

Internal Domain Name Collision 2.0

Philippe Caturegli

RVASec 2025

*“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



INITECH

- Clients include Financial institutions, Manufacturing/Industrial firms, etc.
- ~300 Employees (with strong IT background)
- Limited external footprint (hosted WordPress, Client Portal, Exchange Server, VPN)



 Add to cart



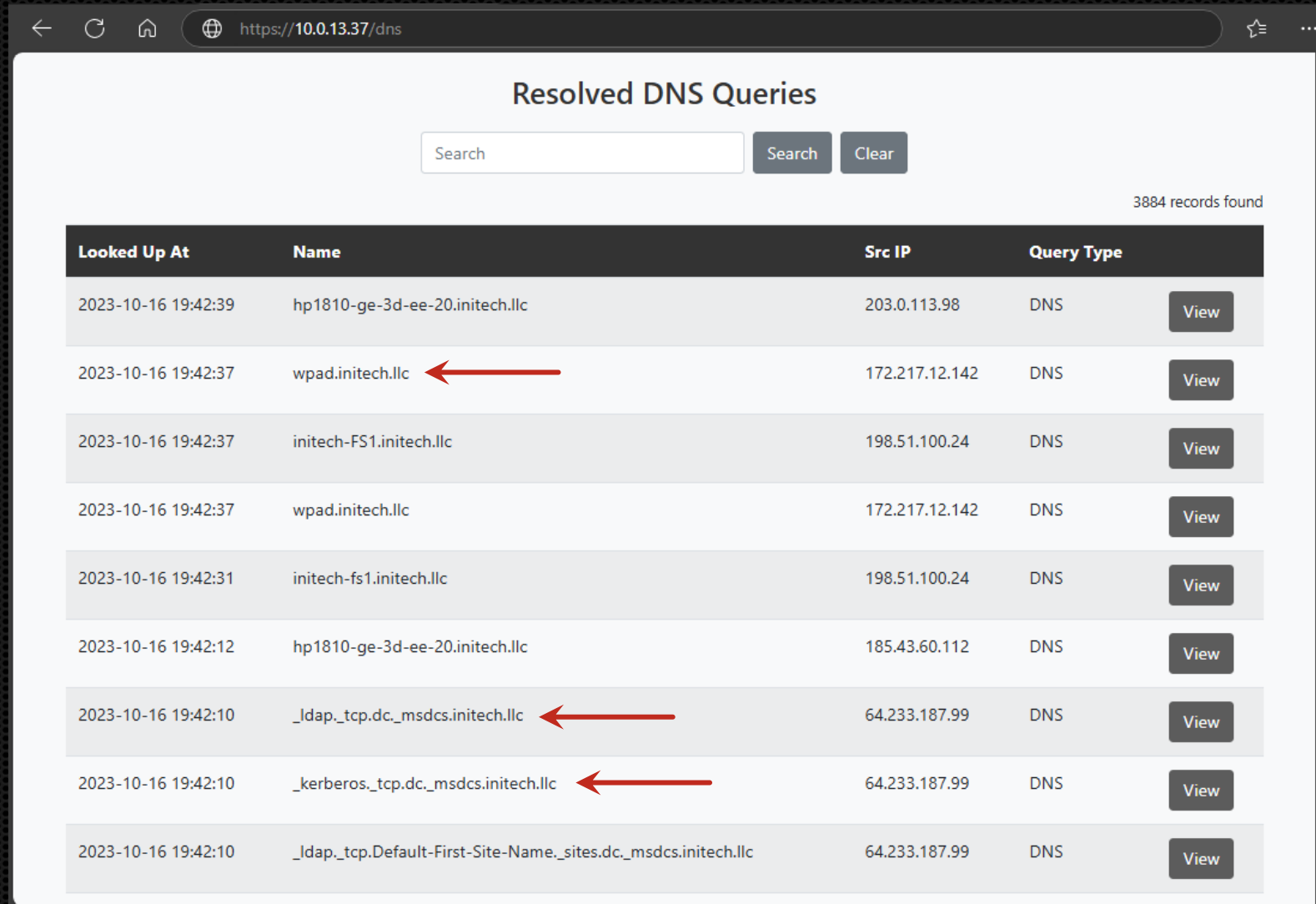
```
└─# nmap -p 25 --script smtp-ntlm-info exch01.initech.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-10-16 17:18 EDT
Nmap scan report for exch01.initech.com (211.219.156.149)
Host is up (0.013s latency).
```

```

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



Resolved DNS Queries

Search Search Clear

3884 records found

Looked Up At	Name	Src IP	Query Type	
2023-10-16 19:42:39	hp1810-ge-3d-ee-20.initech.llc	203.0.113.98	DNS	View
2023-10-16 19:42:37	wpad.initech.llc	172.217.12.142	DNS	View
2023-10-16 19:42:37	initech-FS1.initech.llc	198.51.100.24	DNS	View
2023-10-16 19:42:37	wpad.initech.llc	172.217.12.142	DNS	View
2023-10-16 19:42:31	initech-fs1.initech.llc	198.51.100.24	DNS	View
2023-10-16 19:42:12	hp1810-ge-3d-ee-20.initech.llc	185.43.60.112	DNS	View
2023-10-16 19:42:10	_ldap_tcp.dc.msdc.initech.llc	64.233.187.99	DNS	View
2023-10-16 19:42:10	_kerberos_tcp.dc.msdc.initech.llc	64.233.187.99	DNS	View
2023-10-16 19:42:10	_ldap_tcp.Default-First-Site-Name_sites.dc.msdc.initech.llc	64.233.187.99	DNS	View

- Responder

- Hashcat

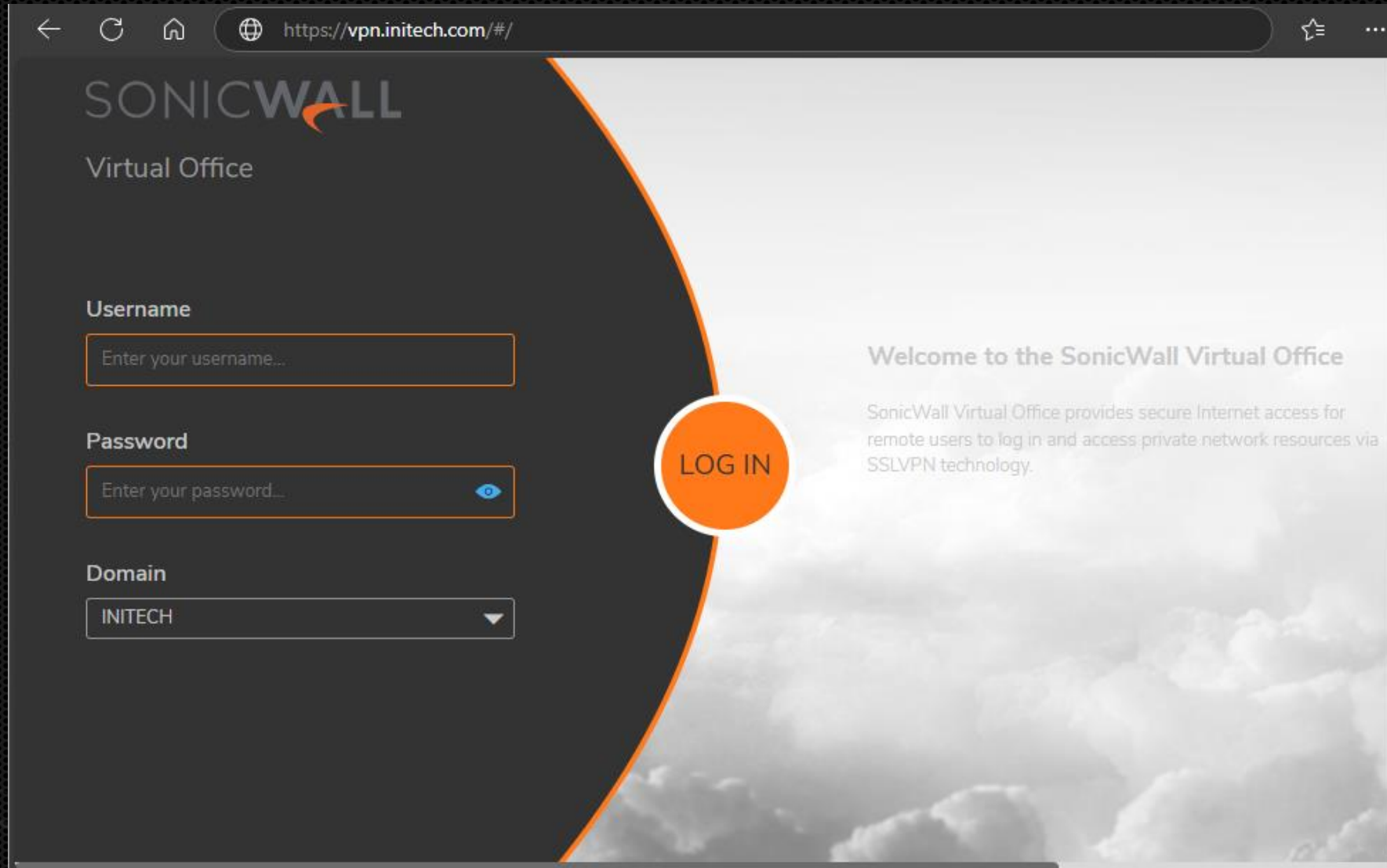
[illegible]

```
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
```

95087
04100
C86AB
E0032
.0 Sa

Introduction



The screenshot shows a web browser window with the address bar displaying `https://vpn.initech.com/#/`. The page features the SonicWall logo and the text "Virtual Office". On the left, there are three input fields: "Username" with a placeholder "Enter your username...", "Password" with a placeholder "Enter your password..." and an eye icon, and "Domain" with a dropdown menu showing "INITECH". A large orange circular button with the text "LOG IN" is positioned in the center. To the right, a welcome message reads: "Welcome to the SonicWall Virtual Office" followed by "SonicWall Virtual Office provides secure Internet access for remote users to log in and access private network resources via SSLVPN technology." The background of the page is a dark grey gradient with a large orange arc and a cloud image.

SONICWALL
Virtual Office

Username
Enter your username...

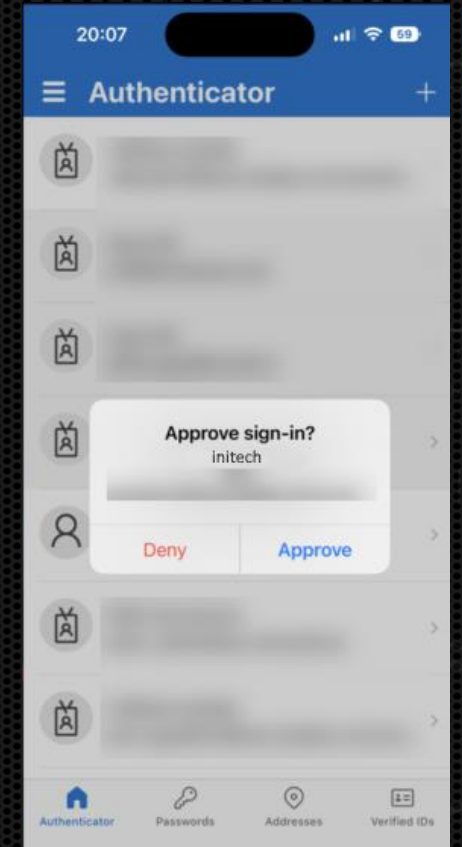
Password
Enter your password...

Domain
INITECH

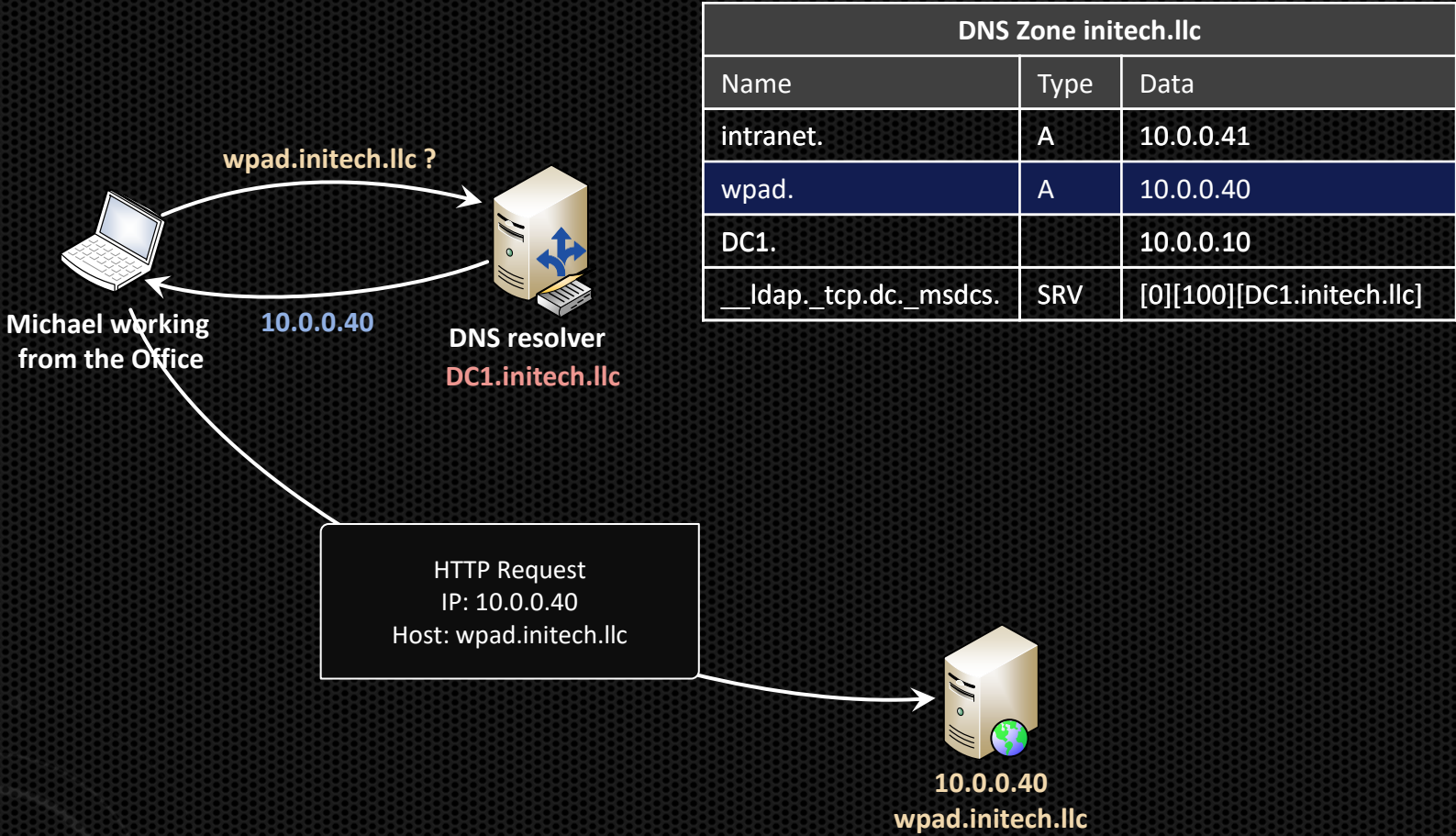
LOG IN

Welcome to the SonicWall Virtual Office

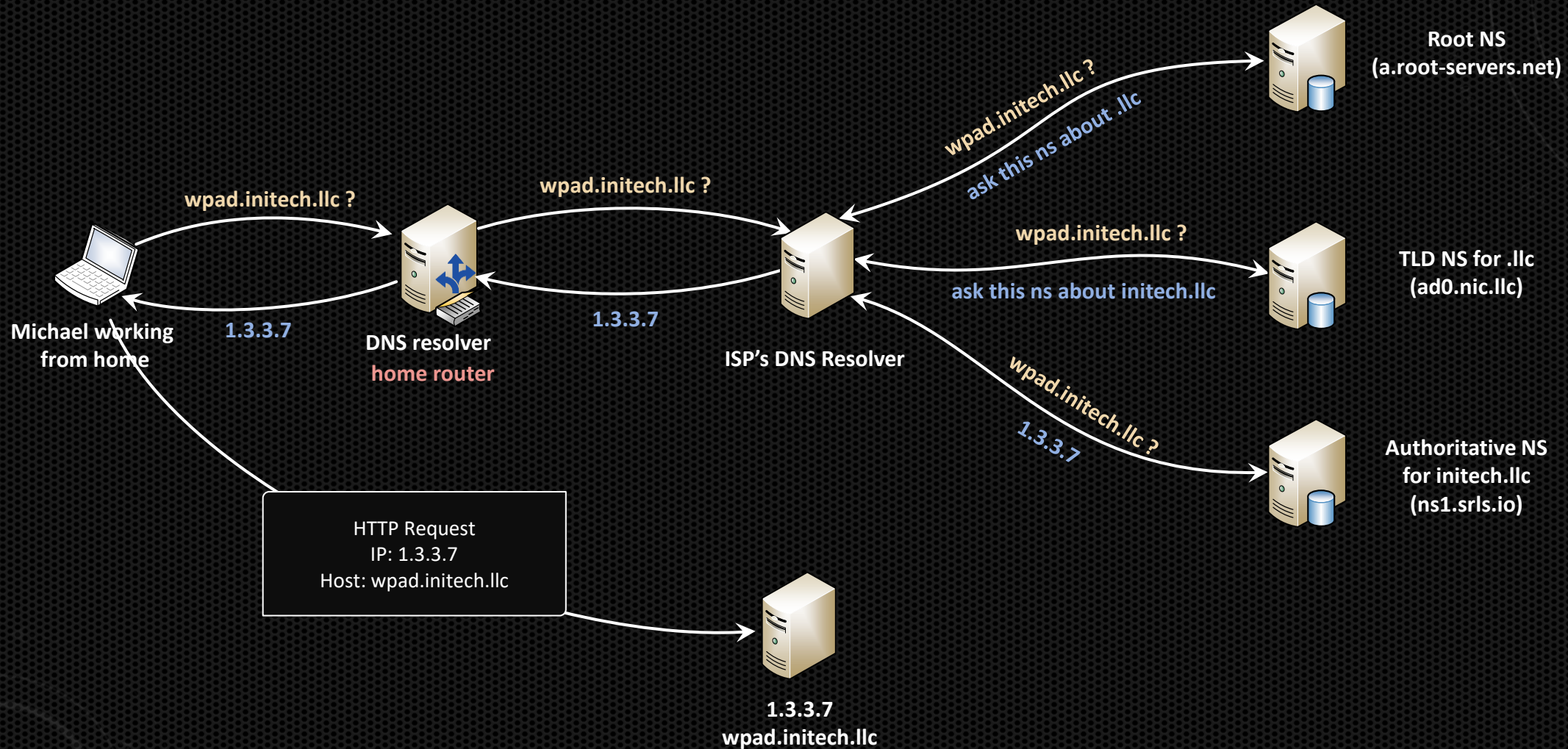
SonicWall Virtual Office provides secure Internet access for remote users to log in and access private network resources via SSLVPN technology.



What happened ?



What happened ?



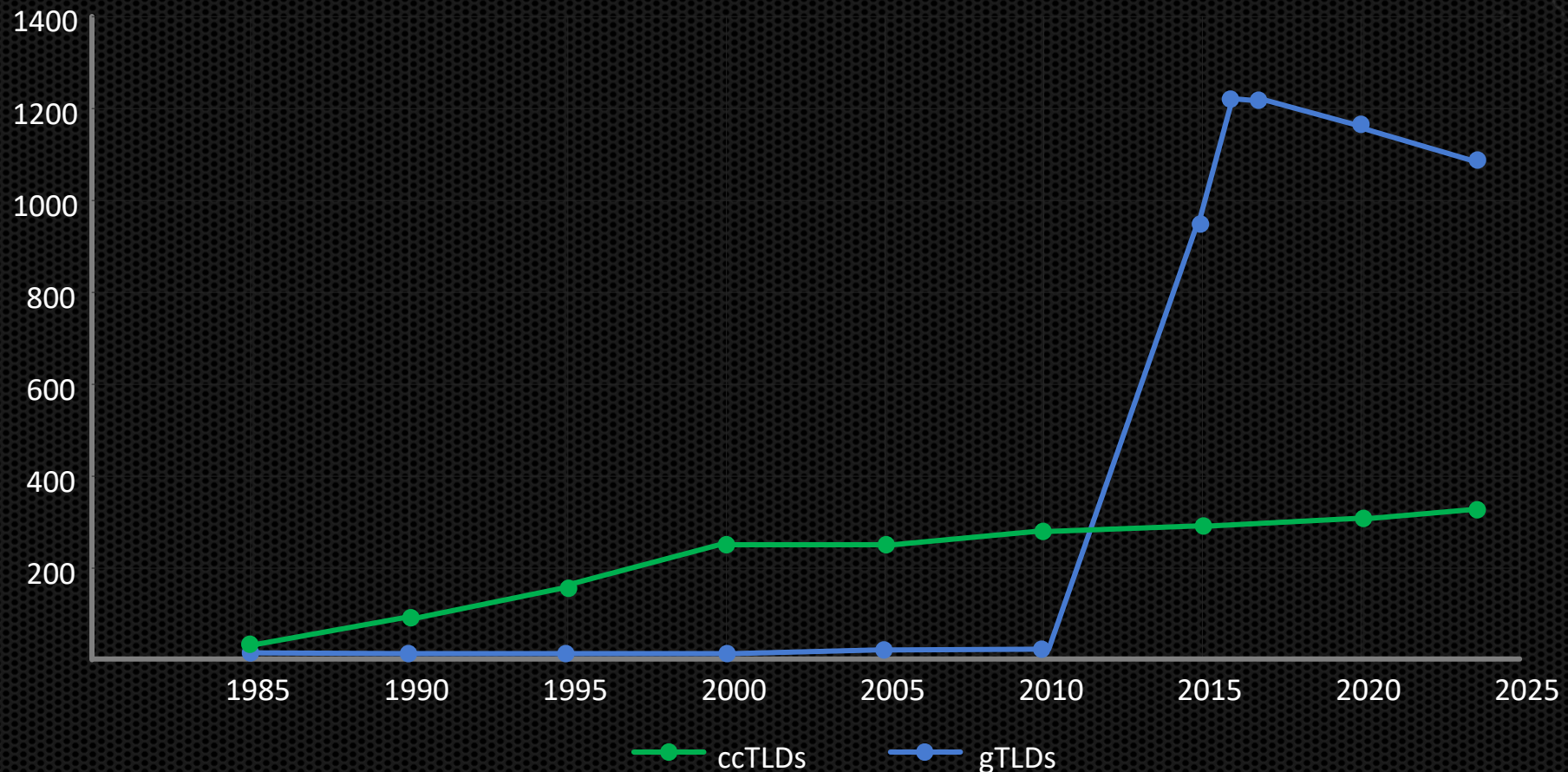
Definitions

Top Level Domains (TLDs)

- Internet Corporation for Assigned Names and Numbers (ICANN)
- 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, .co.uk, .ad, 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.



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 to the Internet's root zone
- Between



1985 1990 1995 2000 2005 2010 2015 2020 2025

—●— ccTLDs

—●— gTLDs

ICANN Revenue

- **One time revenue from new gTLD applicants**

- New gTLDs application fee: **\$185,000** (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**



- **Recurring revenue from gTLD registry operators** (~1200 registry operators)

- Annual registry fee: **\$25,000** per year
- Transaction fee: **\$0.25** per transaction (i.e., registrations, renewals, or transfers) after the first 50,000 transactions/ quarter



- **Recurring 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



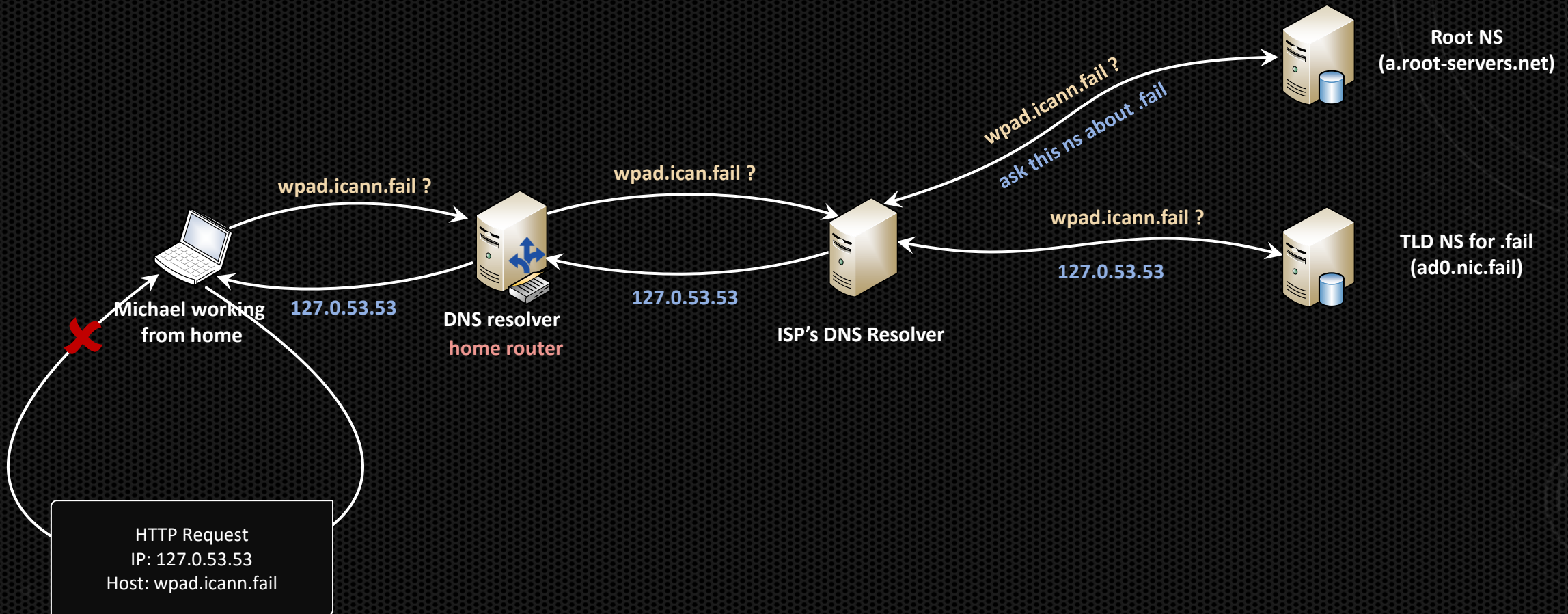
Registry Operator Revenue

- 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**

ICANN's effort to prevent name collision

- Name collision occurrence management framework
 - Restrict “high-risk” strings (e.g., **.home**, **.corp**, **.mail**)
 - **Controlled interruption** for a continuous period of no less than **90 days**.
 - Registry operators must respond to name collision reports from ICANN within **24 hours**.

Controlled interruption



[...] if the browser can't retrieve a the valid wpad.dat the browser falls back to direct connection [...]

Controlled interruption



pot NS
servers.net)

NS for .fail
(.nic.fail)

[...] if the

ction [...]

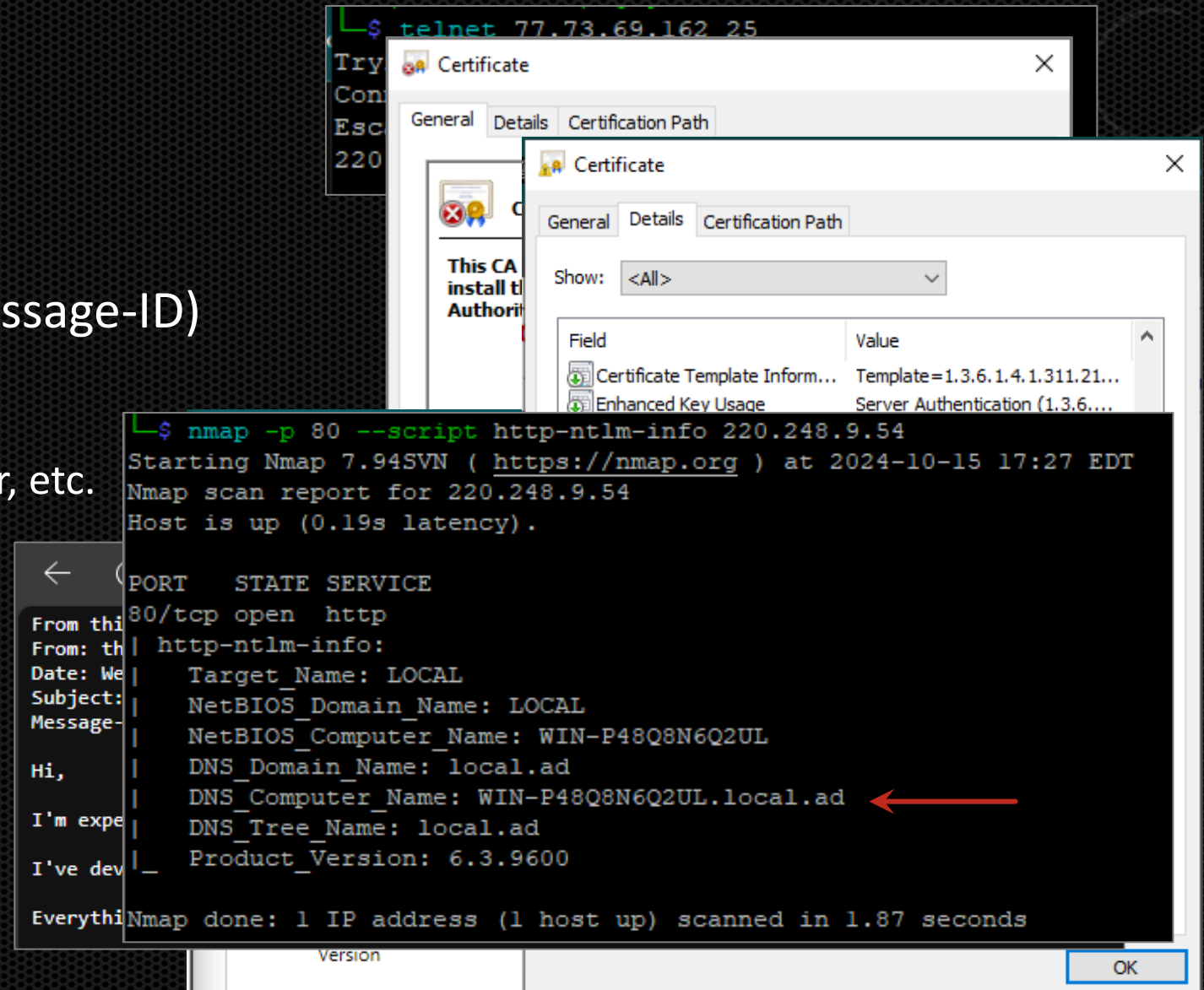
Methodology

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

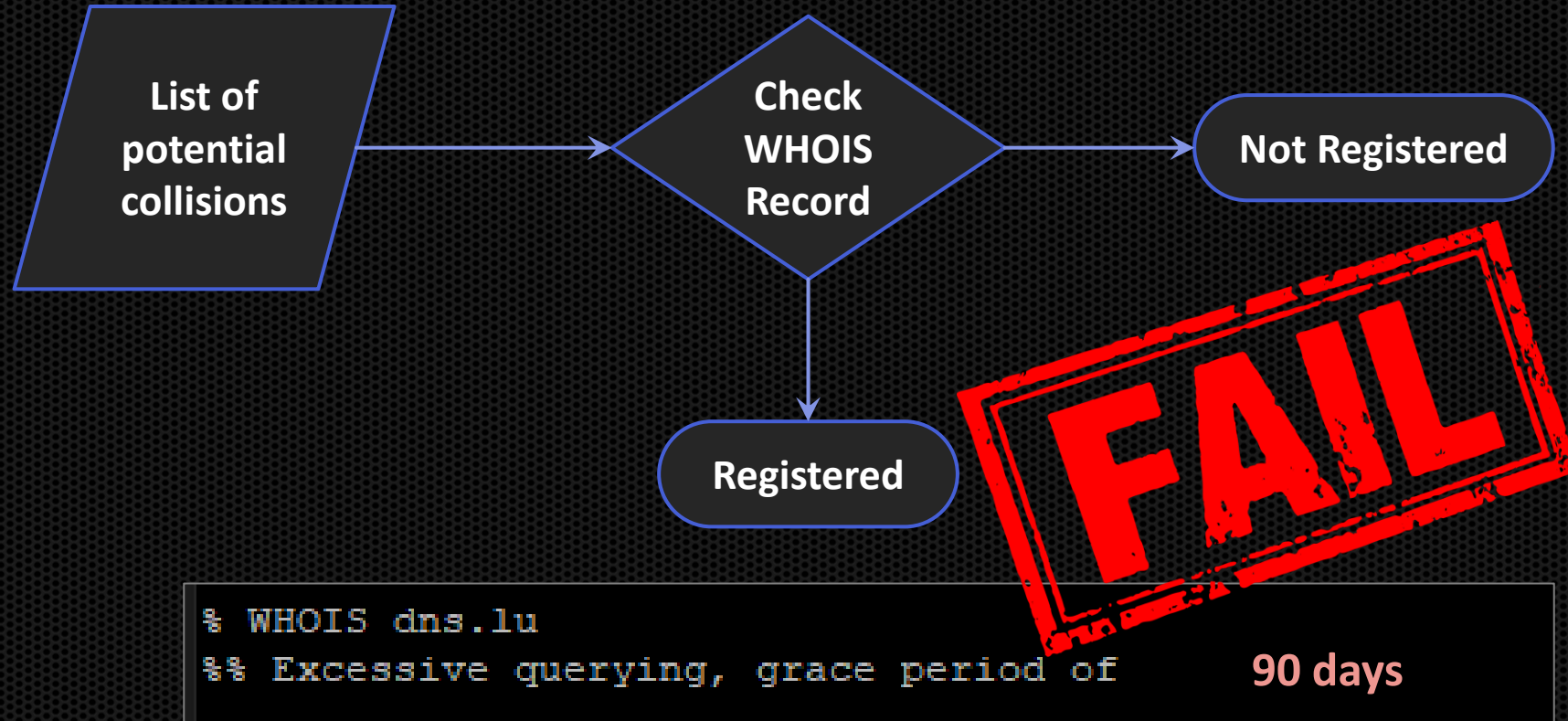
- Banner (e.g., Telnet, FTP, SMTP)
- SSL Self-Signed Cert
- CRL in SSL Certs
- Email Headers (e.g. Received, Message-ID)
- NTLM Authentication
 - HTTP/HTTPS, SMTP, RDP, SQL Server, etc.
- TLS Services
 - RDP, SMTPS, IMAPs, FTPS, etc.



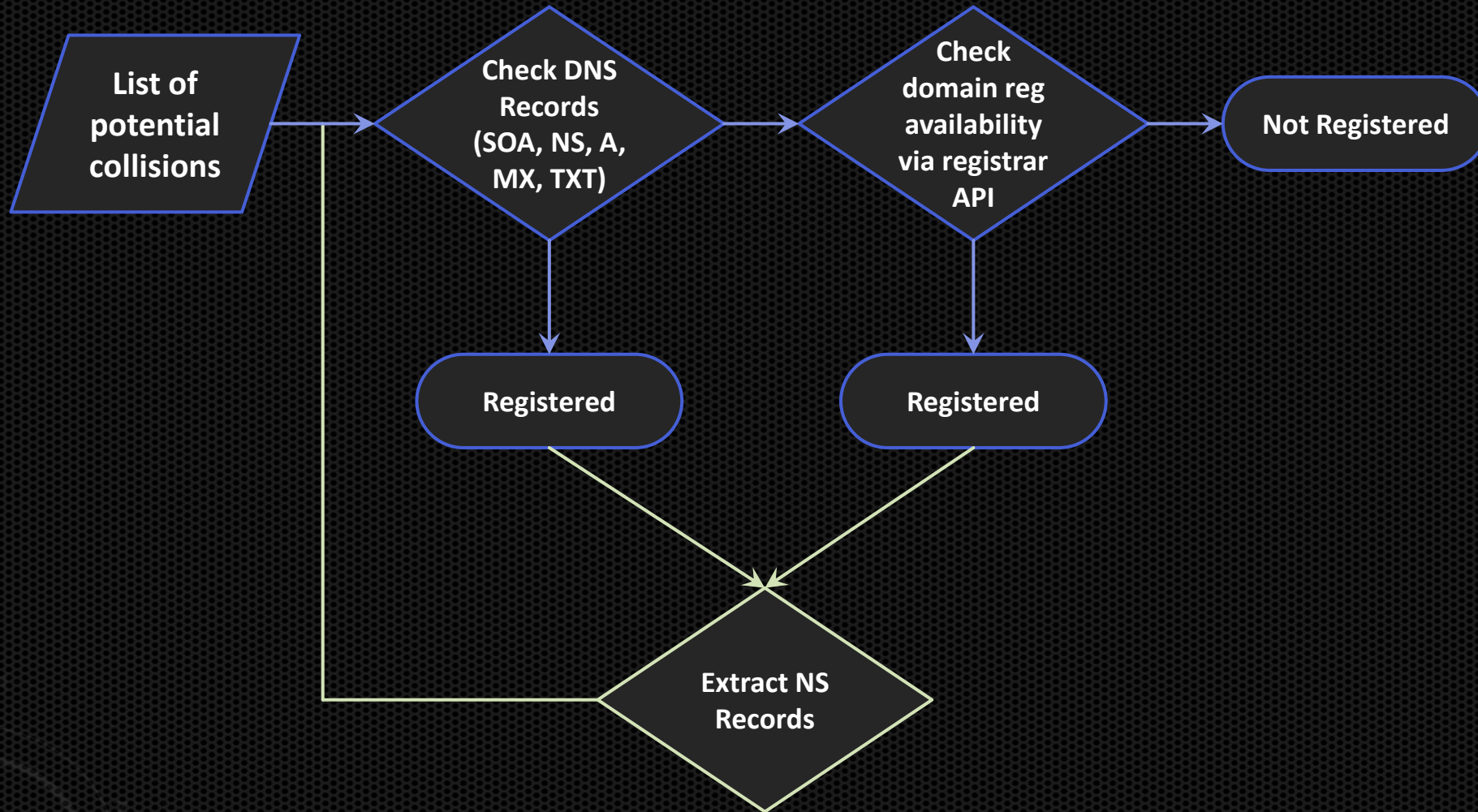
Objective #2 - TLDs prone to ~~confusion~~ collision

- 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)
 - **Common legal entities** (.inc, .llc, .ltd, .gmbh, .limited, .sarl)
 - **Ambiguous / Common technical terms** (.host, .zone, .site, .dev, .box, .cloud)

Objective #3 – Check registration status




Objective #3 – Check registration status



Examples

Examples - memrtcc.ad



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


⚙ 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

MPD-

Examples - memrtcc.ad



MEMPHIS POLICE DEPARTMENT

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 supporting the IT systems and networks throughout the Police Division.

Law enforcement requires timely and secure access to services that provide data whenever and wherever for deterring and reducing crime. The exchange of criminal justice information is

Accomplishments for 2013

During fiscal year 2013, we made significant progress on a number of key initiatives:

- 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.
- KIOSK Upgrade**
The MPD Kiosk system was originally written using Visual FoxPro as its programming language. On January 12, 2010 mainstream support for Microsoft Visual FoxPro ceased. In 2013 a decision was made to rewrite Kiosk using PHP code. The new MPD Kiosk is now

2014 Information Systems Goals

- Cyberwatch program, electronic FTO program and an electronic bid program.
- Institute the (ACES) Automated Case Examination Service investigative protocol.
- Add cameras to the Greater Memphis Greenline.

RTCC = Real Time Crime Center

26 MEMPHIS POLICE DEPARTMENT | 2013 ANNUAL REPORT

Examples - memrtcc.ad



Examples - memrtcc.ad

The screenshot shows a web interface for domain registration. At the top, there are three steps: 1 Cart summary, 2 Configuration, and 3 Review & pay. The main content area is divided into two sections. On the left, under '1 Cart summary', the domain 'memrtcc.ad' is listed with a 'Registration' button and a 'Duration' dropdown set to '2 years'. The price is shown as '€138.00'. On the right, under '3 Review & pay', there is an 'Order summary' section showing 'memrtcc.ad' and a 'Total' price of '€138.00'.

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

1

Cart summary

memrtcc.ad

Registration

Duration

2 years

Dear customer,

We inform you that to register an "ad" trademark in the over requested domain name commercial use registration the domain.

Regarding the DNS Registration



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

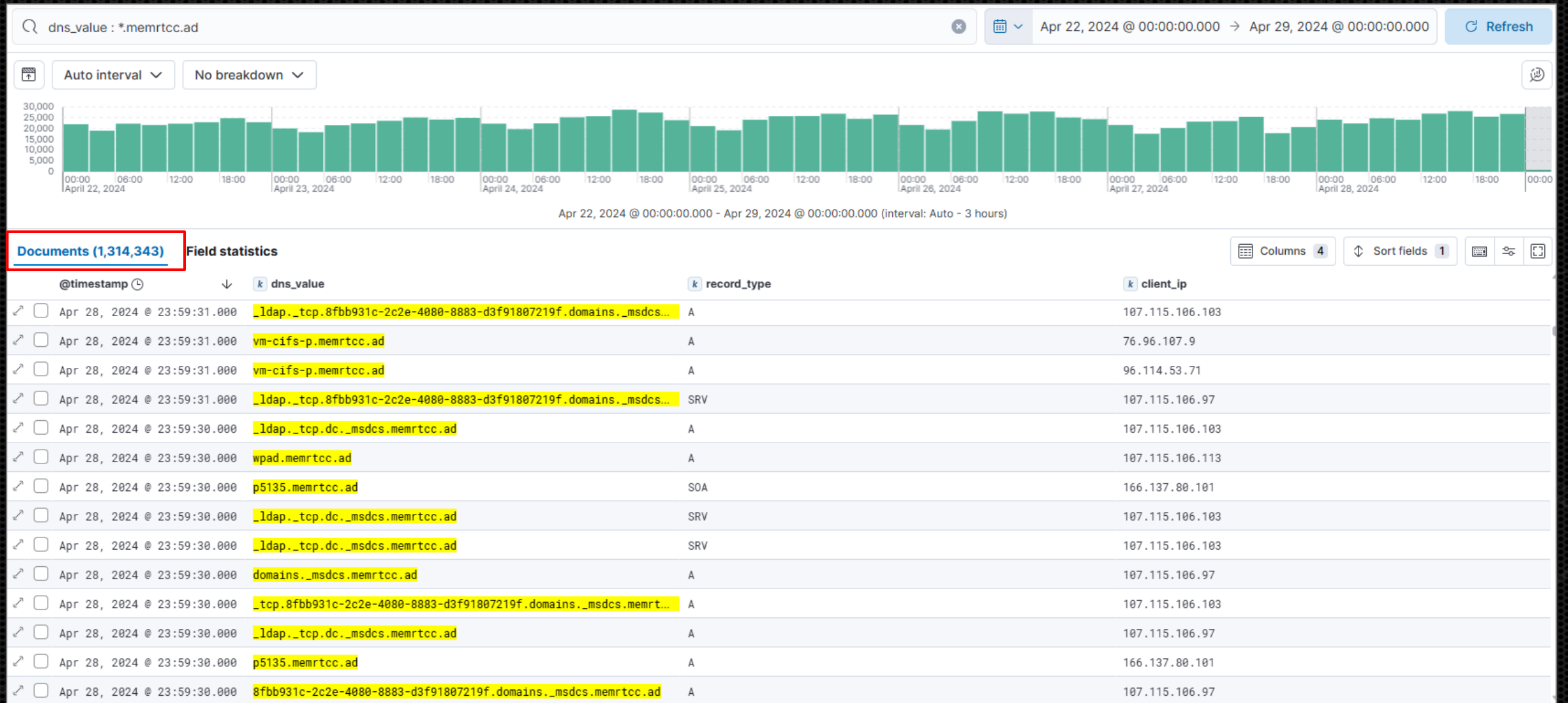
trademark for domain:
agent's fees 150,00 €).

at the registration


the trademark and
attorney signed in the


, we will file the primary
domain.ad management

Examples - memrtcc.ad




Examples - memrtcc.ad

Your Incident INC0223012 has comments added External Inbox x 

 **IT Service Desk** <memphistn@service-now.com> Thu, Apr 11, 3:48 PM ★ ↩ ⋮
to [REDACTED]

Hi Otis Edwards,



INC0223012 - Email Issue

Comments:


04-11-2024 14:48:06 CDT - [REDACTED] Additional comments
@ [REDACTED]: The title has to be updated by HR first.
Resubmit when the change has been made.


04-11-2024 14:44:47 CDT - J [REDACTED] Additional comments
Description :
Please change my email to my new rank ro 2nd Lieutenant. Thank you.
901-672-3879 [REDACTED]

[Take me to the Incident](#)

Thank You,
Service Desk
City of Memphis

Password Changed External Inbox x

 **CoM Okta Support** <okta@memphistn.gov> Thu, Apr 4, 6:43 PM ★ ↩
to [REDACTED]



City of Memphis - Okta Password Changed

Hi Lester,
[REDACTED]

A password was changed for your Okta account Lester.Mikles@memrtcc.ad.
[REDACTED]

Details

Thu, April 4, 2024
Memphis, Tennessee, United States
Performed by: Lester Mikles
[REDACTED]

Don't recognize this activity?

Your account may have been compromised; we recommend reporting the suspicious activity to your organization.

[Report Suspicious Activity](#)

The security of your account is very important to us and we want to ensure that you are updated when important actions are taken.

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)







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 FQDN** extracted
- 2,484 **not registered** (89%)

Examples - local.ad / internal.ad

✓ AVAILABLE

 local.ad


Domains include:  EMAIL  DNS  SSL




 [Domain info](#)

Duration
2 years ▼

€69.00/year 

✓ AVAILABLE

 internal.ad

Domains include:  EMAIL  DNS 

 [Domain info](#)

Duration
2 years ▼

€69.00/year 

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)

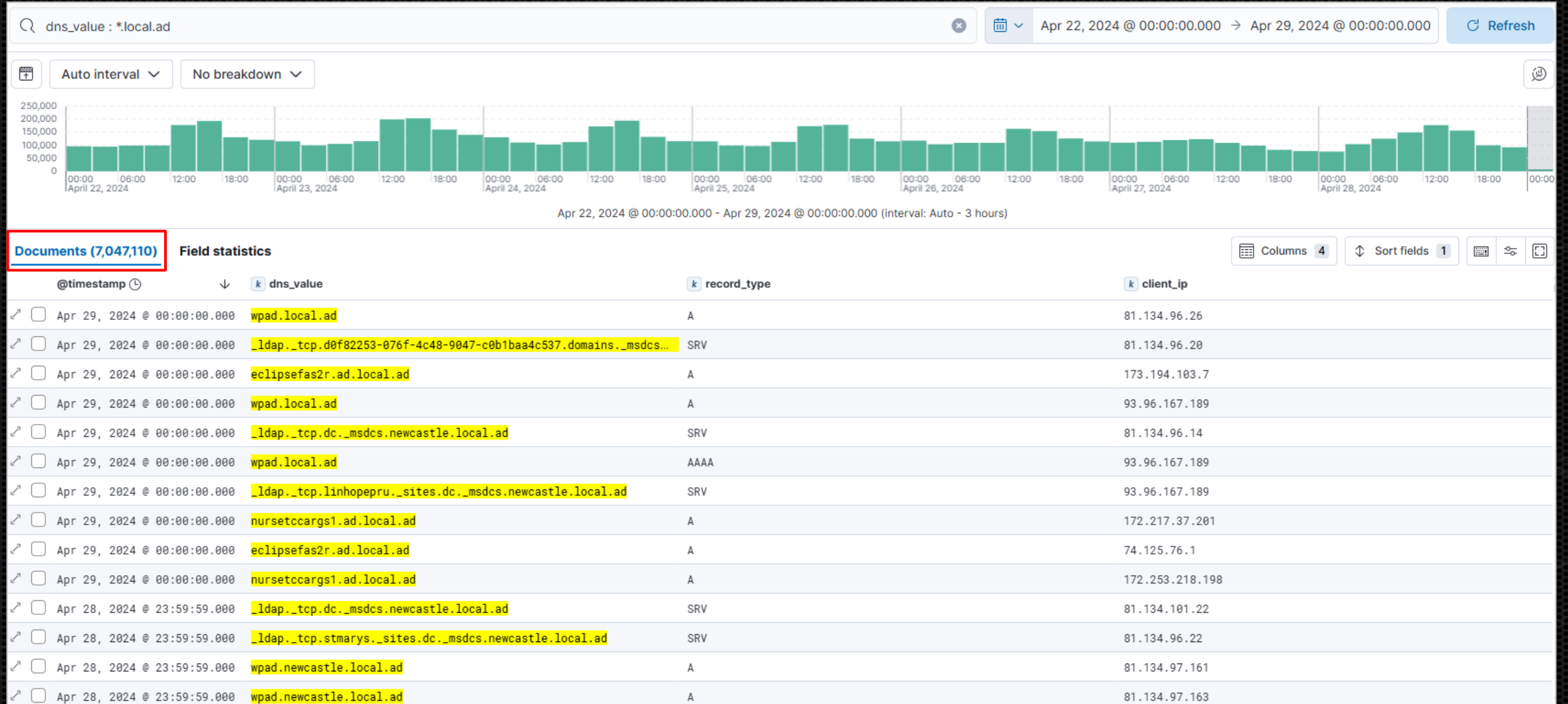
Denominació social (Denominación social / Name of company / Dénomination officielle complète)

SERALYS

Forma jurídica (Forma jurídica / Legal form of constitution / Forme juridique)

SÀRL

Examples - local.ad / internal.ad



Examples - local.ad / internal.ad

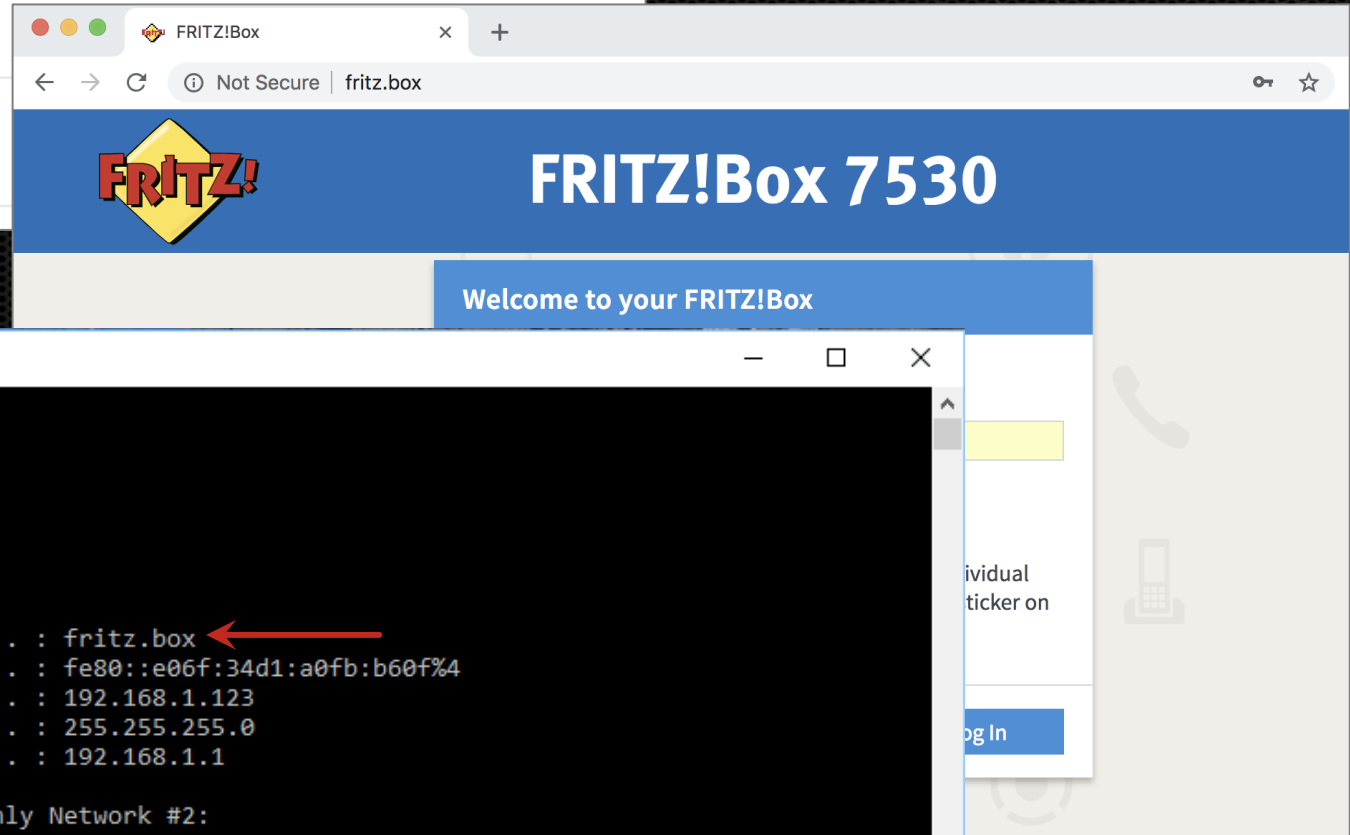
- Over **1,200 different domains / companies** colliding with these domains.
- In 2020, Microsoft purchased “corp.com” before the domain was put for auction.
- Reached out to Microsoft via MSRC, but didn’t even make the triage.
- Asked for an “official statement” for our talk.
- Microsoft corporate domains service group reached out.
- Reopened MSRC case...

Examples - .box

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

PR Newswire

Thu, Jan 18, 2024 • 3 min read



```
Command Prompt

C:\Users\BoxUser>ipconfig

Windows IP Configuration

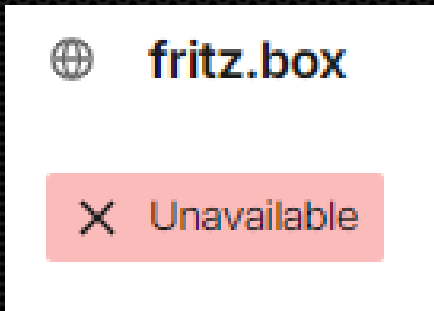
Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : fritz.box
    Link-local IPv6 Address . . . . . : fe80::e06f:34d1:a0fb:b60f%4
    IPv4 Address. . . . . : 192.168.1.123
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter VirtualBox Host-Only Network #2:

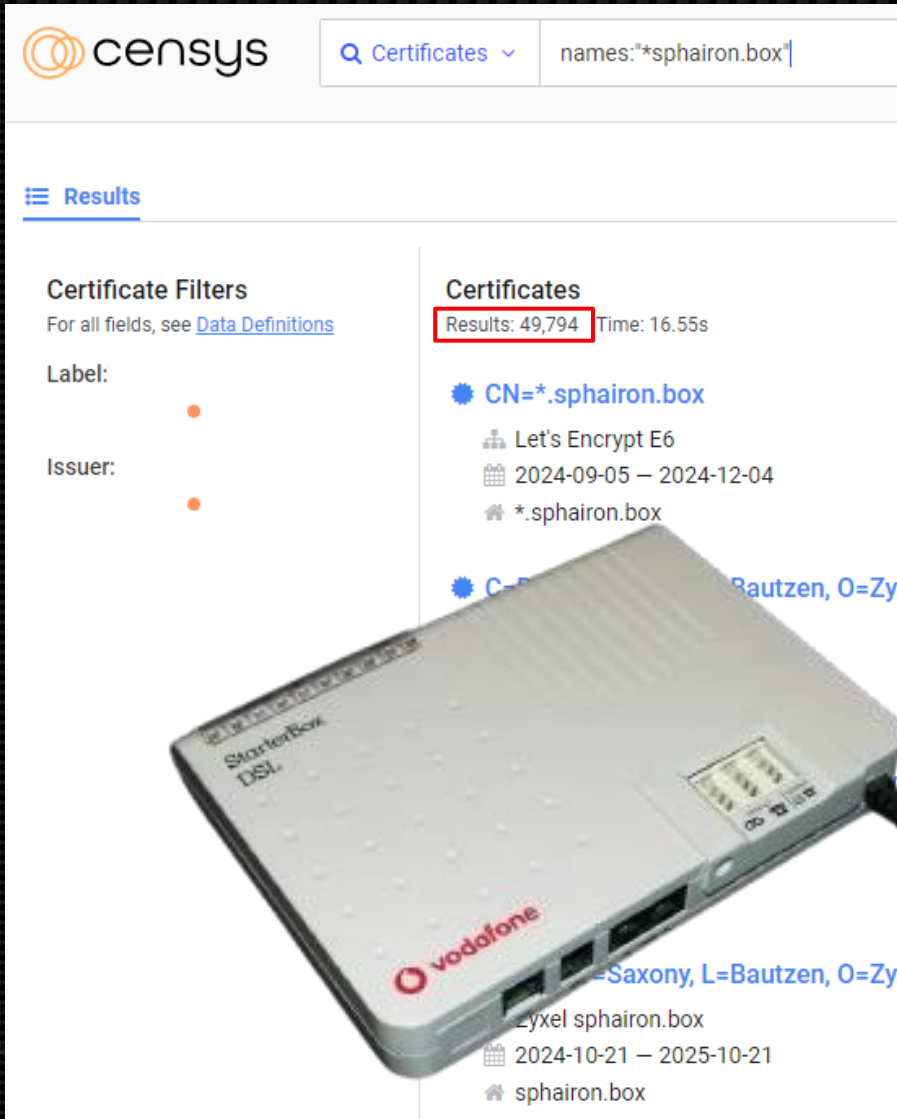
    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::a4cc:d892:bf5f:c968%5
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```


Examples - .box



- 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**

Examples – zyxel.box / sphairon.box



Censys Certificates
names:"*sphairon.box"

Results


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, E=sphairon@zyxel.de, O=Saxony, L=Bautzen, O=Zyxel, OU=Sphairon, CN=zyxel.sphairon.box**
 - 2024-10-21 — 2025-10-21
 - sphairon.box



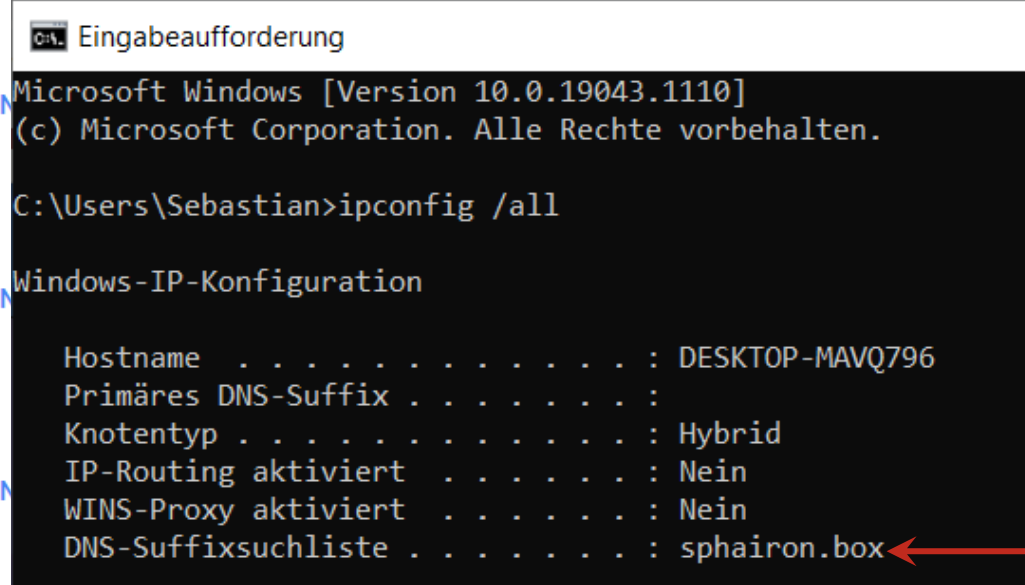


sphairon.box

✓ Available

120.00 USDC

Buy Domain →



Eingabeaufforderung

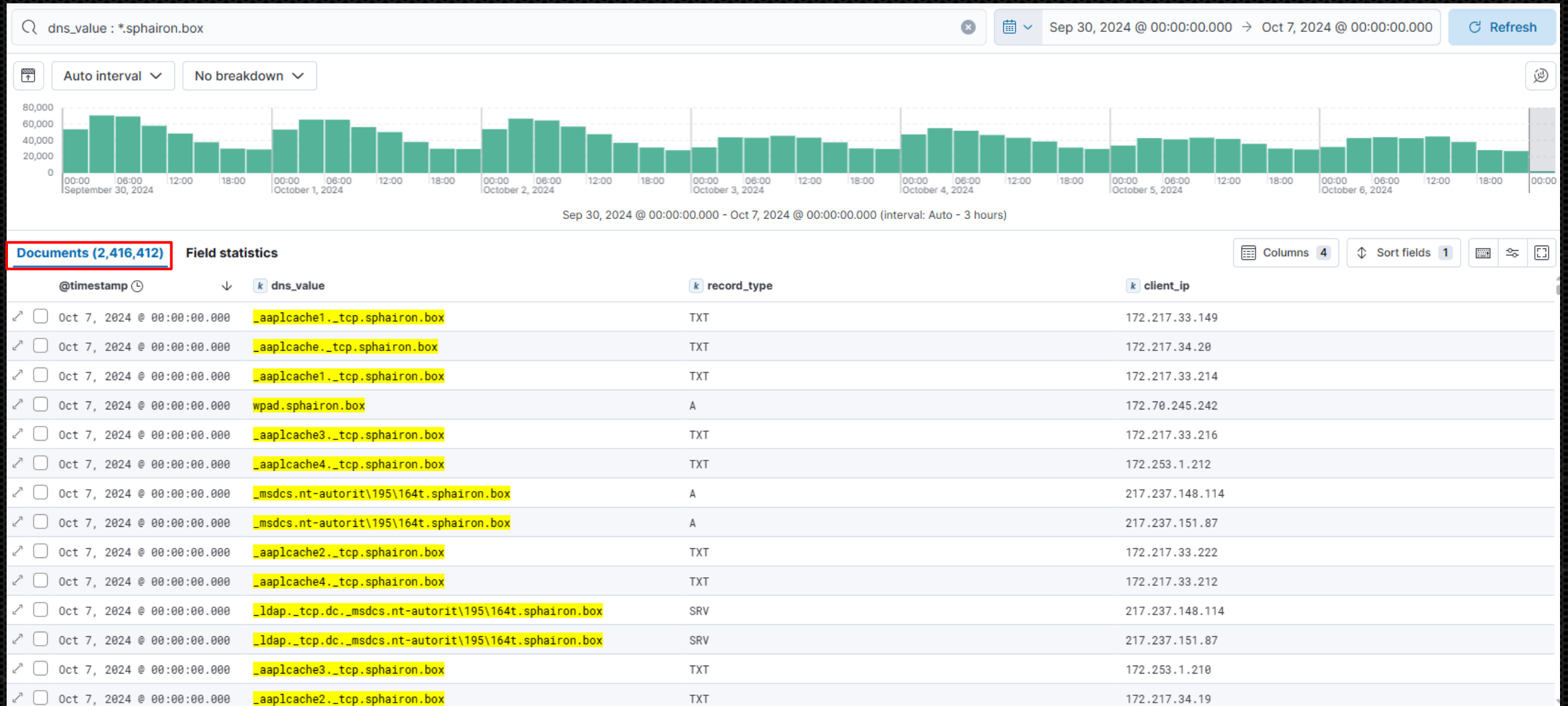
Microsoft Windows [Version 10.0.19043.1110]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Sebastian>ipconfig /all

Windows-IP-Konfiguration

Hostname	: DESKTOP-MAVQ796
Primäres DNS-Suffix	:
Knotentyp	: Hybrid
IP-Routing aktiviert	: Nein
WINS-Proxy aktiviert	: Nein
DNS-Suffixsuchliste	: sphairon.box

Examples – zyxel.box / sphairon.box



Examples – zyxel.box / sphairon.box

Hi Philippe,

Thanks for reaching out. As you provided, we observed that the results were resolved from the real world. **We believe that the data from a LAN-based host can be used by devices using those technologies in some regions in Europe. The risk exposure is relatively low.**

Regards,
Zykel PSIRT

```
[HTTP] GET request from: ::ffff:217.91.154.236 URL: /wpad.dat
[HTTP] NTLMv2 Client      : 217          6
[HTTP] NTLMv2 Username    : DEN          oeller
[HTTP] NTLMv2 Hash        : moeller::DENT01.DOM:c3be3a7463e43e5e:4A5EF50C8367FB1|          908C8BA:01010000
50036003200330001001E00570049004E002D004700320058005A004300310042004100480032|          1400350036003200
20058005A0043003100420041004800320033002E0035003600320033002E004C004F00430041|          1400350036003200
00000200000344280E820D06A7A133827586FB76F50369BF82A9EA88E14A0F39DFDA55631DB0A|          0000000000000000
E007300700068006100690072006F006E002E0062006F0078000000000000000000000
[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:
2000800350036003200330001001E00570049004E002D004700320058005A0043003100420041|          3300040014003500
D004700320058005A0043003100420041004800320033002E0035003600320033002E004C004F|          4C00050014003500
0000100000000020000002E762665F73A2B7F08344238269118D665F8BBCDDF359A026F72CEB9B3|          1000000000000000
10064002E007A007900780065006C002E0062006F0078000000000000000000000000
[HTTP] WPAD (auth) file sent to 93.241.71.209
```


Examples – zyxel.box / sphairon.box

Hi Philippe,

Thanks for reaching out. As you provided, we observed that the hosts were resolved from internal DNS world. **We believe that this is from a LAN-based host** and some devices using those IP addresses in some regions in Europe. **risk exposure is relatively low**.

Regards,
Zyxel PSIRT

```
[HTTP] GET request from: ::ffff:217.91.154.236 URL: /wpad.dat
[HTTP] NTLMv2 Client : 217
[HTTP] NTLMv2 Username : DEN
[HTTP] NTLMv2 Hash : moeller::D
50036003200330001001E00570049004E00
20058005A00430031004200410048003200
00000200000344280E820D06A7A13382758
E007300700068006100690072006F006E00
[HTTP] WPAD (auth) file sent to 217
[HTTP] Sending NTLM authentication
[HTTP] Sending NTLM authentication
[HTTP] Sending NTLM authentication
[HTTP] Sending NTLM authentication
[HTTP] Sending NTLM authentication
[HTTP] GET request from: ::ffff:93.
[HTTP] Sending NTLM authentication
[HTTP] NTLMv2 Client : 93
[HTTP] NTLMv2 Username : RE
[HTTP] NTLMv2 Hash : Re
2000800350036003200330001001E005700
D004700320058005A004300310042004100
000010000000002000002E762665F73A2B7F
10064002E007A007900780065006C002E0062006F007800000000000000000000
[HTTP] WPAD (auth) file sent to 93.241.71.209
```

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

1010000
6003200
6003200
0000000

B31CFE:
4003500
4003500
0000000

Examples – zyxel.box / sphairon.box

FAIL

```
$ 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
```

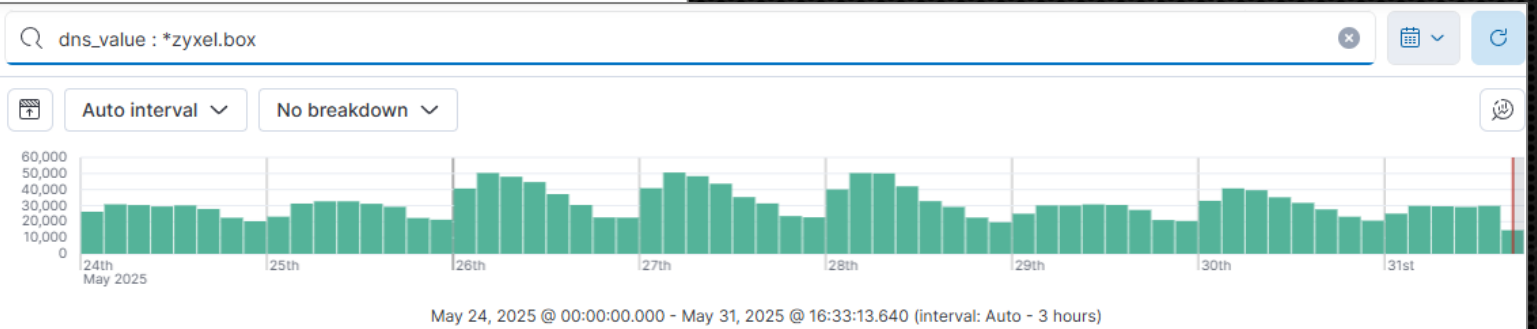
Examples – zyxel.box / sphairon.box



Documents (2,571,308)

Field statistics

@timestamp	dns_value	record_type
May 31, 2025 @ 16:31:03.252	isatap.sphairon.box	A
May 31, 2025 @ 16:31:03.252	isatap.sphairon.box	A
May 31, 2025 @ 16:31:03.250	mas-ext-eu.amazon.com.sphairon.box	A
May 31, 2025 @ 16:31:03.249	trace-server.prod-clustered.bugs.fir...	AAAA
May 31, 2025 @ 16:31:02.247	shiftup-my.sharepoint.com.sphairon.box	A
May 31, 2025 @ 16:31:01.236	dummy.sphairon.box	A
May 31, 2025 @ 16:31:00.229	wpad.sphairon.box	AAAA
May 31, 2025 @ 16:30:59.216	android.apis.google.com.sphairon.box	AAAA
May 31, 2025 @ 16:30:59.216	android.apis.google.com.sphairon.box	A
May 31, 2025 @ 16:30:59.215	sphairon.box	A
May 31, 2025 @ 16:30:56.188	mobilemaps.googleapis.com.sphairon.box	AAAA
May 31, 2025 @ 16:30:56.188	android.apis.google.com.sphairon.box	A
May 31, 2025 @ 16:30:56.187	ipv4only.arpa.sphairon.box	AAAA

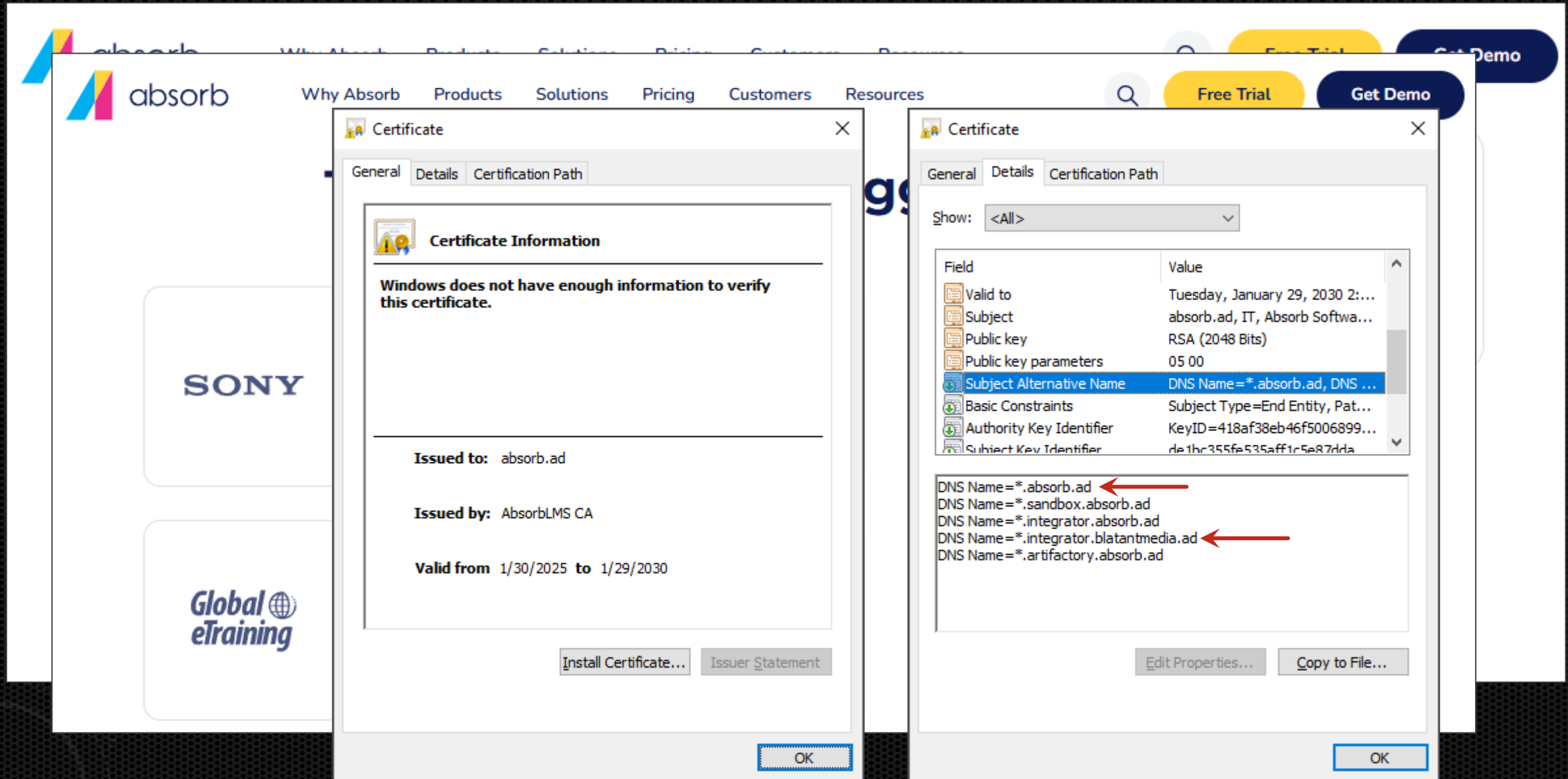


Documents (1,946,044)

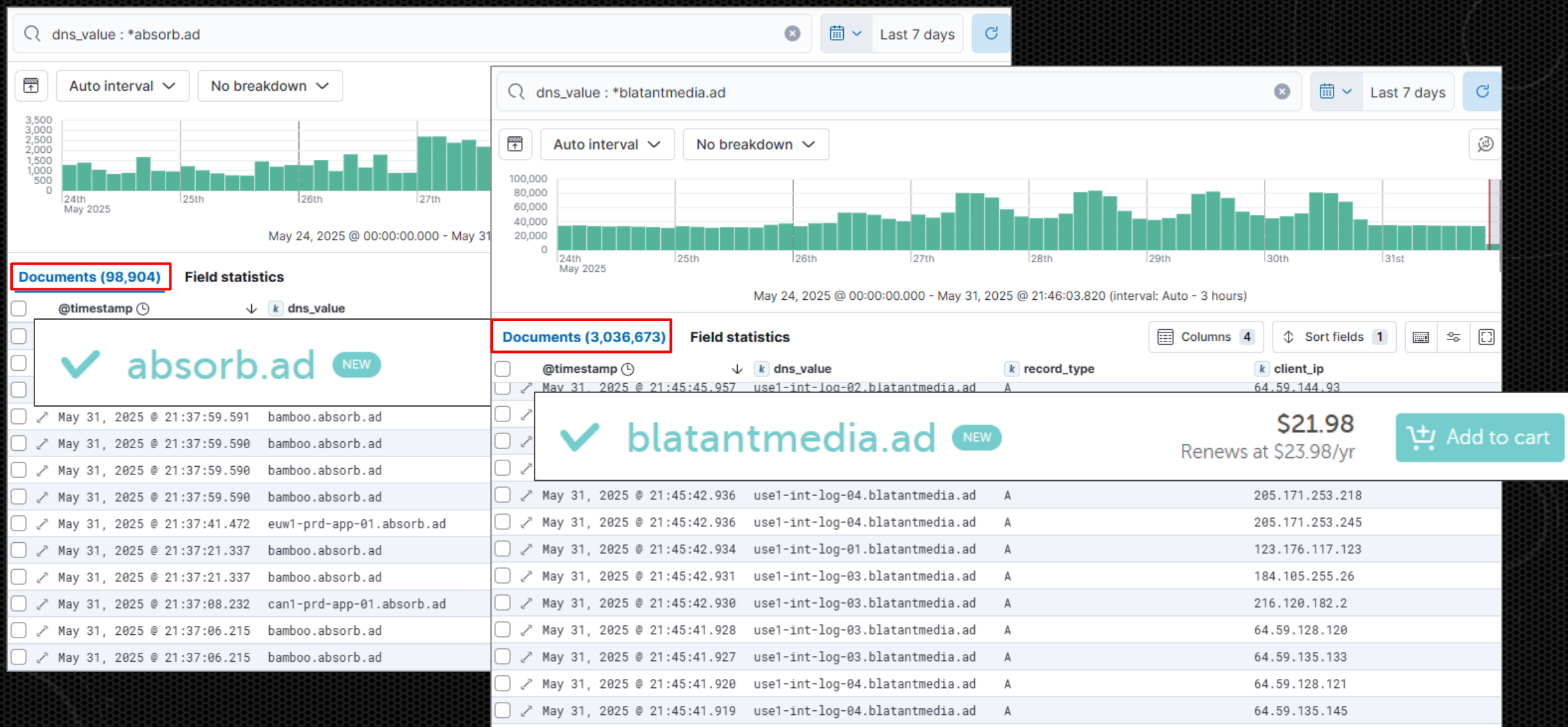
Field statistics

@timestamp	dns_value	record_type	client_ip
May 31, 2025 @ 16:33:01.149	_ldap._tcp.dc._msdcs.nt-authorit\195\...	SRV	172.253.11.29
May 31, 2025 @ 16:33:00.147	dec.quickconnect.to.zyxel.box	AAAA	81.173.194.77
May 31, 2025 @ 16:33:00.147	dec.quickconnect.to.zyxel.box	AAAA	81.173.194.69
May 31, 2025 @ 16:33:00.147	to.zyxel.box	NS	81.173.194.77
May 31, 2025 @ 16:33:00.147	wpad.zyxel.box	A	172.68.20.26
May 31, 2025 @ 16:32:59.137	unifi.zyxel.box	A	172.253.1.209
May 31, 2025 @ 16:32:59.137	alt8-mtalk.google.com.zyxel.box	AAAA	172.217.33.222
May 31, 2025 @ 16:32:58.128	cs-lu-local.zyxel.box.zyxel.box	A	172.217.33.153
May 31, 2025 @ 16:32:56.115	vb-gae-front.ey.r.appspot.com.zyxel....	AAAA	172.217.34.29
May 31, 2025 @ 16:32:56.114	p16-pu-sign-useast8.tiktokcdn-us.com...	AAAA	172.253.1.211
May 31, 2025 @ 16:32:56.111	googleads.g.doubleclick.net.zyxel.box	AAAA	172.217.33.147
May 31, 2025 @ 16:32:56.111	app-measurement.com.zyxel.box	AAAA	172.217.33.148
May 31, 2025 @ 16:32:55.107	zyxel.box	DNSKEY	172.69.113.27

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)

➤ Sales SLA: 6 minutes

➤ Security SLA: 90 days

Your request couldn't be created



GRC - Compliance <jira@absorblms.atlassian.net>

To • Philippe Caturegli



If there are problems with how this message is displayed, click here to view it in a web browser.

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Your request to security@absorblms.com could not be created. If you would still like to get help, please contact the team directly.

If you have received this email in error, please ignore it.

Powered by Jira Service Management



Example: Absorb LMS (How bad is it ?)

- Set up a webserver to record all incoming requests for 24 hours
- *.absorb.ad and *.blatantmedia.ad
- Let's Encrypt SSL certificates

```
$ grep "Request Method:" log | sort | uniq -c | sort -nr
120043 Request Method: GET
 1499 Request Method: PROPFIND
  220 Request Method: POST
   85 Request Method: OPTIONS
   29 Request Method: HEAD
```

- JetBrains ReSharper (JRS) license server – (use1-int-jrs-01.absorb.ad)
 - 28 usernames
- Atlassian Bamboo (CI/CD) – (bamboo.absorb.ad)
- JFrog Artifactory – (artifactory.absorb.ad)
 - Npm install (npm/11.3.0 node/v24.1.0 linux x64)
 - NuGet Command Line/6.14.0 (WINDOWS)
- JWT Tokens – (conversations.localdev.blatantmedia.ad, absorb.localdev.blatantmedia.ad)
- User credentials – (POST /userlogin.action)
- WebDAV – (use1-prd-dms-01.absorb.ad)

Example: Fat fingered NameServers (.gov)

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

; <<>> DiG 9.19.17-2~kalil-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
```



dmaincntrol.com

\$6.49 WITH NEWCOM649

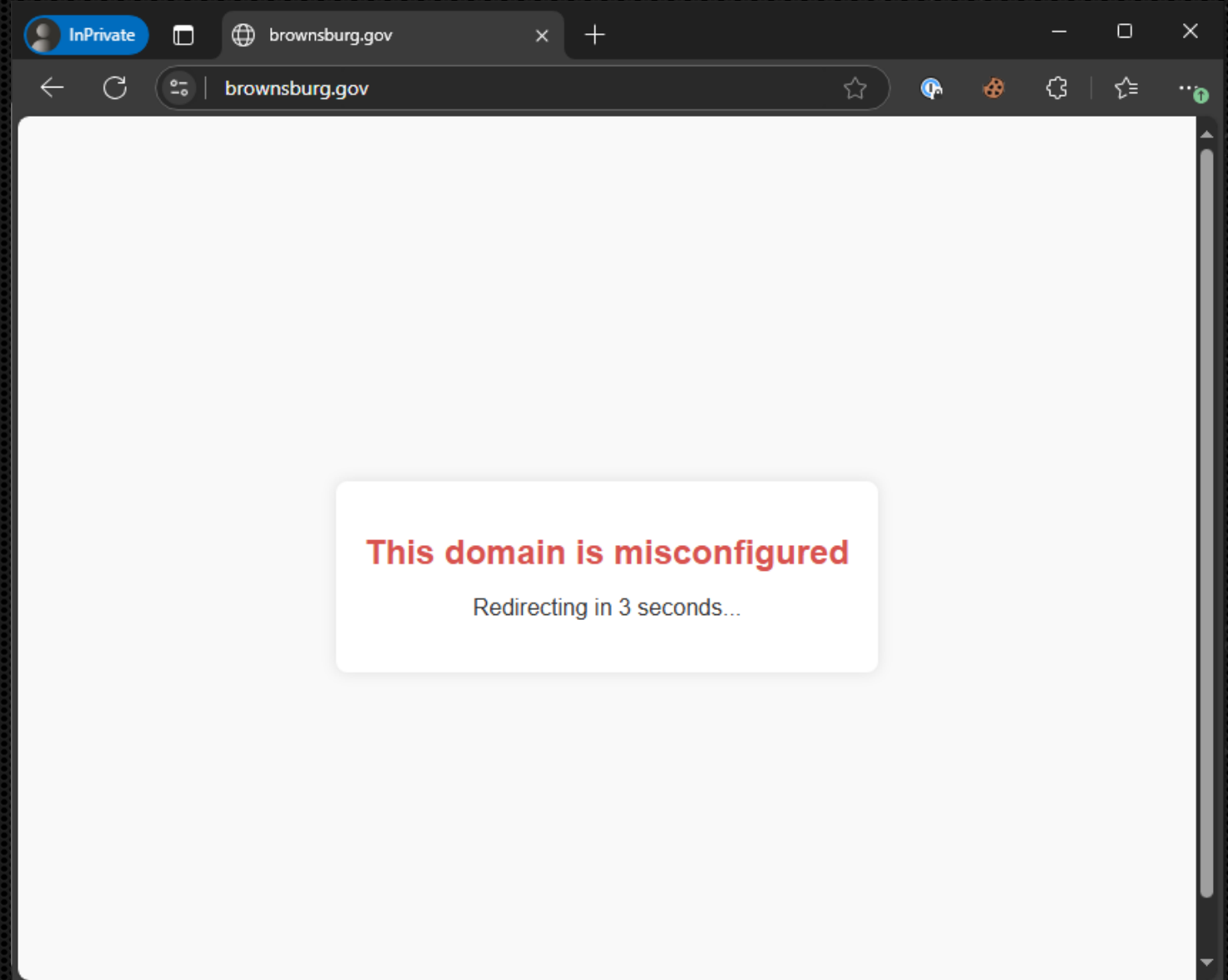
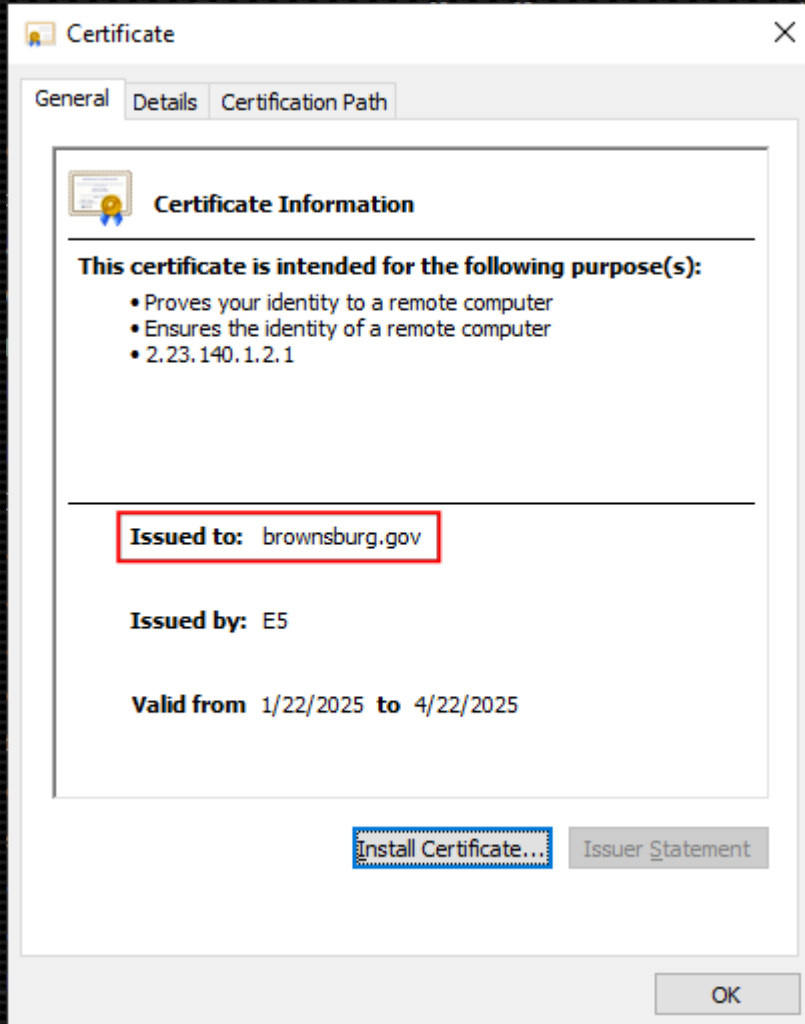


\$11.28/yr
Retail \$14.98/yr



Add to cart

Example: Fat fingered NameServers (.gov)



Example: Fat fingered NameServers (.gov)

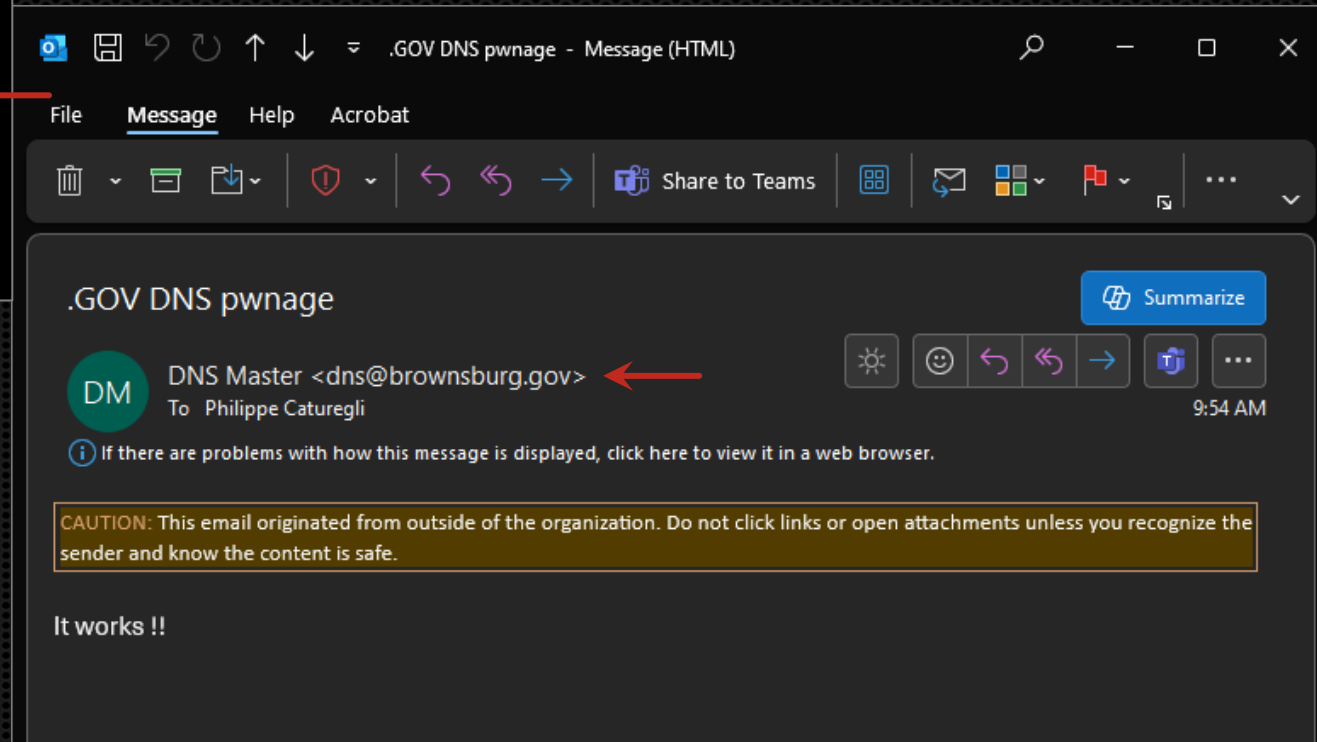
```
# dig MX @8.8.8.8 brownsburg.gov

; <<>> DiG 9.19.17-2~kalil-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

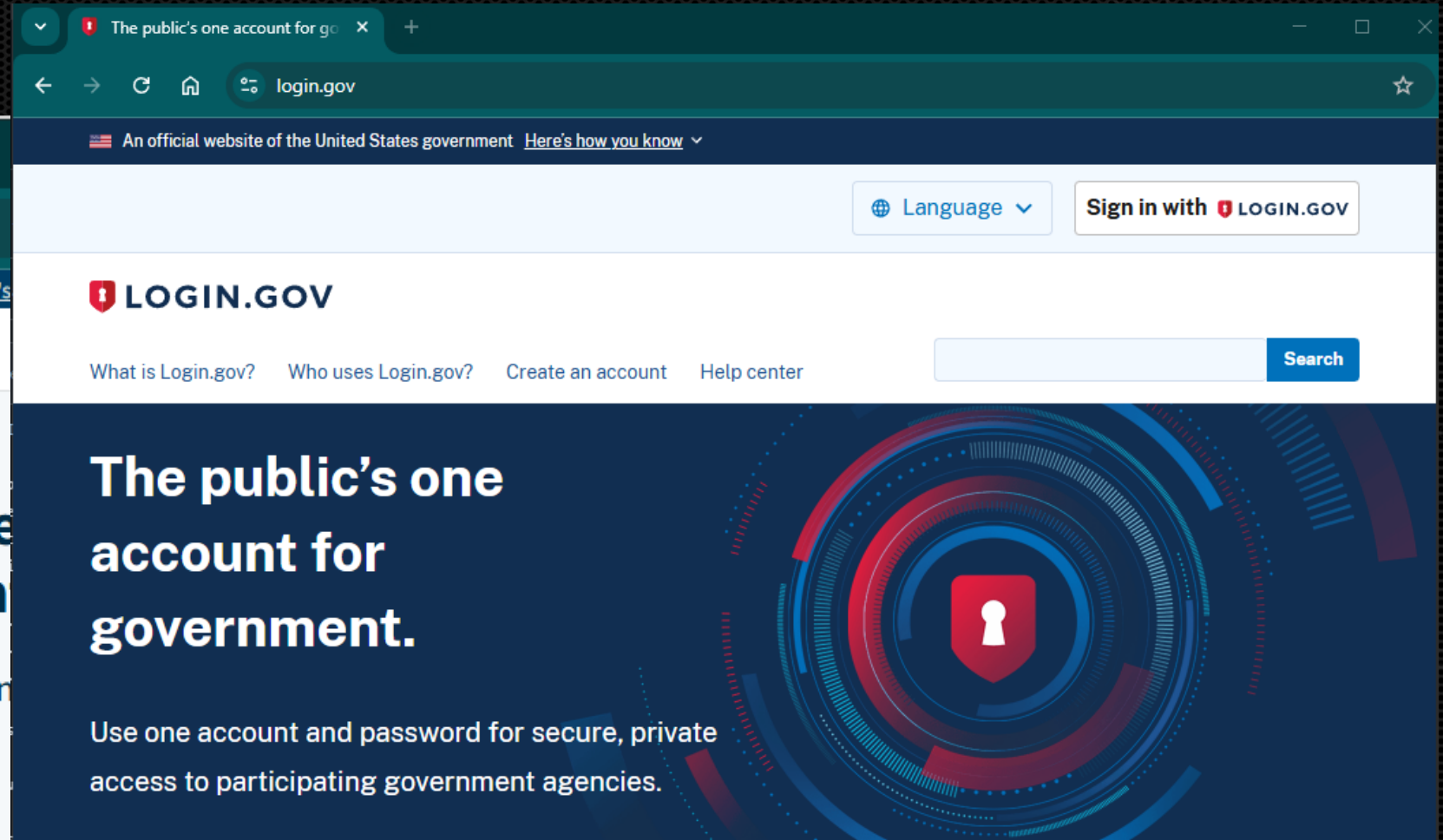
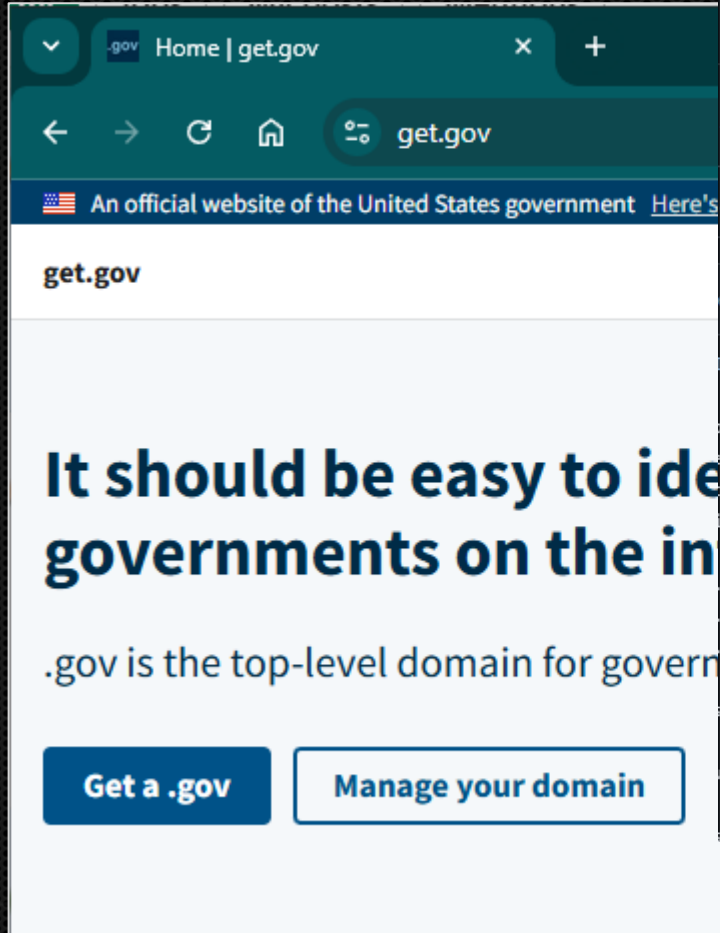
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;brownsburg.gov.                IN      MX

;; 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
```



manage.get.gov



manage.get.gov

GitHub - cisagov/manage.get.gov

Public

Code Issues 319 Pull requests 12 Actions Projects 1 Wiki Security Insights

main

eriny song 3684: Organization overview pa... 9d6d51e · 5 days ago 12,278 Commits

File	Commit	Time
.github	Clarify language and fix links in dev o...	last week
docs	Define platform in docker-compose fil...	2 weeks ago
ops	#3806: Add aa sandbox to workflows (...)	2 weeks ago
src	3684: Organization overview page [ES]...	5 days ago
.gitignore	tweak gitignore	7 months ago
CONTRIBUTING.md	Update contributing.md (#3815)	2 weeks ago
LICENSE.md	Dedicate our work to the public	3 years ago
README.md	Update README.md	last year

About

A Django-based domain name registrar that interfaces with an EPP registry

get.gov

64 stars

9 watching

25 forks

Report repository

Releases 358

V1.118.0 Latest 4 days ago

+ 357 releases

Contributors 30

Infrastructure as a (public) service

The .gov domain helps U.S.-based government organizations gain public trust by being easily recognized online. This repo contains the code for the new .gov registrar – where governments request and manage domains – and other artifacts about our product strategy and research.

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

manage.get.gov

gov | Django site admin

manage.get.gov/admin/analytics/

Relaunch to update

.gov admin

Home

Start typing to filter...

You don't have permission to view or edit anything.

Registrar Analytics

At a glance

- User Count: 11396
- Domain Count: 13120
- Domains in READY state: 11972
- Domain applications (last 30 days): 627
- Approved applications (last 30 days): 97
- Average approval time for applications (last 30 days): 10 days

Current domains

[All domain metadata](#) [Current full](#) [Current federal](#)

[All domain requests metadata](#)

Growth reports

Start date: 01/14/2025 End date: 01/14/2025

[Domain growth](#) [Request growth](#) [Managed domains](#) [Unmanaged domains](#) [Update charts](#)

Commit 3192107

[Browse files](#)



rachidatecs committed on Jan 30 · 7 / 10 · **Verified**

Use `method_decorator` and mixins on report views



main (#3436) · v1.118.0 · staging-143-hotfix

1 parent [dc1322c](#) commit 3192107

Example: Fat fingered NameServers (akam.ne)

```
# dig -t NS santanderconsumer.es

; <<>> DiG 9.19.17-2~kalil-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

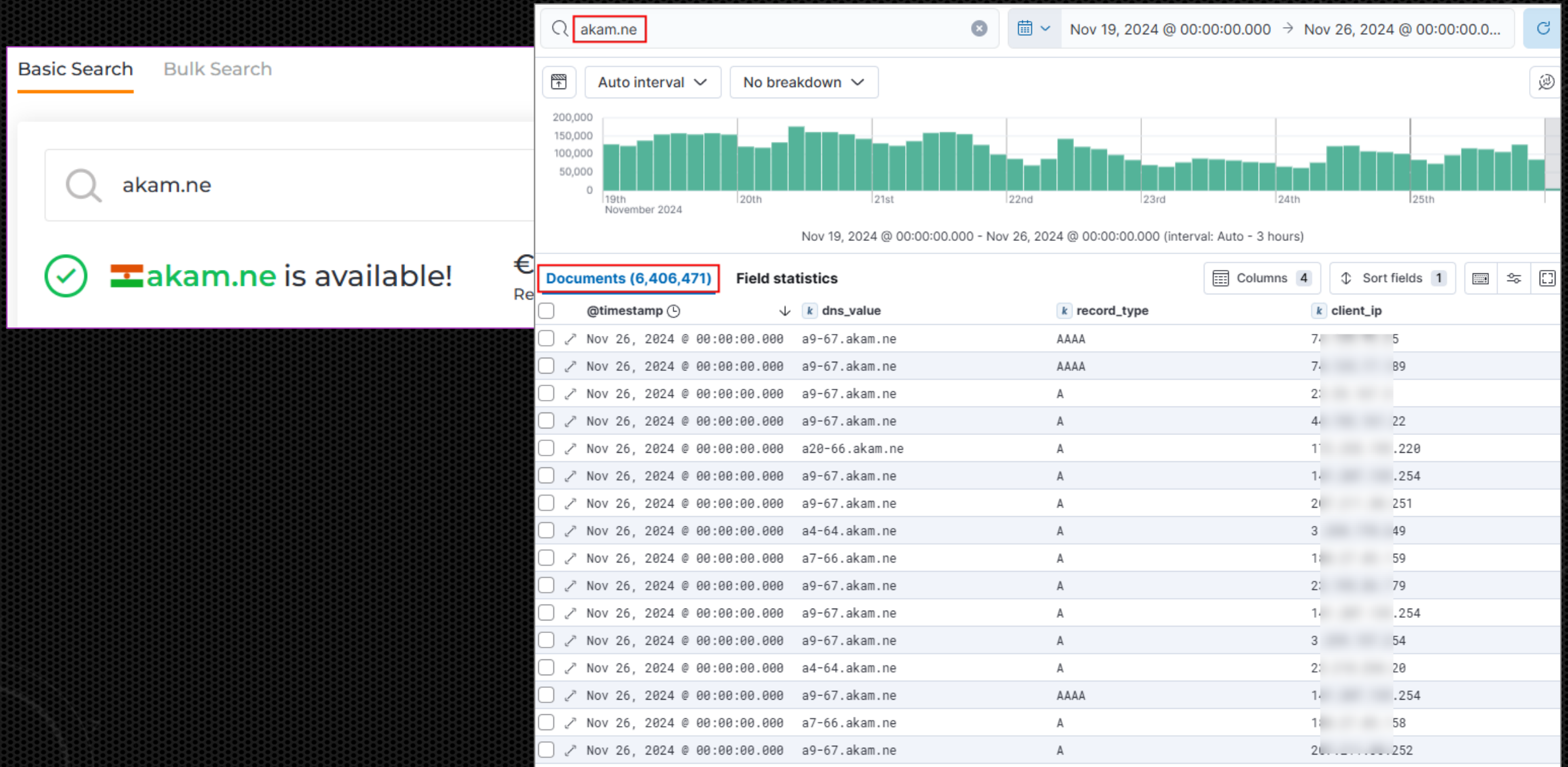
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 512
;; QUESTION SECTION:
;santanderconsumer.es.      IN      NS

;; 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.
```


Example: Fat fingered NameServers (akam.net)



Example: Fat fingered NameServers (akam.ne)



Example: Fat fingered NameServers (akam.ne)

232908	tr ██████████.com.au	13.211.12.222	A
232909	_kerberos_tcp.Casa-Central_sites.dc.█████████.COM.AR	181.30.140.202	SRV
232910	book.█████████.com	184.178.231.18	A
232911	R0000s0008apl.bh.com.ar	181.30.140.141	A
232912	sv ██████████.com	45.32.216.172	A
232913	sv ██████████.com		None
232914	apigw.prod.westus.az.mastercard.com	172.70.161.98	NS
232915	apigw.prod.westus.az.mastercard.com	172.69.193.220	A
232916	westus.az.mastercard.com	172.69.193.220	A
232917	099r ██████████.com.ar	181.30.140.138	SOA
232918	_ldap_tcp.pdc_msdc.█████████.edu	69.252.230.203	SRV
232919	tr ██████████.com	3.0.27.156	A

Example: Fat fingered NameServers (akam.net)

```
# 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.net.
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
```

```
$ 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.net.

;; 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
```

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

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

Some numbers

- **25,976,061** SSL certificates analyzed (CN, SAN, CRL)
- **7,372,697** Services with NTLM Auth analyzed
- **89,125** domains not registered
- **148** domains registered
- **\$7,538** spent
- **3,334,253,945** DNS request recorded over the last 12 months

Questions ?



Philippe Caturegli
Chief Hacking Officer at Seralys



<mailto:pcaturegli@seralys.com>

