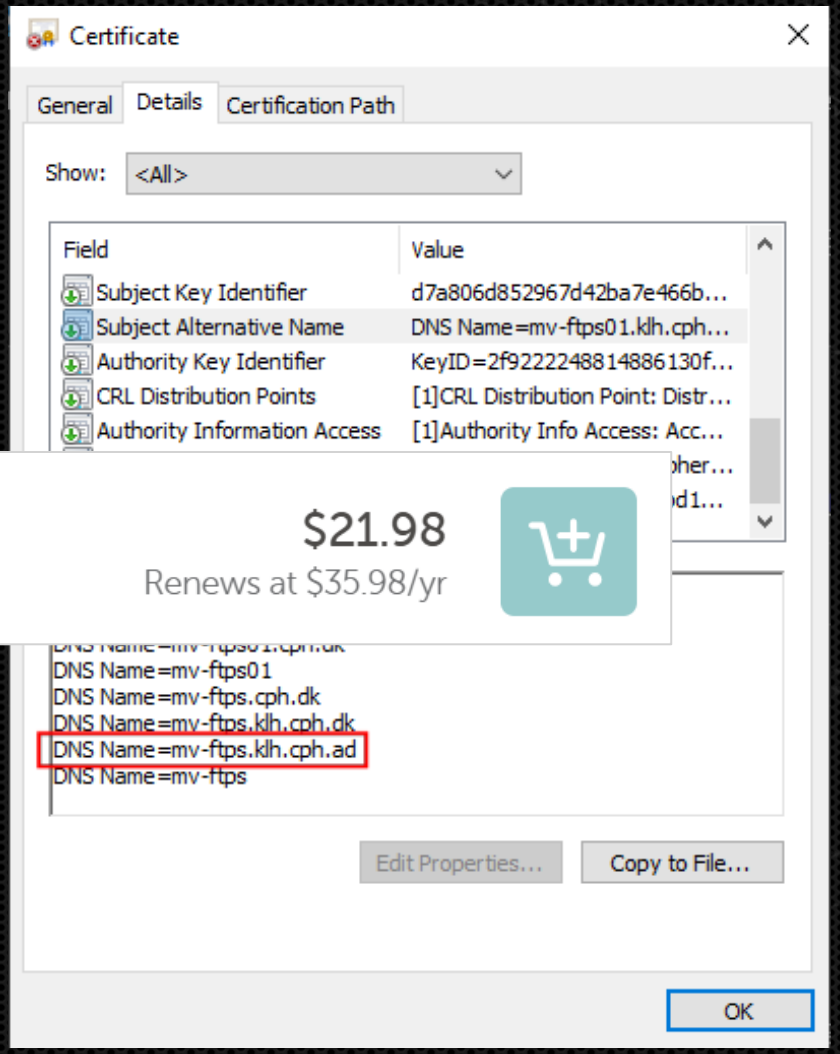
Example – ~~cph.dk~~ / cph.ad

```
└─$ openssl s_client -connect ftps.cph.dk:21 -starttls ftp
Connecting to 193.110.198.42
CONNECTED(00000003)
depth=1 DC=ad, DC=cph, DC=klh, CN=CPH Issuing CA SHA256-1
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN=mv-ftps01.klh.cph.dk
verify return:1
---
Certificate chain
 0 s:CN=mv-ftps01.klh.cph.dk
   i:DC=ad, DC=cph, DC=klh, CN=CPH Issuing CA SHA256-1
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Aug 15 08:32:18 2025 GMT; NotAfter: Aug 15 08:32:18 2027 GMT
 1 s:DC=ad, DC=cph, DC=klh, CN=CPH Issuing CA SHA256-1
   i:CN=CPH Root CA SHA256-1
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Dec 16 09:55:58 2020 GMT; NotAfter: Dec 16 10:05:58 2030 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIFJTCCBA2gAwIBAgITXwABge0IJ0TduoW3qwAAAAGB7TANBgkqhkiG9w0BAQsF
ADBgMRIwEAYKCZImiZPyLGQBGRYCYWQxEzARBgoJkiaJk/IsZAEZFgNjcGgxEzAR
BgoJkiaJk/IsZAEZFgNrbGgxIDAeBgNVBAMTF0NQSCBJc3N1aW5nIENBIFNIQTI1
Ni0xMB4XDTI1MDgxNTA4MzIxOFoXDTI3MDgxNTA4MzIxOFowHzEdMBsGA1UEAxMU
bXYtZnRwczAxLmtsaC5jcGguZGswggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDTqOzgf+cn7ml3HRM7Su3IeEXfZrt53JLl2qb7b+zWttRaZ+odZ2o6rGHc
31K+1FLUUGP/MtzxLO5cRuaNojaCBDpuxEo9jT631Cfqsl/nl56rejkqShll50K0
5SuVI7Fz6LUx5FoRiRRRi5uCzOnalqov4jsGoI88klWDAlmBNwG62Ejn2NICP8sl
UANIpG+Dbvr3W8hel2VBE6FpMLOTYC+ljs5Qe0QHjfMzhNTe/WGKkBUS46kvmPHV
```



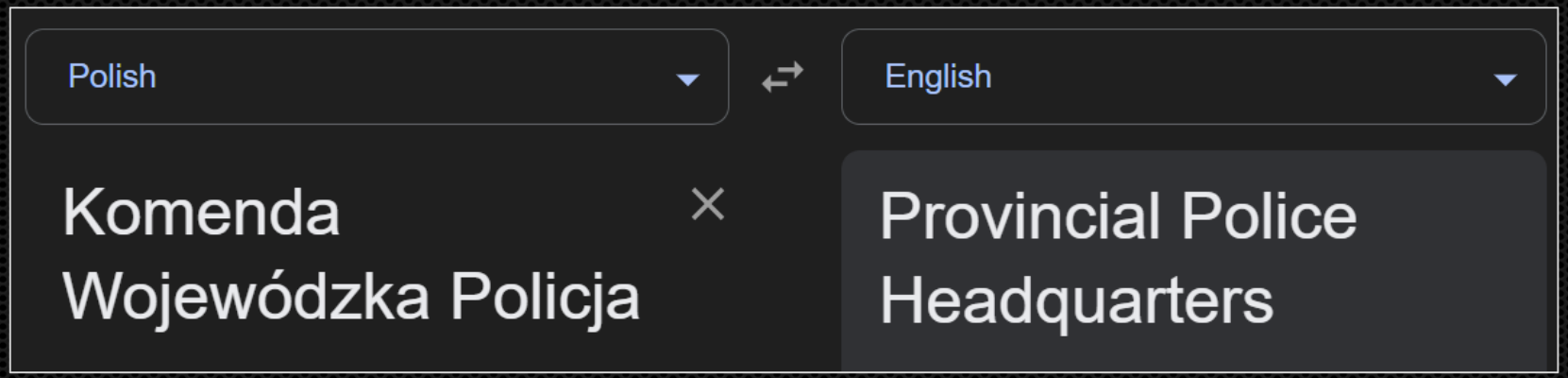
Example – ~~cph.dk~~ / cph.ad

```
$ openssl s_client -connect ftps.cph.dk:21 -starttls ftp
Connecting to 193.110.198.42
CONNECTED(00000003)
depth=1 DC=ad, DC=cph, DC=klh, CN=CPH Issuing CA SHA256-1
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN=mv-ftps01.klh.cph.dk
verify return:1
---
Certificate chain
 0 s:CN=mv-ftps01.klh.cph.dk
   i:DC=ad, DC=cph, DC=klh, CN=CPH Issuing CA SHA256-1
   a:PK
   v:No
 1 s:DC
   i:CN
   a:PK
   v:No
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIFJTCCBA2gAwIBAgITXwABge0IJ0TduoW3qwAAAAGB7TANBgkqhkiG9w0BAQsF
ADBgMRIwEAYKCZImiZPyLGQBGRYCYWQxEzARBgoJkiaJk/IsZAEZFgNjcGgxEzAR
BgoJkiaJk/IsZAEZFgNrbGgxIDAeBgNVBAMTF0NQSCBJc3N1aW5nIENBIFNIQTI1
Ni0xMB4XDTI1MDgxNTA4MzIxOFoXDTI3MDgxNTA4MzIxOFowHzEdMBsGA1UEAxMU
bXYtZnRwczAxLmtsaC5jcGguZGswggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDTqOzgf+cn7ml3HRM7Su3IeEXfZrt53JLl2qb7b+zWttRaZ+odZ2o6rGHc
31K+1FLUUGP/MtzxLO5cRuaNojaCBDpuxEo9jT631Cfqsl/nl56rejkqShll50K0
5SuVI7Fz6LUx5FoRiRRRi5uCzOnalqov4jsGoI88klWDAlmBNwG62Ejn2NICP8sl
UANIpG+Dbvr3W8hel2VBE6FpMLOTYC+ljs5Qe0QHjfMzhNTe/WGKkBUS46kvmPHV
```



Example – domenakwp.ad

```
└─$ openssl s_client -connect 91.229.22.179:443 -showcerts
Connecting to 91.229.22.179
CONNECTED(00000003)
---
Certificate chain
 0 s:C=PL, ST=Małopolska, L=Kraków, O=KWP, OU=Policja, CN=sveaba.domenakwp.ad, CN=files.sveaba.domenakwp.ad, CN=*domenakwp.ad
   i:DC=ad, DC=domenakwp, CN=KWPSubCA
   a:PKEY: RSA, 2048 (bit); sigalg: sha512WithRSAEncryption
   v:NotBefore: Sep  4 10:12:37 2025 GMT; NotAfter: Sep  4 10:12:37 2027 GMT
-----BEGIN CERTIFICATE-----
MIIH0DCCBbigAwIBAgITYwADRQMBG4L1KYVYbgAAAANFAzANBgkqhkiG9w0BAQ0F
ADBCMRIwEAYKCZImiZPyLGQBGRYCYWQxGTAXBgoJkiaJk/IsZAEZFglkb211bmFr
d3AxETAPBgNVBAMTCEtXUFN1YkNBMB4XDTI1MDkwNDEwMTIzNloXDTI3MDkwNDEw
MTIzNlowga8xCzAJBgNVBAYTAlBMMRQwEgYDVQQIDAtNYcWCb3BvbHNrYTEQMA4G
AlUEBwwHS3Jha8OzdzEMMAoGA1UEChMDS1dQMRAwDgYDVQQLEwdQb2xpY2phMRww
GgYDVQQDExNzdmVhYmEuZG9tZW5ha3dwLmFkMSIwIAYDVQQDExlmaWxlcy5zdmVh
YmEuZG9tZW5ha3dwLmFkMRYwFAYDVQQDDA0qZG9tZW5ha3dwLmFkMIIBIjANBgkq
```



Example – domenakwp.ad

dns_value : *.domenakwp.ad

Refresh

Auto interval | No breakdown

Sep 5, 2025 @ 00:00:00.000 - Sep 12, 2025 @ 03:25:13.763 (interval: Auto - 3 hours)

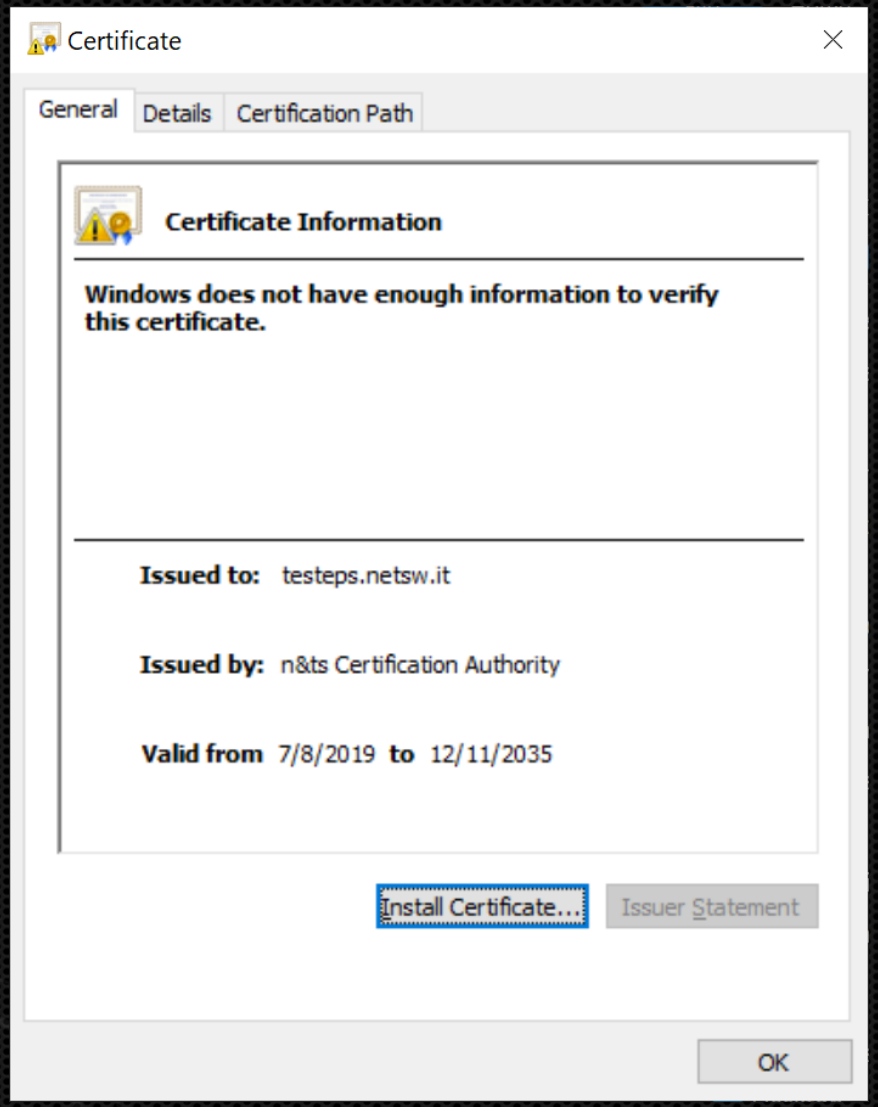
Documents (729,155) | Field statistics | Columns 4 | Sort fields 1

@timestamp	dns_value	record_type	client_ip
Sep 12, 2025 @ 03:25:00.639	msoid.domenakwp.ad	A	20.50.75.107
Sep 12, 2025 @ 03:24:59.632	svav.domenakwp.ad	A	194.69.174.51
Sep 12, 2025 @ 03:24:59.631	svav.domenakwp.ad	A	194.69.174.53
Sep 12, 2025 @ 03:24:59.631	msoid.domenakwp.ad	A	13.74.202.165
Sep 12, 2025 @ 03:24:59.630	msoid.domenakwp.ad	AAAA	20.50.75.1
Sep 12, 2025 @ 03:24:59.630	msoid.domenakwp.ad	A	20.50.75.202
Sep 12, 2025 @ 03:24:59.630	msoid.domenakwp.ad	A	20.50.82.184
Sep 12, 2025 @ 03:24:59.629	msoid.domenakwp.ad	A	20.50.82.9

Example – domenakwp.ad

```
└─$ grep -ai "X-User-Identity:" log | sort -u
X-User-Identity: B[redacted]lik@malopolska.policja.gov.pl
X-User-Identity: J[redacted]@malopolska.policja.gov.pl
X-User-Identity: J[redacted]ierski@krakow.policja.gov.pl
X-User-Identity: M[redacted]lczyk@krakow.policja.gov.pl
X-User-Identity: M[redacted]n@malopolska.policja.gov.pl
X-User-Identity: S[redacted]anik@krakow.policja.gov.pl
X-User-Identity: S[redacted]Michalczyk@krakow.policja.gov.pl
X-User-Identity: j[redacted]@krakow.policja.gov.pl
X-User-Identity: k[redacted]@chrzanow.policja.gov.pl
X-User-Identity: k[redacted]k@chrzanow.policja.gov.pl
X-User-Identity: l[redacted]a@oswiecim.policja.gov.pl
X-User-Identity: m[redacted]hrzanow.policja.gov.pl
X-User-Identity: m[redacted]ior@chrzanow.policja.gov.pl
X-User-Identity: m[redacted]@tarnow.policja.gov.pl
X-User-Identity: s[redacted]ak@chrzanow.policja.gov.pl
X-User-Identity: s[redacted]yn@chrzanow.policja.gov.pl
```

Example – ~~netsgroup.com~~ / netsw.it



N&TS GROUP

N&TS GROUP has been operating in the **electronic payments market for 30 years** as a technological partner. It is recognized as a leading European company in electronic payment software solutions, with a strong commitment to security and compliance within industry standards.

- Founded in 1995
- Domain netsw.it registered on 1999-05-04
- Domain netsgroup.com registered on 2016-10-24
- Domain netsw.it expired on 2025-06-01

Example – ~~netsgroup.com~~ / netsw.it

```
GET /wpad.dat HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: WinHttp-Autoproxy-Service/5.1
Host: wpad.netsw.it
```

```
└─$ grep -a "GET /wpad.dat HTTP/1.1" log | wc -l
19849
```

Example: Absorb LMS

absorb

Why Absorb | Products | Solutions | Pricing | Customers | Resources

Free Trial | Get Demo

34 M Users

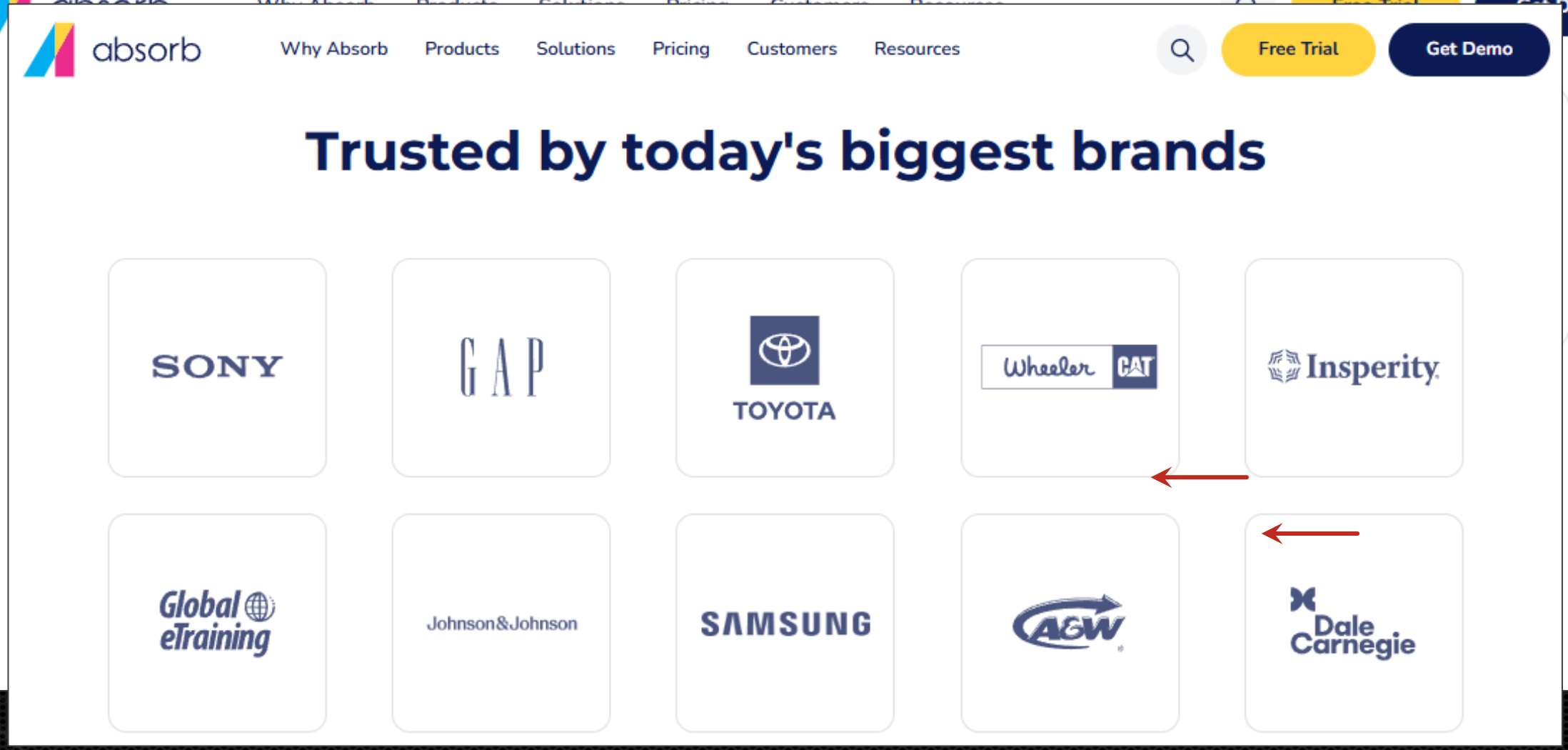
2,900+ Customers

190 Verticals

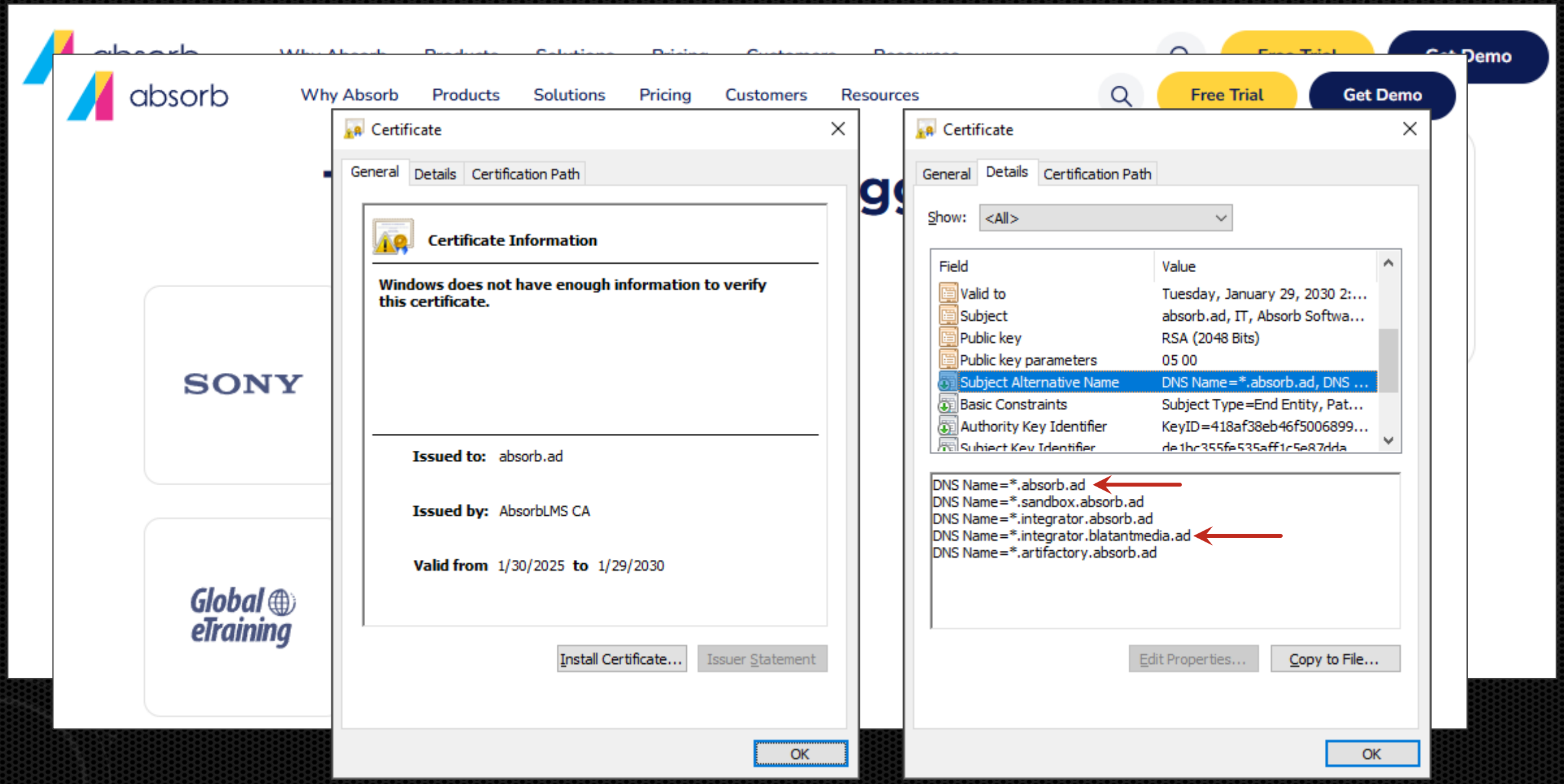
34 Countries

112 Awards

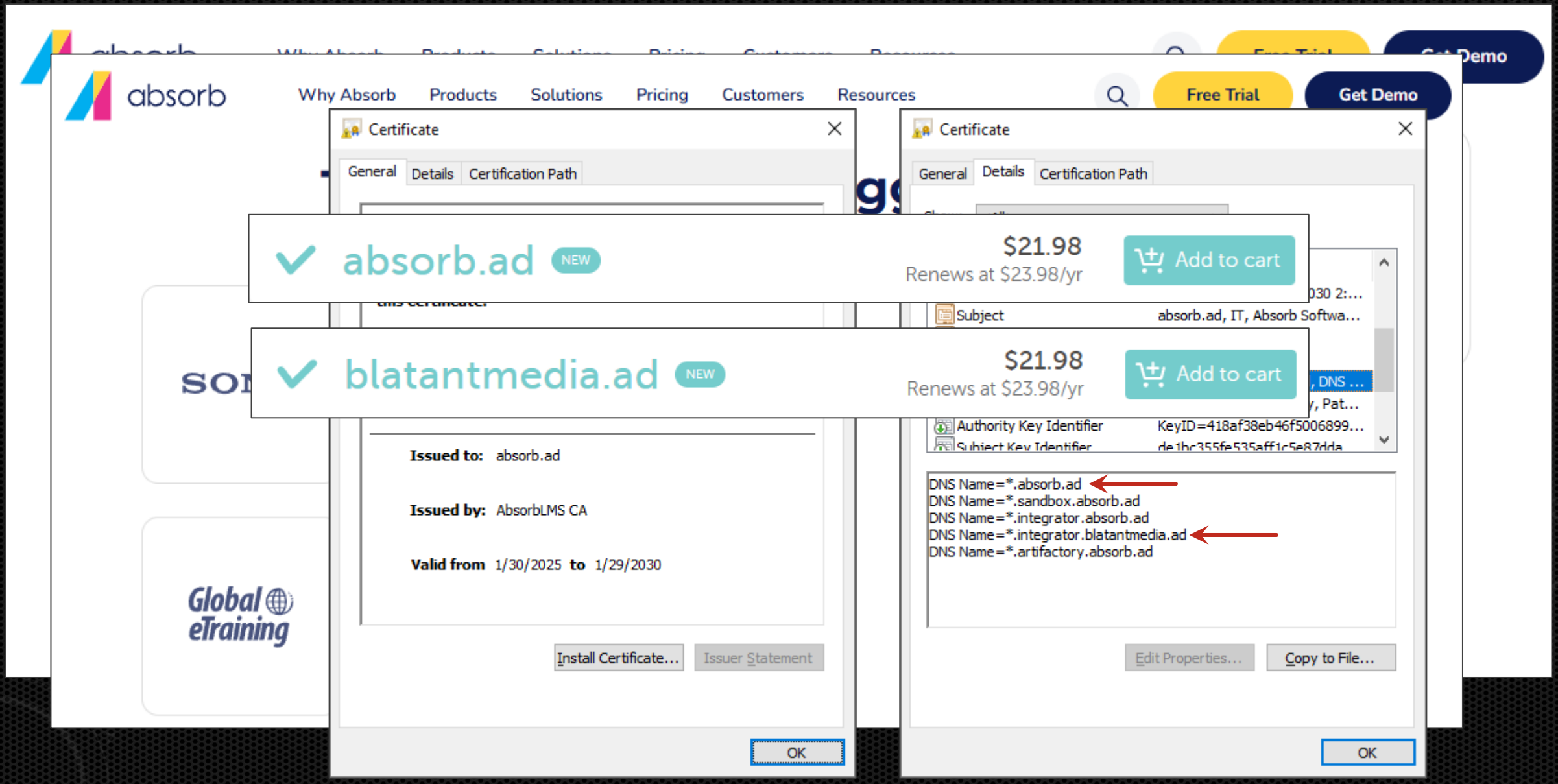
Example: Absorb LMS



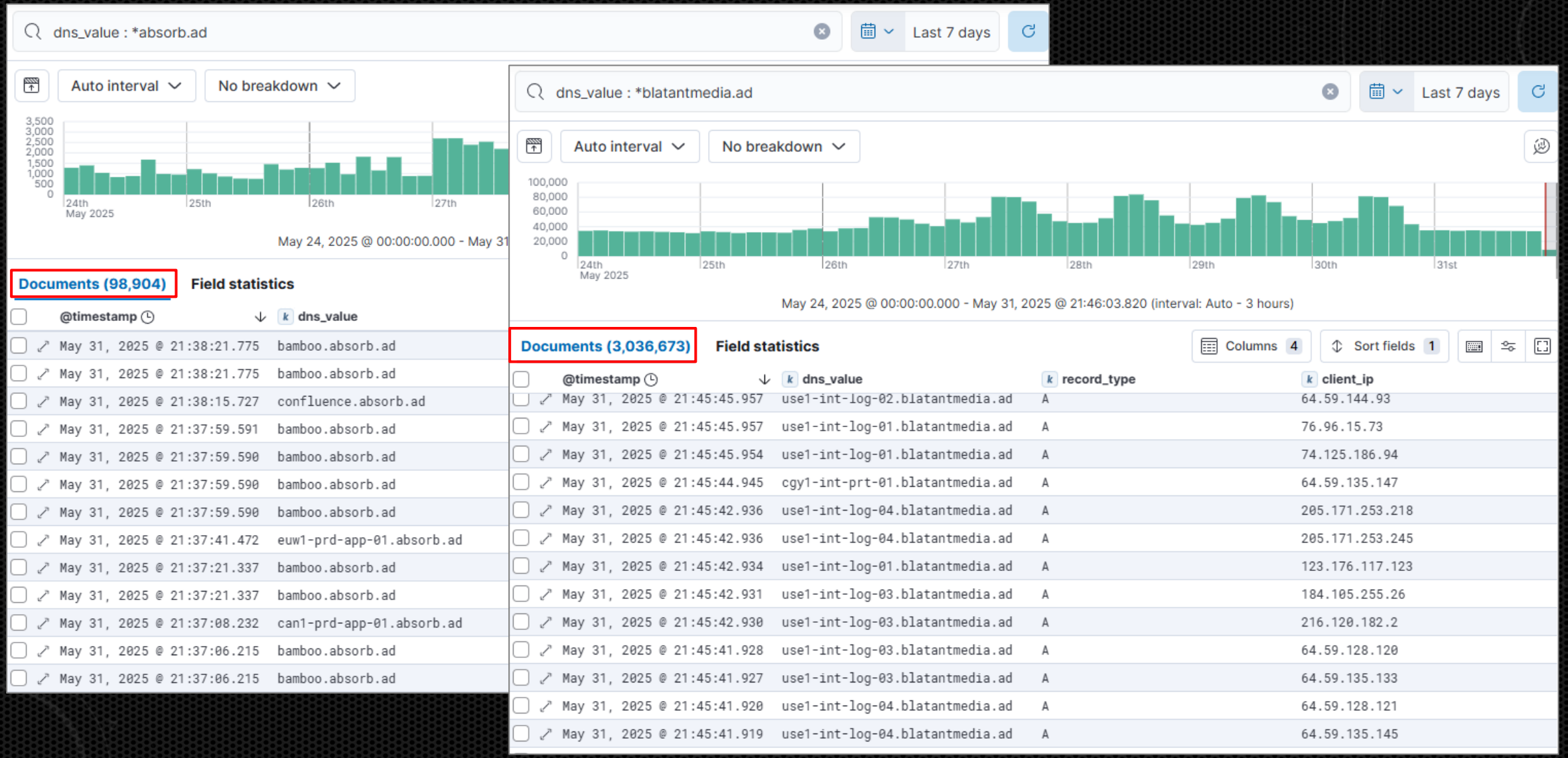
Example: Absorb LMS



Example: Absorb LMS



Example: Absorb LMS



Example: Absorb LMS (Disclosure)

- Reported to security@absorblms.com – (May 9th)
- Messaged Absorb Software's social media (LinkedIn & X) – (May 9th)
- Messaged Absorb CTO (Obaidur Rashid) via LinkedIn – (May 12th)
- Public post on LinkedIn – (May 15th)
- Emailed security@absorblms.com again… – (May 15th)
- Reported via contact form on their website – (May 19th @ 7:42pm)
  - Email from Sales - (May 19th @ 7:48pm)
  - Phone call from Sales - (May 19th @ 7:54pm)

Example: Absorb LMS

RE: [AbsorbLMS/BlatantMedia] - Internal Domain Name Collision

Summarize

Reply | Reply All | Forward

S

Security <security@absorblms.com>
To Philippe Caturegli

Thu 8/7/2025 1:51 PM

You replied to this message on 8/13/2025 9:02 AM.

b. Confirm successful transfer via Admin panel of Absorb registrar
7. Notify the researcher once complete.

As for the identified vulnerability, we have confirmed your findings and will offer a payout of $2000 (USD) in accordance with our bug bounty program. The payout will be processed via ACH or wire transfer, depending on your preference. Please let us know which method you would prefer, and we will follow up regarding the required payment details.

Thanks again for your collaboration and responsible handling of this issue. We look forward to resolving this together and continuing a productive relationship.

Best Regards,

absorb

Example: Absorb LMS

RE: [AbsorbLMS/BlatantMedia] - Internal Domain Name Collisio

Reply

Security <security@absorblms.com>
To Philippe Caturegli

You replied to this message on 8/13/2025 9:02 AM.

b. Confirm successful transfer via Admin panel of Absorb reg
7. Notify the researcher once complete.

As for the identified vulnerability, we have confirmed your findings and will
ance with our bug bounty program. The payout will be processed via AC
preference. Please let us know which method you would prefer, and we
payment details.

Thanks again for your collaboration and responsible handling of this issue. We look forward to resolving this together and continuing a productive relationship.

Best Regards,

absorb

absorb

Bug Bounty Program

Example: Absorb LMS

RE: [AbsorbLMS/BlatantMedia] - Internal Domain Name Collisio

S

Security <security@abs

To Philippe Caturegli

You replied to this message on 8/13/2

b. Confirm su

7. Notify the researc

As for the identified vulnerability, we have confirmed your findings and will

ance with our bug bounty

preference. Please let us

payment details.

Thanks again for your co

together and continuing

Best Regards,

absorb

absorb

- **No Unauthorized Access**

Participants must not access, modify, or delete any data that does not belong to them. Any attempt to access sensitive data, including user information or proprietary company data, without explicit authorization is a breach of this agreement and will result in immediate disqualification from the Bug Bounty Program and may result in legal action.

- **Confidentiality**

You agree to keep all details of discovered vulnerabilities confidential until they have been resolved and publicly disclosed by **Absorb**. Premature disclosure could expose users to risks and will be treated as a violation of this agreement.

- **No Public Disclosure**

Participants are prohibited from publicly disclosing vulnerabilities without prior written consent from **Absorb**. Unauthorized disclosure will result in disqualification from the Bug Bounty Program and may lead to legal action. This ensures vulnerabilities are addressed responsibly without exposing users to potential harm.

Example: Absorb LMS

absorb

- **No Unauthorized Access**

RE: [AbsorbLMS/BlatantMedia] - Internal Domain Name Collisio

Security <security@abs
To

You replied

7.

As for
ance
prefe
paym

Than
toget

Best Regards

ab

This message and
to use, copy, or for
immediately.

Reply | Reply All | Forward

Security <security@absorblms.com>
To Philippe Caturegli
Cc Karina Rudnytsky

Thu 9/4/2025 1:34 PM

You replied to this message on 9/4/2025 3:18 PM.

Hi Philippe,

Thank you again for your recent bug bounty submission.

We wanted to let you know that we are actively working on the matter. Karina Rudnytsky, our VP of Legal, will be reaching out to you shortly to discuss the next steps.

We appreciate your patience and the time you have taken to report this.

Best regards,

absorb

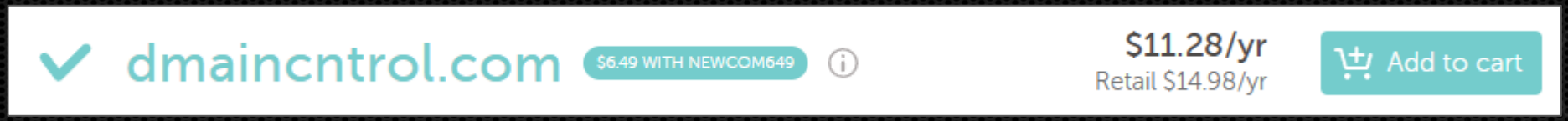
mpt to
xplicit
e Bug

solved
reated

from
l may
ers to

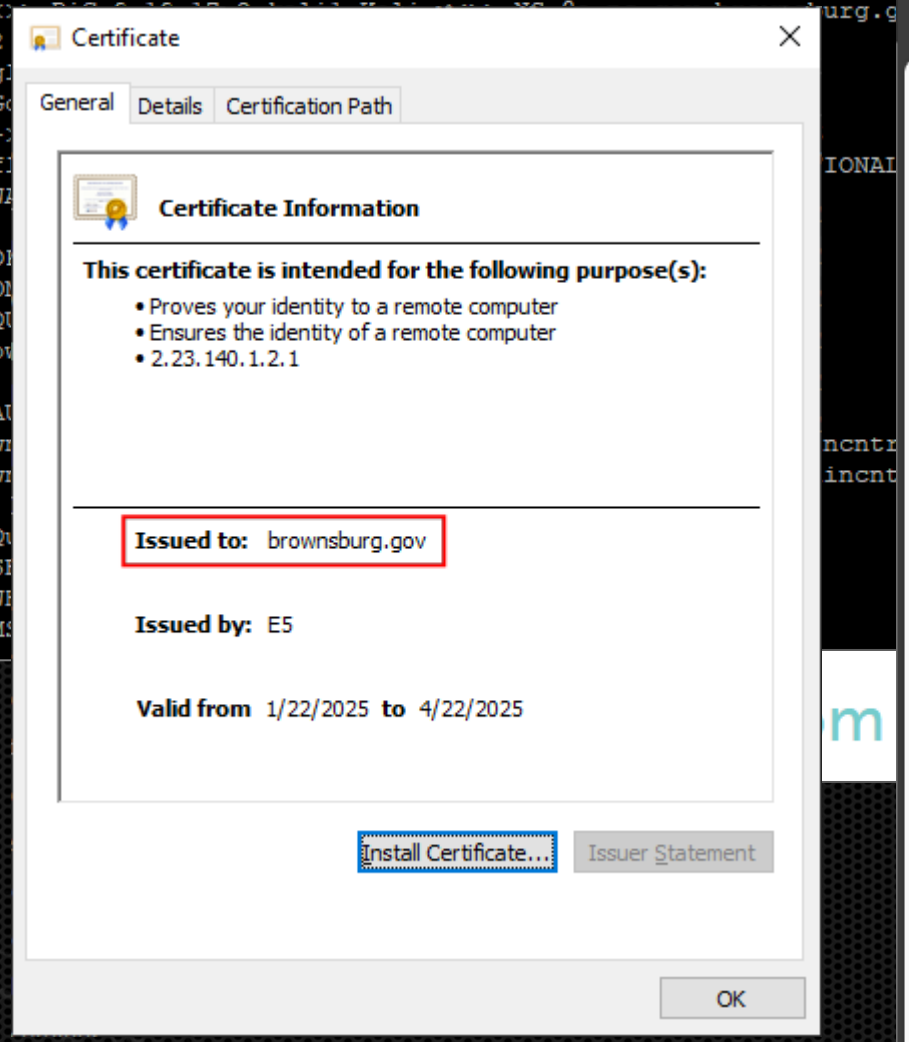
Other Example: Fat fingered NameServers (.gov)

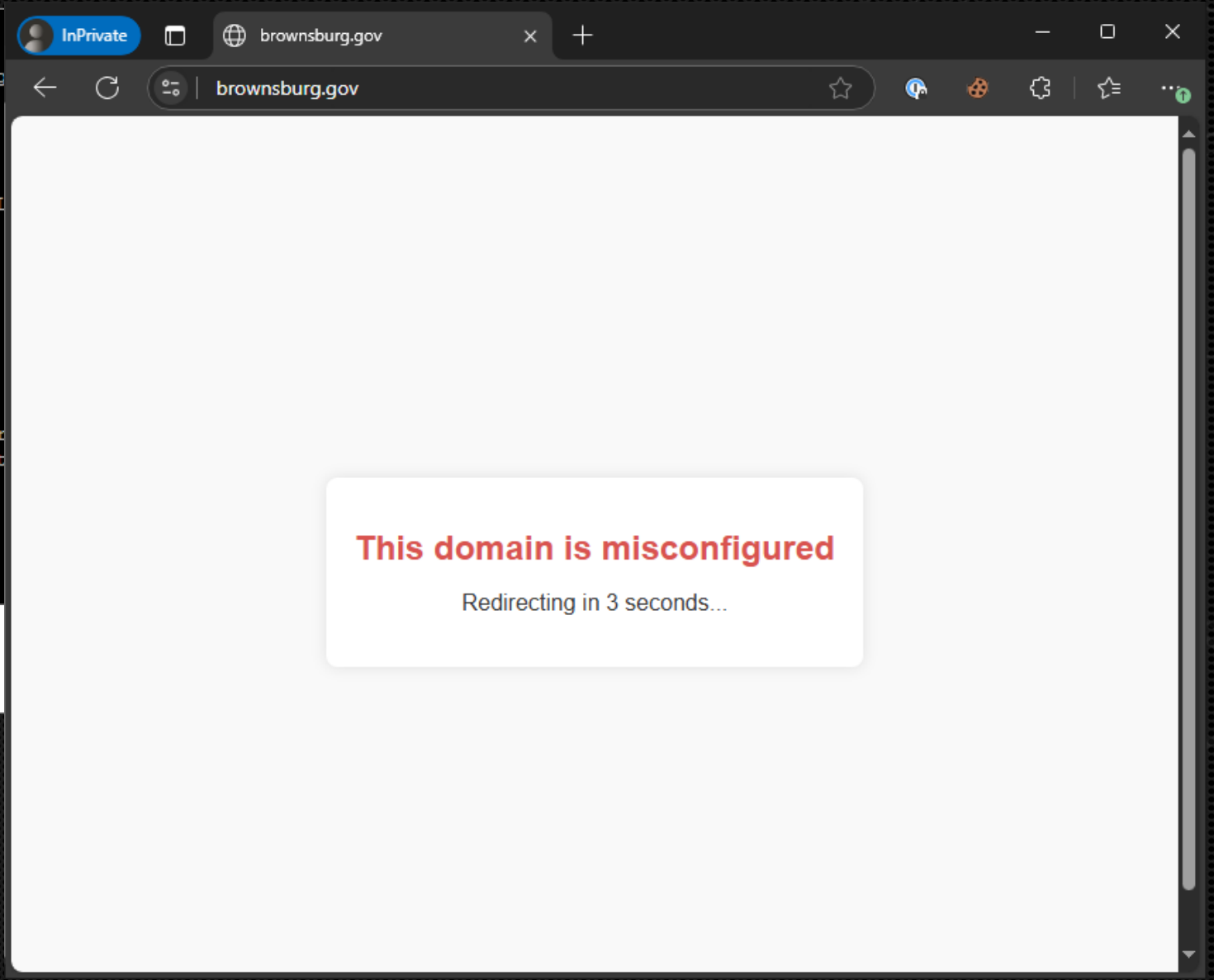
```
└─# dig NS @a.ns.gov brownsburg.gov

; <<>> DiG 9.19.17-2~kali1-Kali <<>> NS @a.ns.gov brownsburg.gov
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28476
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;brownsburg.gov.                        IN      NS

;; AUTHORITY SECTION:
brownsburg.gov.         10800   IN      NS      ns51.dmaincntrol.com.
brownsburg.gov.         10800   IN      NS      ns51.domaincntrol.com.

;; Query time: 8 msec
;; SERVER: 199.33.230.1#53(a.ns.gov) (UDP)
;; WHEN: Tue Jan 14 09:19:30 EST 2025
;; MSG SIZE  rcvd: 109
```



Other Example: Fat fingered NameServers (.gov)

```
# dig NS @a.ns.gov brownsburg.gov
```



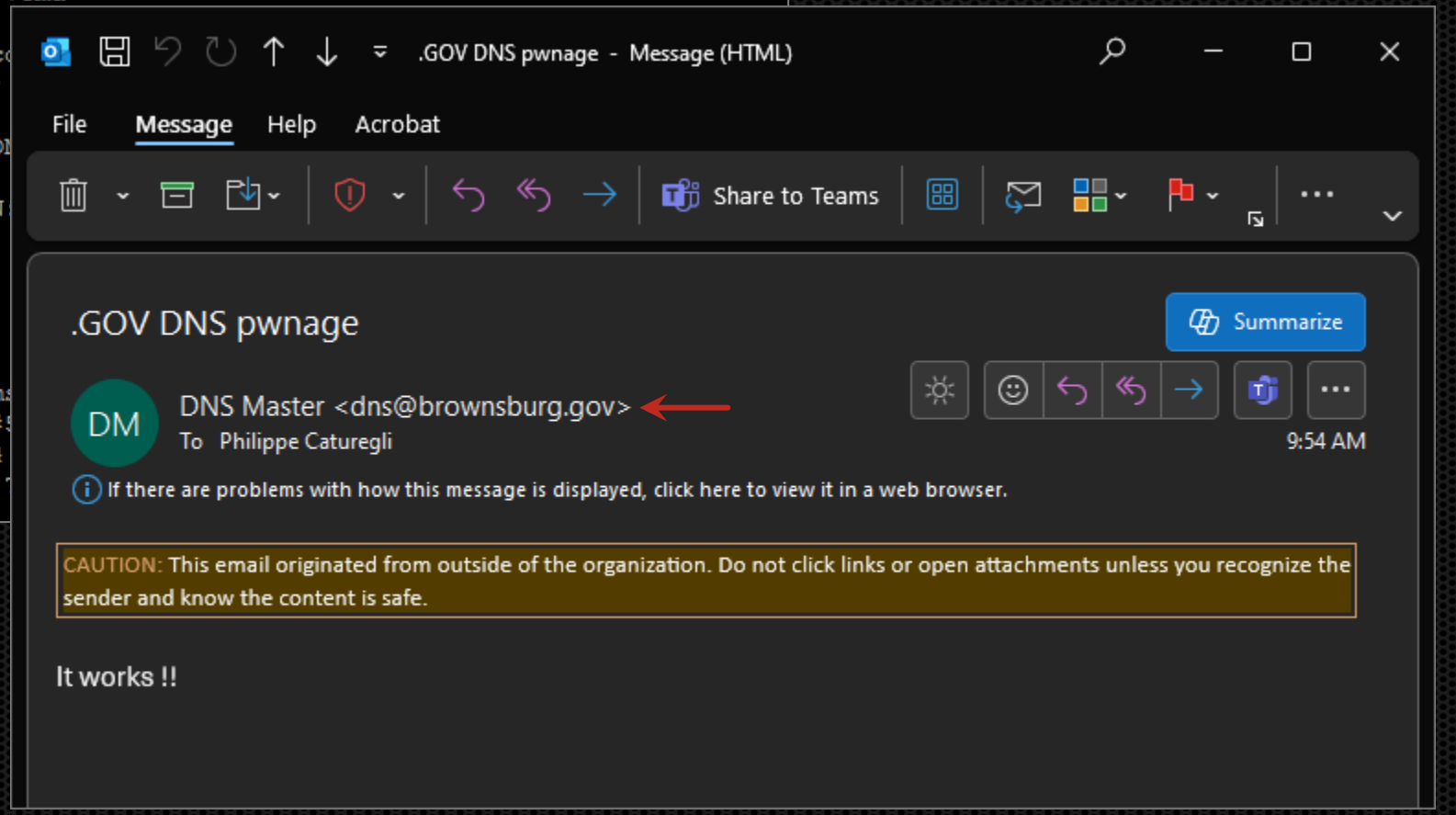


Other Example: Fat fingered NameServers (.gov)

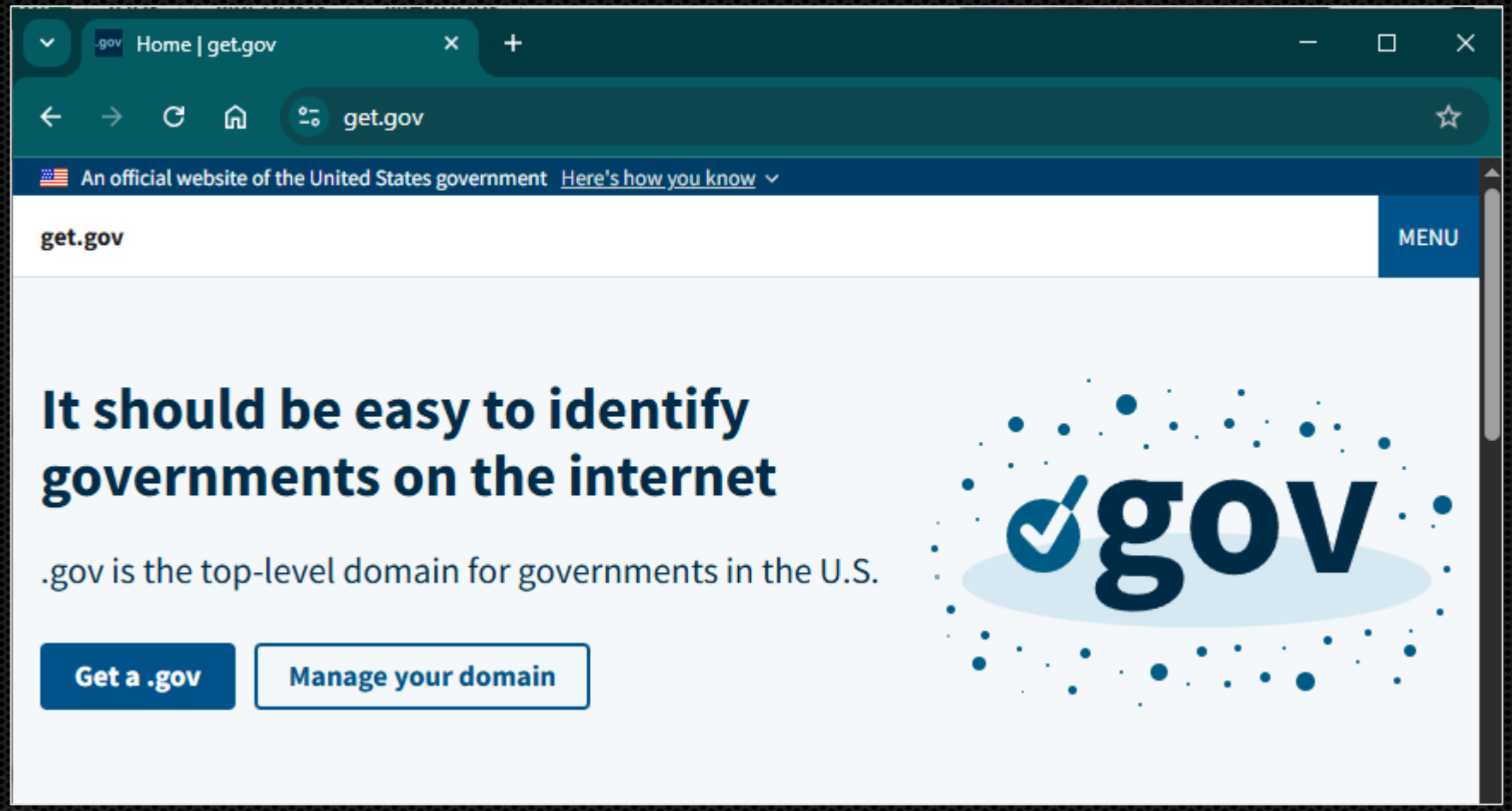
```
└─# dig MX @8.8.8.8 brownsburg.gov

; <<>> DiG 9.19.17-2~kali1-Kali <<>> MX @8.8.8.8 brownsburg.gov
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58403
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;brownsburg.gov.                        IN      MX

;; ANSWER SECTION:
brownsburg.gov.         21600   IN      MX      1 smtp.google.com.

;; Query time: 80 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Tue Jan 14 09:48:59 EST 2025
;; MSG SIZE  rcvd: 74
```

Other Example: Fat fingered NameServers (.gov)

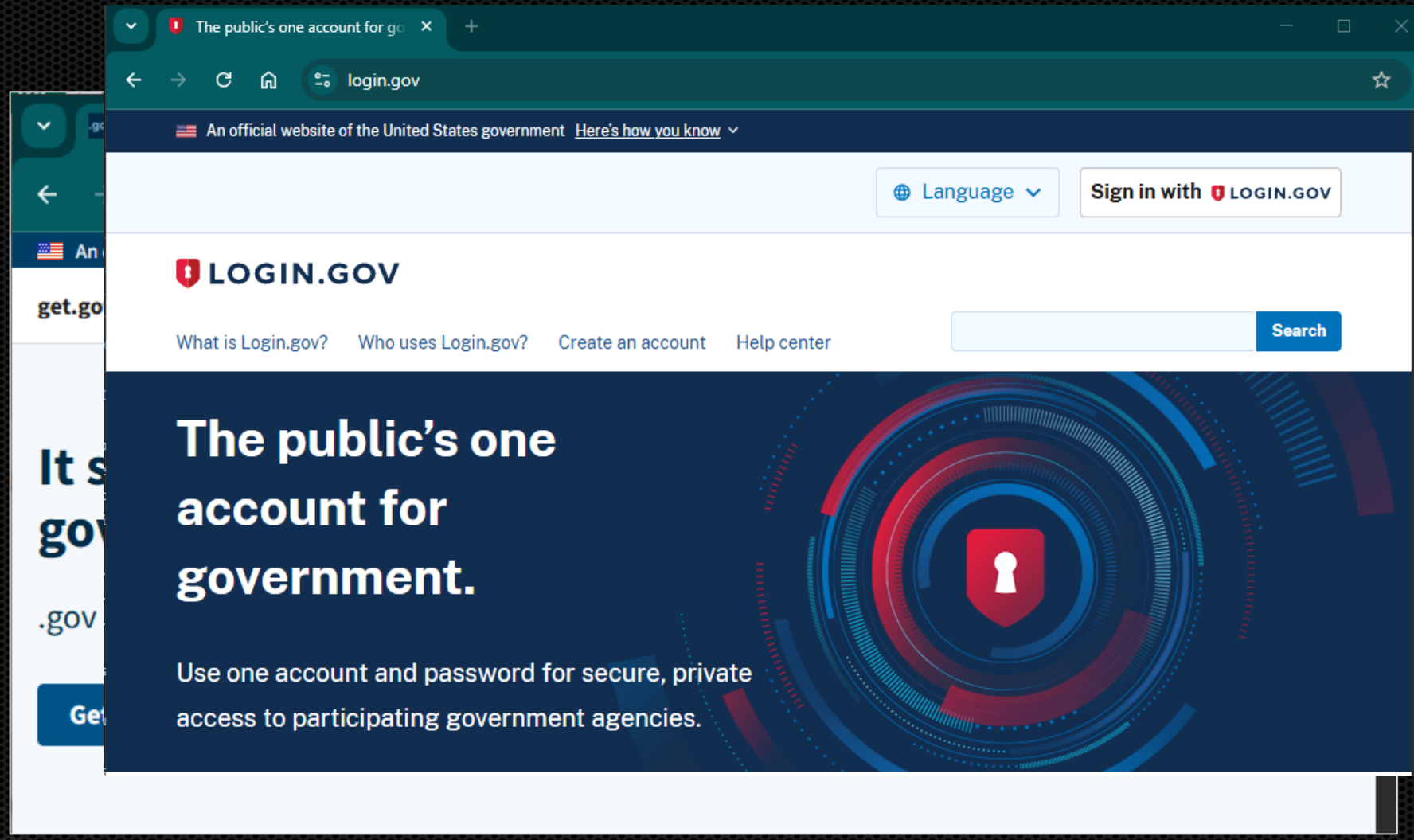
```
└─# dig MX @8.8.8.8 brownsburg.gov

; <<>> DiG 9.19.17-2~kali1-Kali <<>> MX @8.8.8.8 brownsburg.gov
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opc
;; flags: qr rd ra;

;; OPT PSEUDOSECTION
; EDNS: version: 0,
;; QUESTION SECTION
;brownsburg.gov.

;; ANSWER SECTION:
brownsburg.gov.

;; Query time: 80 ms
;; SERVER: 8.8.8.8#
;; WHEN: Tue Jan 14
;; MSG SIZE  rcvd:
```



manage.get.gov

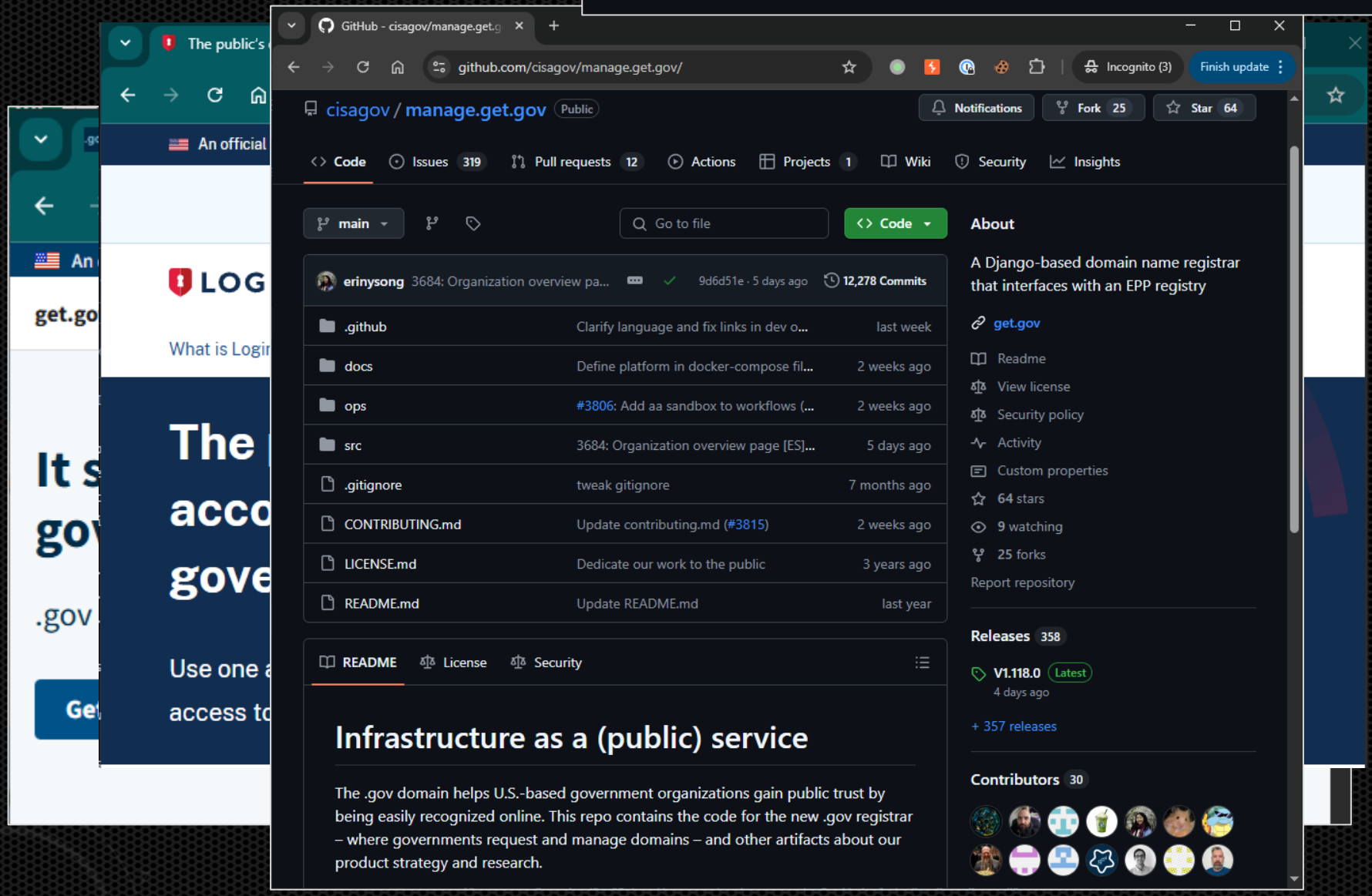


manage.get.gov

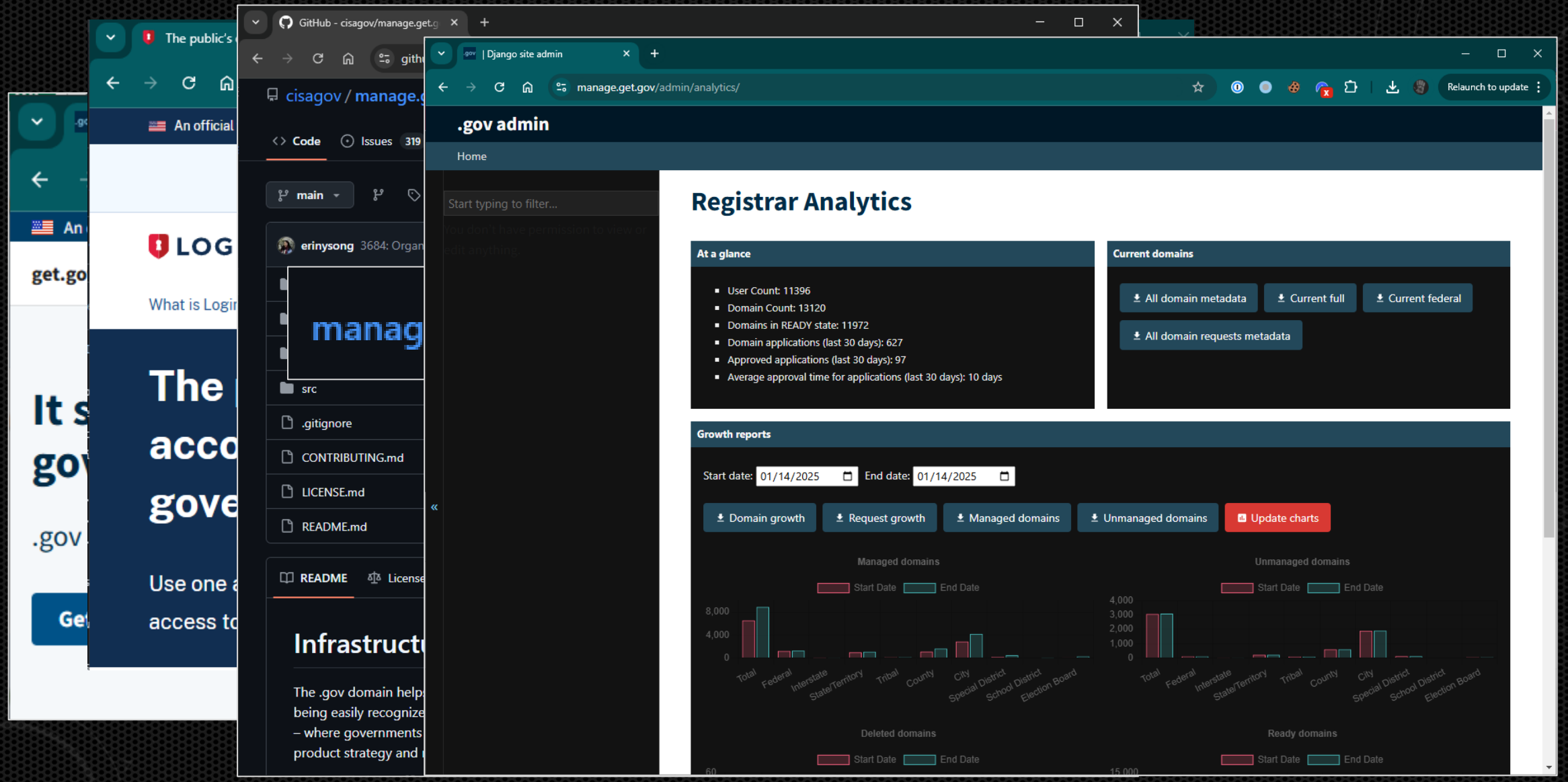


manage.get.gov

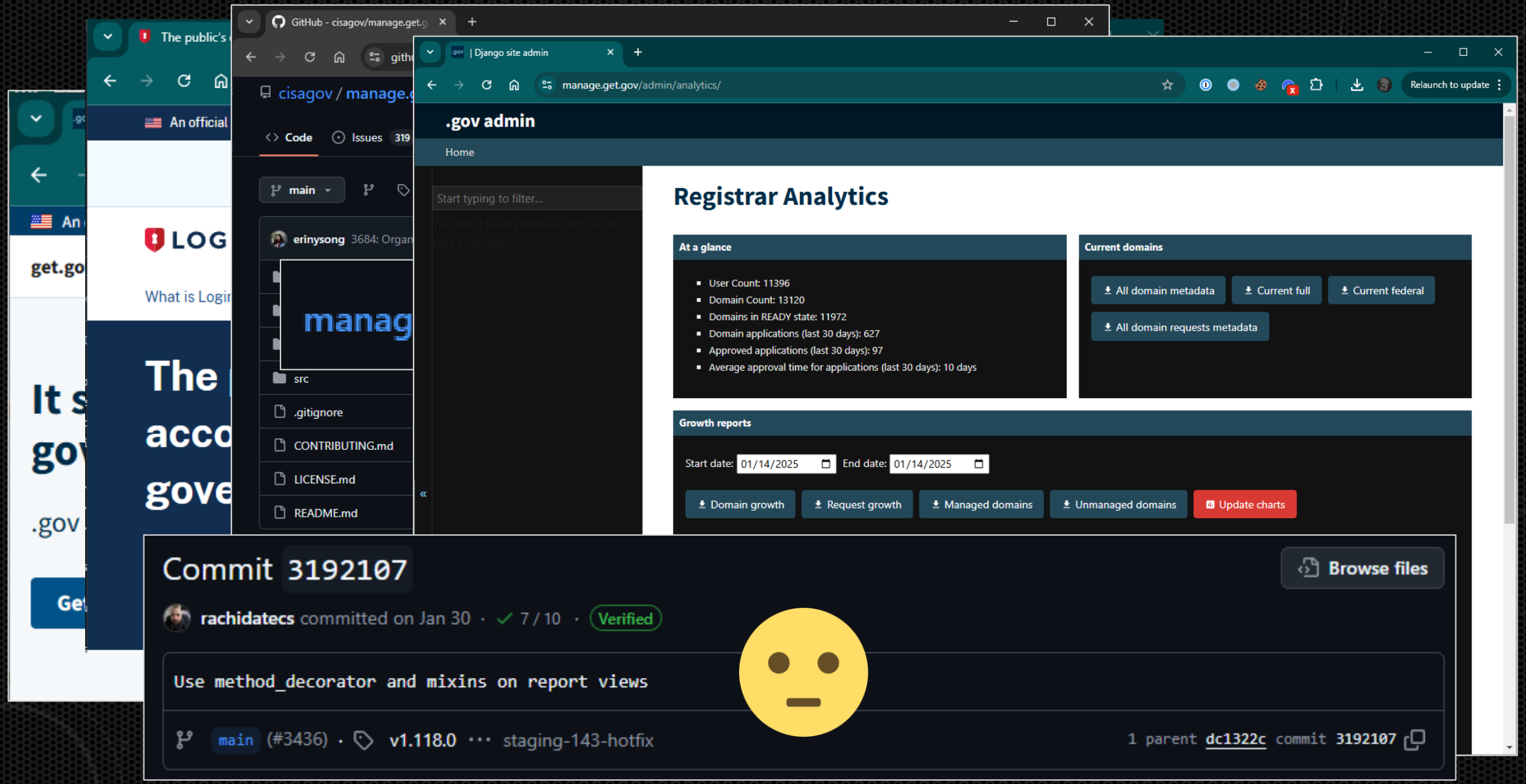
manage.get.gov / src / registrar / config / urls.py



manage.get.gov



manage.get.gov

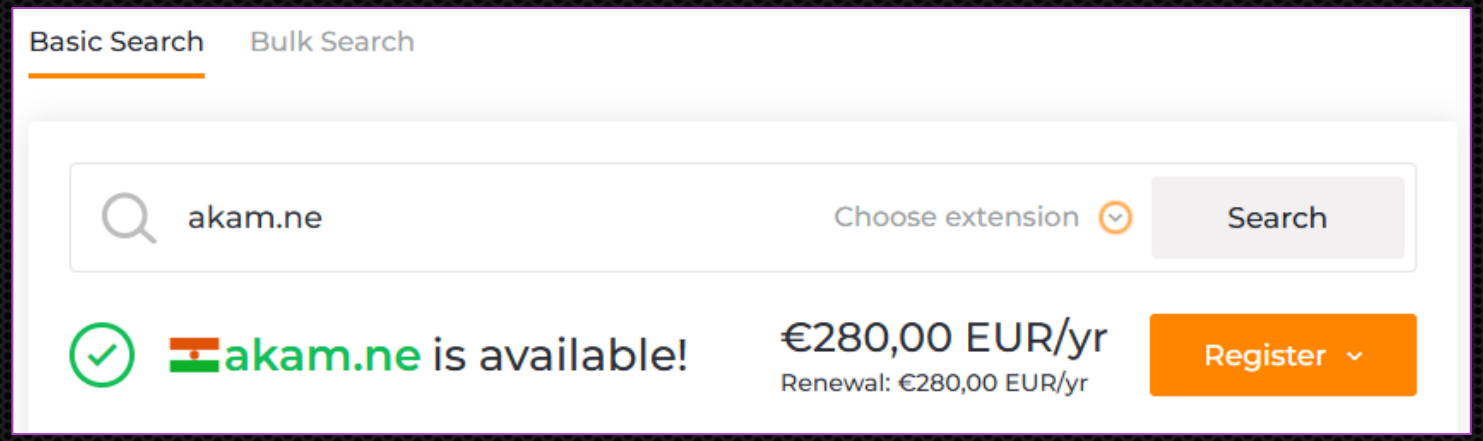


Other Example: Fat fingered NameServers (akam.ne)

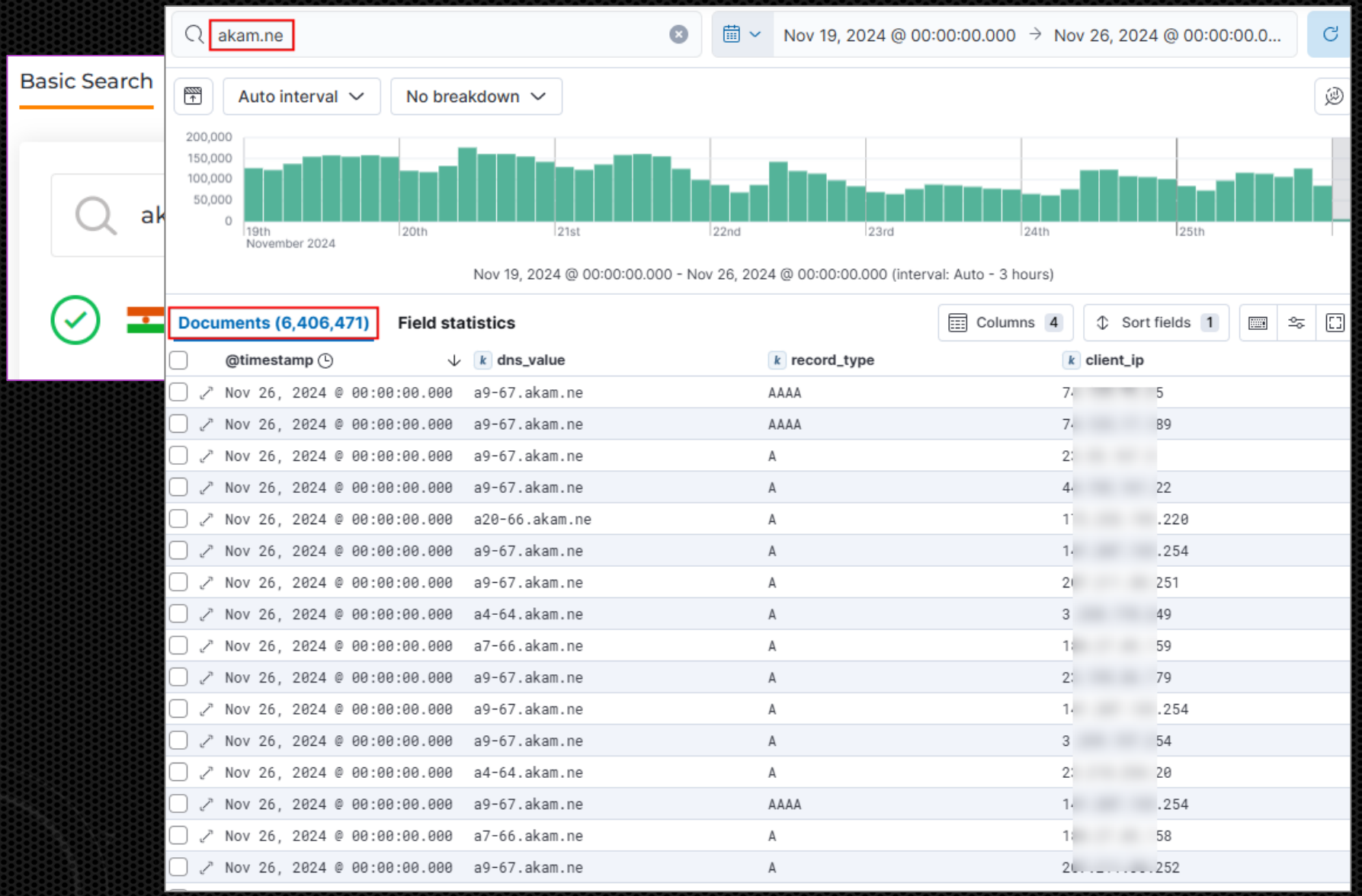
```
└─# dig -t NS santanderconsumer.es

; <<>> DiG 9.19.17-2~kali1-Kali <<>> -t NS santanderconsumer.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32481
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;santanderconsumer.es.          IN      NS

;; ANSWER SECTION:
santanderconsumer.es.   21600   IN      NS      dns02.santandergroup.net.
santanderconsumer.es.   21600   IN      NS      a11-67.akam.ne.
santanderconsumer.es.   21600   IN      NS      a12-65.akam.ne.
santanderconsumer.es.   21600   IN      NS      a2-65.akam.net.
santanderconsumer.es.   21600   IN      NS      a14-67.akam.ne.
santanderconsumer.es.   21600   IN      NS      a9-65.akam.net.
santanderconsumer.es.   21600   IN      NS      dns01.santandergroup.net.
santanderconsumer.es.   21600   IN      NS      a1-49.akam.net.
```

Other Example: Fat fingered NameServers (akam.ne)

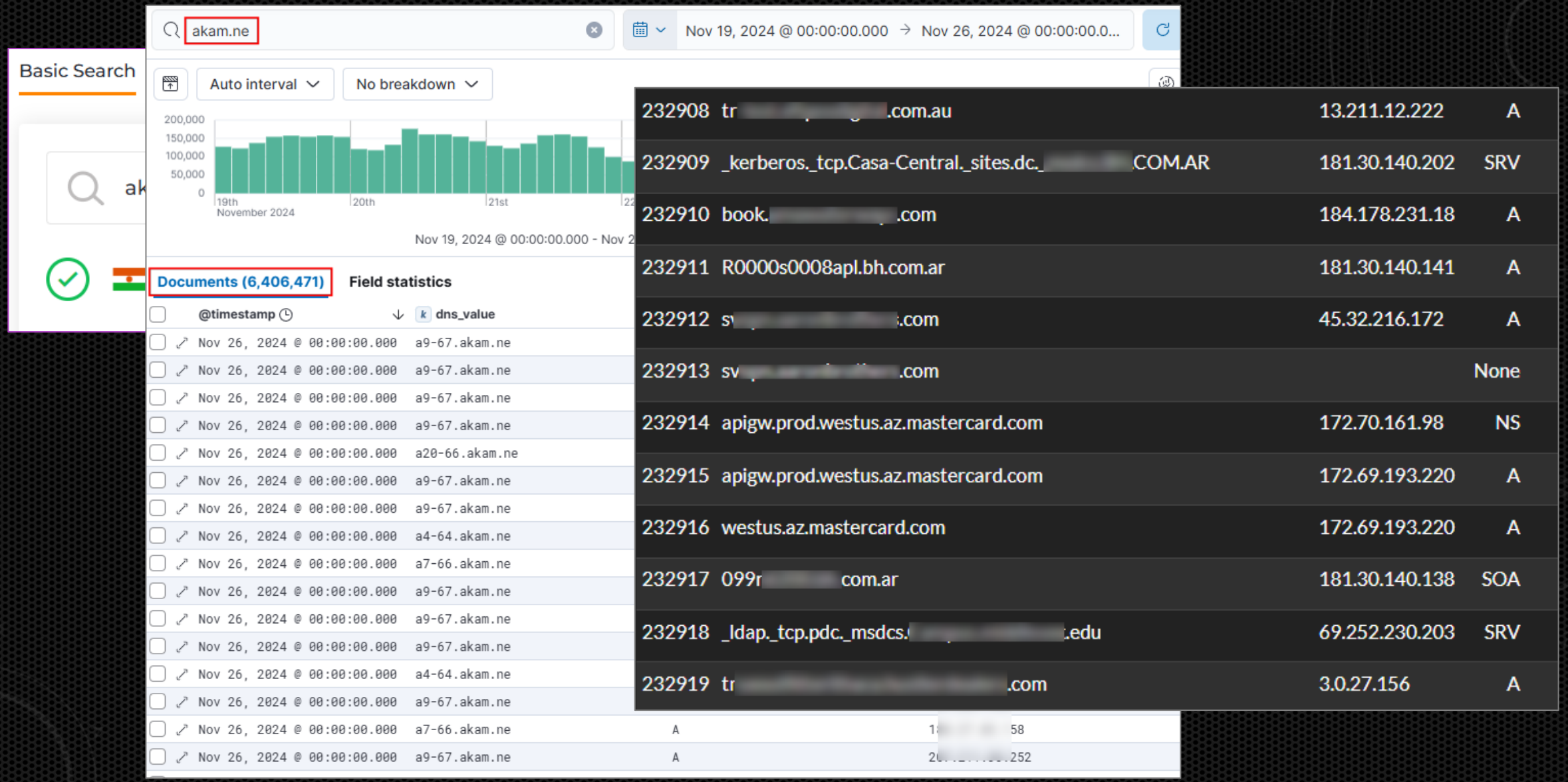
Other Example: Fat fingered NameServers (akam.ne)



Other Example: Fat fingered NameServers (akam.ne)



Other Example: Fat fingered NameServers (akam.ne)



Other Example: Fat fingered NameServers (akam.ne)

```
└─# dig +tcp @dns2.mastercard.com az.mastercard.com

; <<>> DiG 9.20.2-1-Debian <<>> +tcp @dns2.mastercard.com az.mastercard.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22219
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 8423f7def694b34bd41bf38b673b74e70b3b147cb66ae538 (good)
;; QUESTION SECTION:
;az.mastercard.com.             IN      A

;; AUTHORITY SECTION:
az.mastercard.com.      3600    IN      NS      a1-29.akam.net.
az.mastercard.com.      3600    IN      NS      a9-64.akam.net.
az.mastercard.com.      3600    IN      NS      a26-66.akam.net.
az.mastercard.com.      3600    IN      NS      a22-65.akam.ne.
az.mastercard.com.      3600    IN      NS      a7-67.akam.net.

;; Query time: 144 msec
;; SERVER: 216.119.210.53#53(dns2.mastercard.com) (TCP)
;; WHEN: Mon Nov 18 12:09:59 EST 2024
;; MSG SIZE  rcvd: 191
```

https://krebsonsecurity.com/2025/01/mastercard-dns-error-went-unnoticed-for-years/

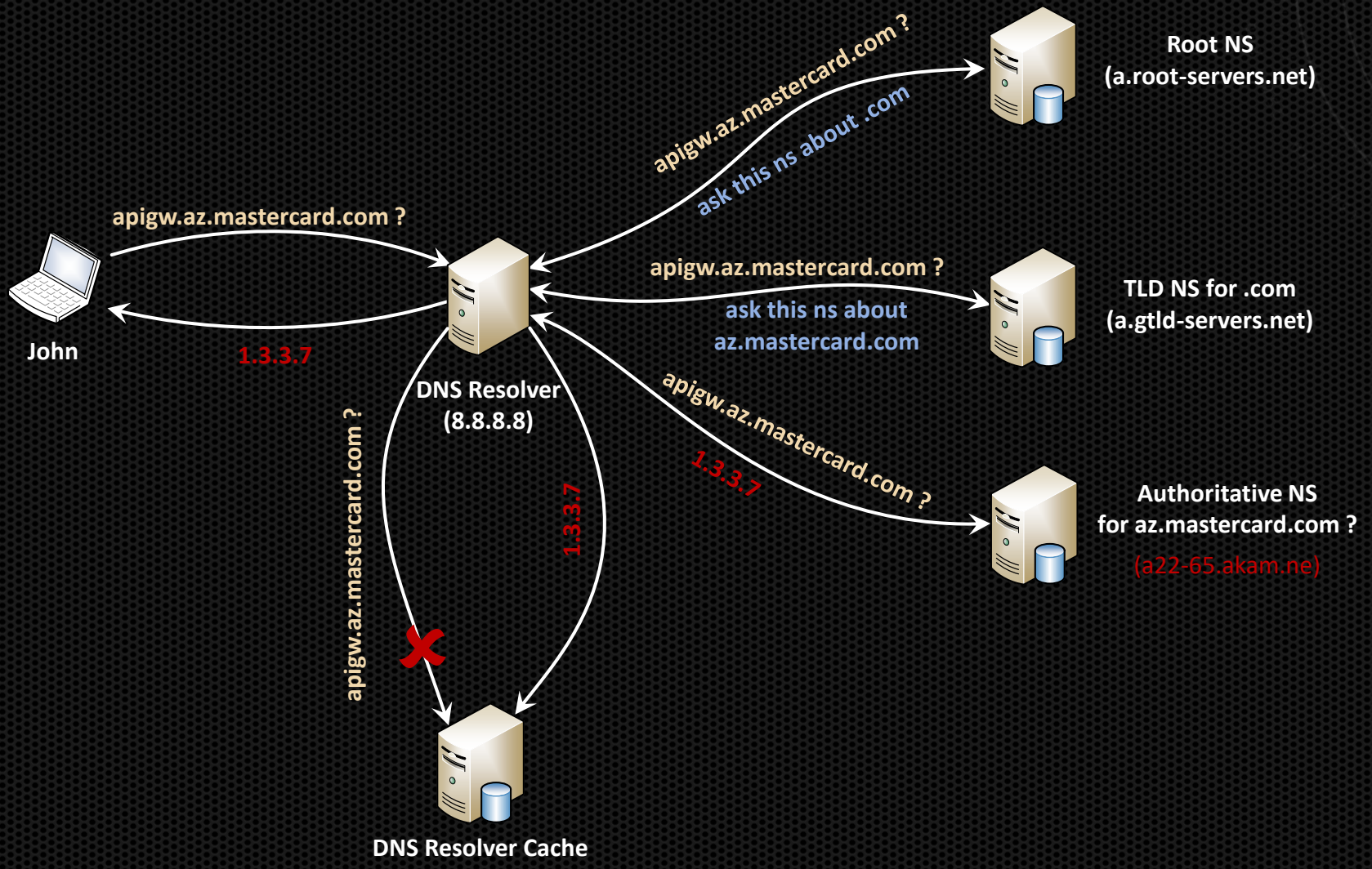
Other Example: Fat fingered NameServers (akam.ne)

```
└─# dig +tcp @dns2.mastercard.com az.mastercard.com

; <<>> DiG 9.20.2-1-Debian <<>> +tcp @dns2.mastercard.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22219
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDIT
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 8423f7def694b34bd41bf38b673b74e70b3b147cb66ae53
;; QUESTION SECTION:
;az.mastercard.com.             IN      A

;; AUTHORITY SECTION:
az.mastercard.com.      3600    IN      NS      a1-29.aka
az.mastercard.com.      3600    IN      NS      a9-64.aka
az.mastercard.com.      3600    IN      NS      a26-66.ak
az.mastercard.com.      3600    IN      NS      a22-65.ak
az.mastercard.com.      3600    IN      NS      a7-67.aka

;; Query time: 144 msec
;; SERVER: 216.119.210.53#53(dns2.mastercard.com) (TCP)
;; WHEN: Mon Nov 18 12:09:59 EST 2024
;; MSG SIZE  rcvd: 191
```

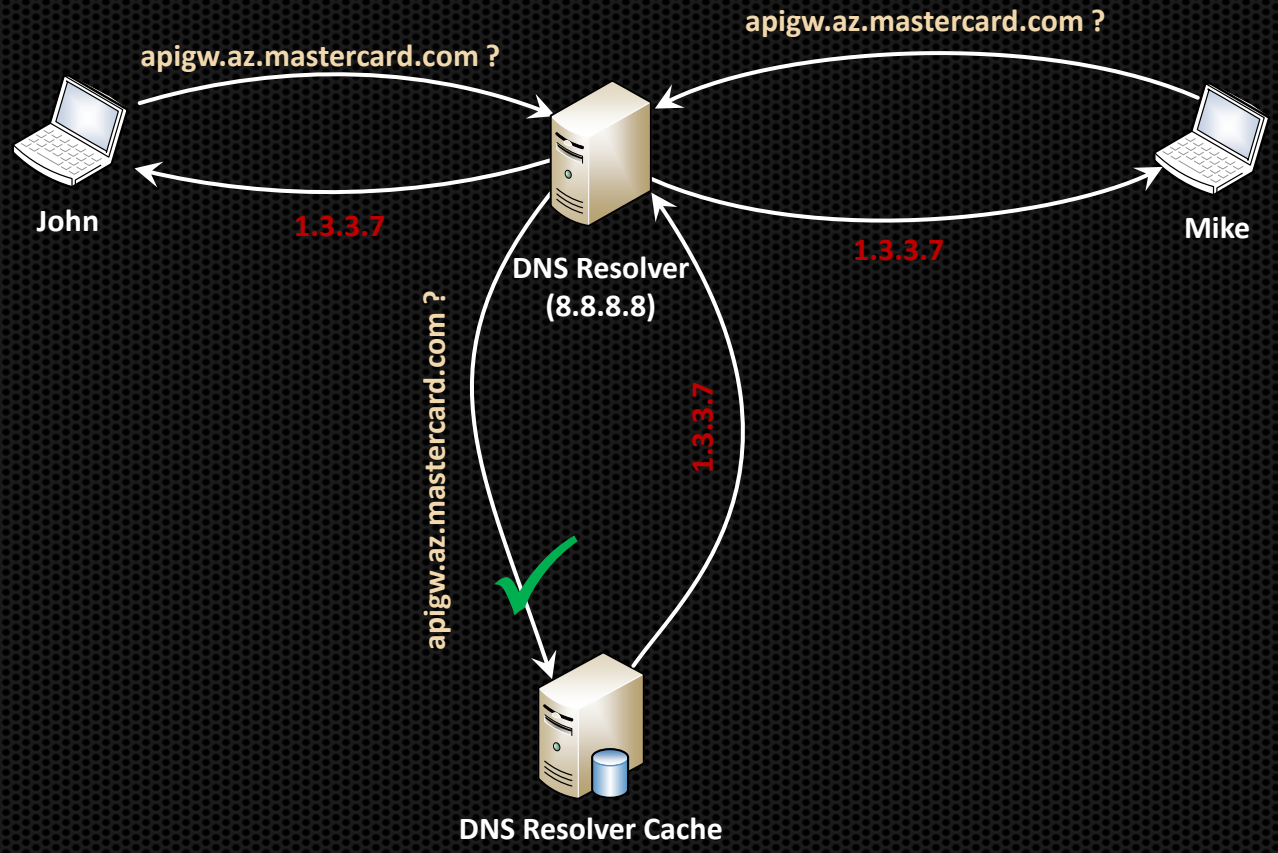
```
└─$ dig @a3-65.akam.net NS bh.com.ar

; <<>> DiG 9.20.2-1-Debian <<>> @a3-65.akam.net NS bh.com.ar
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9664
;; flags: qr aa rd; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;bh.com.ar.                     IN      NS

;; ANSWER SECTION:
bh.com.ar.              86400   IN      NS      a2-64.akam.net.
bh.com.ar.              86400   IN      NS      a3-65.akam.net.
bh.com.ar.              86400   IN      NS      a4-66.akam.net.
bh.com.ar.              86400   IN      NS      a14-64.akam.net.
bh.com.ar.              86400   IN      NS      a1-214.akam.net.
bh.com.ar.              86400   IN      NS      a9-67.akam.ne.

;; Query time: 4 msec
;; SERVER: 96.7.49.65#53(a3-65.akam.net) (UDP)
;; WHEN: Mon Nov 18 12:28:24 EST 2024
;; MSG SIZE  rcvd: 175
```

https://krebsonsecurity.com/2025/01/mastercard-dns-error-went-unnoticed-for-years/

Example: Fat fingered NameServers (1-out-of-X misconception)



Example: Fat fingered NameServers (1-out-of-X misconception)



Other Example: Fat fingered NameServers (akam.ne)

In a classic case of 'how not to handle vulnerability disclosure', Mastercard ignored our initial report (and did not offer to cover the $300 we spent registering the domain to protect them). But they did respond to Brian Krebs:

"We have looked into the matter and there was not a risk to our systems. This typo has now been corrected."

We obviously disagree with this assessment. But we'll let you judge—here are some of the DNS lookups we recorded before reporting the issue.

Don't be like Mastercard... Don't dismiss risk, and don't let your marketing team handle security disclosures...

```
sqlite> select source_ip,domain,type  from dns_query_log where domain like "%mastercard.com";
141.101.70.214|authnz360.heracles.prod.westeurope.az.mastercard.com|NS
172.69.193.220|heracles.prod.eastus.az.mastercard.com|CNAME
172.69.21.100|ausoutheast.az.mastercard.com|A
172.69.145.39|az.az.mastercard.com|A
172.68.153.32|az.az.mastercard.com|A
172.69.145.39|apigw.stage.beta.eastus.az.az.mastercard.com|A
172.68.153.32|az.az.mastercard.com|A
172.68.153.32|heracles.heracles.az.mastercard.com|A
94.23.164.164|heracles.prod.eastus.az.mastercard.com|A
172.70.120.40|westus.az.mastercard.com|A
172.70.120.40|heracles.prod.aueast.az.mastercard.com|A
172.68.173.112|prod.authnz360.heracles.prod.eastus.az.mastercard.com|AAAA
172.69.193.220|westus.az.mastercard.com|A
172.69.193.220|apigw.prod.westus.az.mastercard.com|A
172.70.161.98|apigw.prod.westus.az.mastercard.com|NS
172.68.168.102|apigw.dev.beta.work.eastus.az.mastercard.com|AAAA
141.101.70.90|eastus.az.mastercard.com|A
172.71.5.53|apigw.prod.australiaeast.az.mastercard.com|A
172.71.5.53|apigw.prod.australiaeast.az.mastercard.com|A
141.101.70.90|westeurope.az.mastercard.com|A
```

Other Example: Fat fingered NameServers (akam.ne)

In a classic case of 'how not to handle vulnerability disclosure' Mastercard ignored
our initial report (and did not offer to cover th
domain to protect them). But they did respond
"We have looked into the matter and there wa
has now been corrected."
We obviously disagree with this assessment. B
of the DNS lookups we recorded before repor
Don't be like Mastercard... Don't dismiss risk, a
handle security disclosures...

```
sqlite> select source_ip,domain,type  from dns_query_lo
141.101.70.214|authnz360.heracles.prod.westeurope.az.ma
172.69.193.220|heracles.prod.eastus.az.mastercard.com|C
172.69.21.100|ausoutheast.az.mastercard.com|A
172.69.145.39|az.az.mastercard.com|A
172.68.153.32|az.az.mastercard.com|A
172.69.145.39|apigw.stage.beta.eastus.az.az.mastercard.
172.68.153.32|az.az.mastercard.com|A
172.68.153.32|heracles.heracles.az.mastercard.com|A
94.23.164.164|heracles.prod.eastus.az.mastercard.com|A
172.70.120.40|westus.az.mastercard.com|A
172.70.120.40|heracles.prod.aueast.az.mastercard.com|A
172.68.173.112|prod.authnz360.heracles.prod.eastus.az.ma
172.69.193.220|westus.az.mastercard.com|A
172.69.193.220|apigw.prod.westus.az.mastercard.com|A
172.70.161.98|apigw.prod.westus.az.mastercard.com|NS
172.68.168.102|apigw.dev.beta.work.eastus.az.mastercard.
141.101.70.90|eastus.az.mastercard.com|A
172.71.5.53|apigw.prod.australiaeast.az.mastercard.com|A
172.71.5.53|apigw.prod.australiaeast.az.mastercard.com|A
141.101.70.90|westeurope.az.mastercard.com|A
```

Request to Remove Public Post Regarding DNS Disclosure

Summarize

BS Bugcrowd Support <support@bugcrowd.com>

1/16/2025

Hello titon,

We hope this message finds you well. We're reaching out regarding this public post you recently made on LinkedIn titled, *"classic case of how not to handle vulnerability disclosure"*, which references DNS records associated with Mastercard.

Mastercard has expressed concerns about the public nature of this disclosure. As a Bugcrowd researcher, you are familiar with the importance of responsible disclosure practices and how they help maintain trust and professionalism in the cybersecurity community.

We kindly request that you take down the post as a gesture of good faith and professionalism. Addressing this proactively will demonstrate your commitment to ethical security practices and help maintain positive relationships with organizations in the industry.

Please let us know once the post has been removed or if there's anything we can clarify to support your understanding of the situation. We appreciate your cooperation and timely action in this matter.

Thank you for your attention, and we look forward to your response.

Best Regards
Platform Behavior Standards Team

Conclusion

> “A long-lasting solution to eliminate the potential issues arising from name collision in a private name space comes from implementing fully qualified domain names”

Cyrus Namazi, ICANN Vice President, DNS

https://youtu.be/jpnxGa2gAuY

Conclusion

> “A long-lasting solution to eliminate the potential issues arising from name collision in a private name space comes from implementing fully qualified domain names **that you actually registered**”

Cyrus Namazi, ICANN Vice President, DNS

https://youtu.be/jpnxGa2gAuY

Some numbers

- **38,942,387** SSL certificates analyzed (CN, SAN, CRL)
- **9,583,846** Services with NTLM Auth analyzed
- **92,238** domains not registered
- **186** domains registered
- **$8,628** spent
- **5,992,624,974** DNS request recorded over the last 12 months

Honorable mention

- Town of NewCastle, UK – **newcastle.local.ad**
- Institute of Meteorology and Water Management – **imgw.ad**
- Nigelec (electric power generation and transmission utility in Niger) – **nigelec.ad**
- State of Montana – **billings.ad**
- Arkansas Department of Environmental Quality – **adpce.ad**
- Placer County, CA – **placerco.ad**
- United Southeast Federal Credit Union – **usfcu.ad**
- Celcomdigi (largest mobile operator in Malaysia) – **celcom.ad**
- Marcatel (telco operator in Mexico) – **marcatel.ad**
- Linxens (Global electronic supplier) – **mic.ad**
- NuStar Energy (largest pipeline operator in the US) – **usdom1.ad**
- BitMEX (Crypto Exchange) – **bitmex.ad**

Thank you !

Philippe Caturegli

Chief Hacking Officer at Seralys

mailto: pcaturegli@seralys.com