## Azure Gov Cloud

Note: need cool headline and I have more screenshots to illustrate but here's the text etc

Critical Federal Infrastructure Deliberately Exposed to Cyberattack

Numerous Federal Systems Deliberately Misconfigured; Immediate Cyberattack Risk

US Federal Systems Are Ripe for Easy Cyberattack

**On January 14, 2025, multiple U.S. government servers—including those belonging to the Department of Energy, Department of Defense, and the Treasury—were found publicly accessible on the internet, exposing core infrastructure systems such as databases, remote access protocols, and identity services.** This was not the result of an isolated misconfiguration but a **systemic, deliberate exposure** of critical systems tied to national security.

A simple Shodan query—**hostname:database.usgovcloudapi.net no password**—revealed that these servers were accepting unauthenticated login attempts, bypassing standard federal protections such as smartcard and token-based authentication in favor of simple username-password. For this to occur, administrators within Azure Government Cloud would have had to **intentionally assign public IPs and weaken security controls**, overriding built-in safeguards and triggering visible security alerts.

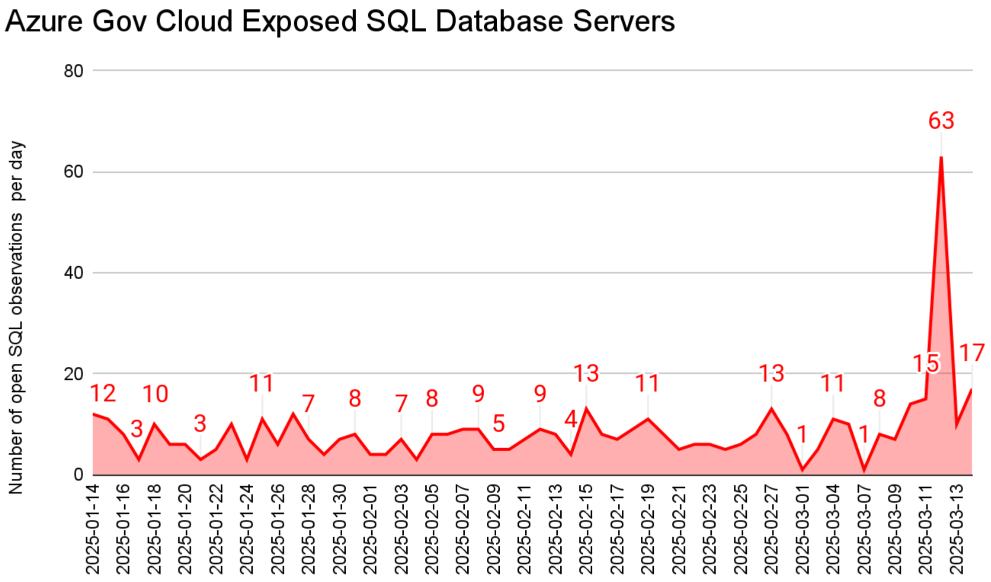
This timeline marks a likely turning point: either a large-scale breach was initiated or a malicious insider enabled adversary access from within. The nature, breadth, and persistence of the exposures strongly indicate **intentional action** rather than oversight.

**This represents a direct threat to national security.** If exploited, these vulnerabilities could allow hostile actors to disrupt federal operations, steal sensitive data, and potentially compromise our nuclear deterrence posture. Any one of these exposures would warrant urgent investigation. **Together, they signal the most significant cybersecurity failure in the history of U.S. government cloud infrastructure.**

Source: Shodan.io query “hostname:database.usgovcloudapi.net no password”

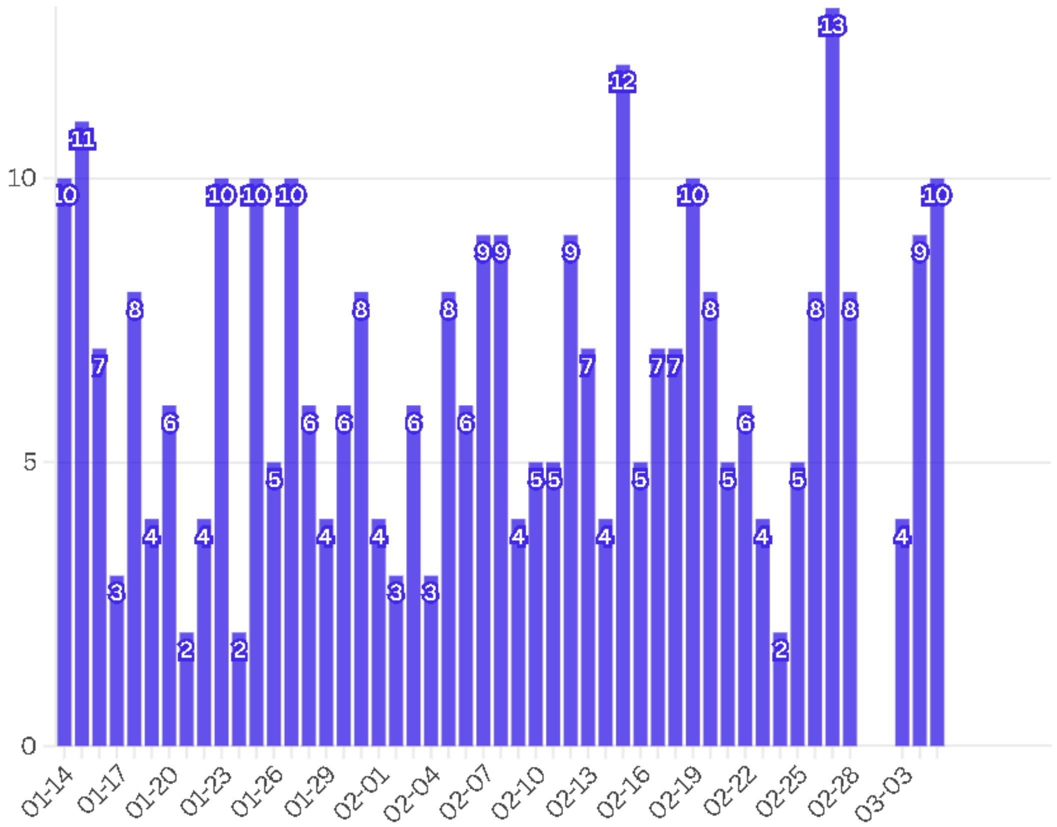
### Database Servers Publicly Exposed and Responding to Connection Attempts, Indicating Simple username-password Authentication

US government database management servers with insecure authentication methods were observed over 1100 times between January and March 2025. There were no entries in Shodan of these federal databases before January 14, 2025, indicating that after this date, all databases were insecurely configured and became publicly visible and accessible via only simple username and password.



About 1/3 of the database endpoint hostnames did not have any historic DNS records and many bore self-signed TLS certificates, suggesting those endpoints are either newly-created or previously-internal.

## 54 Newly-Discovered Azure Gov Cloud Database (PostgreSQL) endpoints allowed 321 Connection Attempts Jan-March 2025

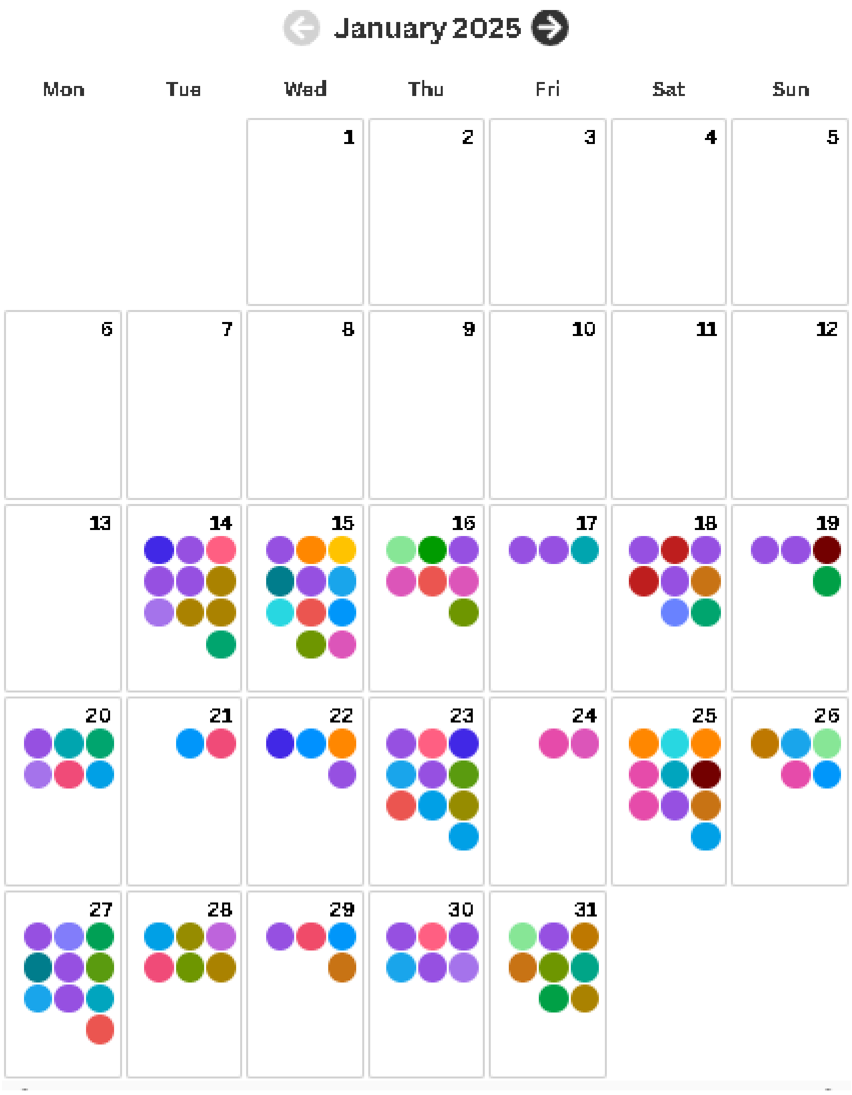


Interactive version:
https://public.flourish.studio/visualisation/22181910/

# Previously Internal Government Databases Exposed, Azure Government Cloud, PostgreSQL Jan - March 2025

All ▾

■ a10ca6cc647c.database.usgovcloudapi.net
■ ffaa22468dee.database.usgovcloudapi.net
■ dcee12fb47c5.database.usgovcloudapi.net
■ ea79ef5c1b8b.database.usgovcloudapi.net
■ cdae8fc464aa.database.usgovcloudapi.net
■ c9168023682a.database.usgovcloudapi.net
■ e1f33ddbcb22.database.usgovcloudapi.net
■ cf88310dd140.database.usgovcloudapi.net
■ d9cadf794d17.database.usgovcloudapi.net
■ f5bd63cad53b.database.usgovcloudapi.net
■ c230e602543e.database.usgovcloudapi.net
■ aa695e2b146a.database.usgovcloudapi.net
■ e7d6d6d94a95.database.usgovcloudapi.net
■ a0ab09d130b1.database.usgovcloudapi.net
■ db6830e627b3.database.usgovcloudapi.net
■ dd61d59e3732.database.usgovcloudapi.net
■ ac73b6eb4219.database.usgovcloudapi.net
■ be37b86600aa.database.usgovcloudapi.net
■ ba47b0a9dd16.database.usgovcloudapi.net
■ d9dc8337521f.database.usgovcloudapi.net
■ d41557d0c606.database.usgovcloudapi.net
■ e4023a82c901.database.usgovcloudapi.net
■ e60632439c51.database.usgovcloudapi.net
■ cb5b09c78d2a.database.usgovcloudapi.net
■ a985f7966cd4.database.usgovcloudapi.net
■ aa1e2e0f4556.database.usgovcloudapi.net
■ a14b0e51fc53.database.usgovcloudapi.net
■ ebaf5bfb5472.database.usgovcloudapi.net
■ ae53cfbfbca5.database.usgovcloudapi.net
■ a8cef95bd513.database.usgovcloudapi.net
■ d52ae69ca7a7.database.usgovcloudapi.net
■ afa1b722fa14.database.usgovcloudapi.net
■ fc55fb649104.database.usgovcloudapi.net
■ d54b688b956f.database.usgovcloudapi.net
■ ee1e868486a3.database.usgovcloudapi.net
■ d10197a3f917.database.usgovcloudapi.net
■ a823e3518bdc.database.usgovcloudapi.net
■ c01ea904fff4.database.usgovcloudapi.net
■ ab13084e649b.database.usgovcloudapi.net
■ ef854311b57e.database.usgovcloudapi.net
■ d782c56817ea.database.usgovcloudapi.net
■ b0ac2bcd9f4f.database.usgovcloudapi.net
■ da4225857ea1.database.usgovcloudapi.net
■ bf9ec49503e2.database.usgovcloudapi.net
■ f52da910f53a.database.usgovcloudapi.net
■ a7b0bfd0401b.database.usgovcloudapi.net
■ dbafc2ca5222.database.usgovcloudapi.net
■ aaf8e6e265fc.database.usgovcloudapi.net
■ a7ba5ae07e7d.database.usgovcloudapi.net
■ a742058f6eaa.database.usgovcloudapi.net
■ a49fef2fd1ef.database.usgovcloudapi.net
■ bf2189e2db9f.database.usgovcloudapi.net
■ f1a8925af5b4.database.usgovcloudapi.net



Source: Shodan.io • Last updated 3/5/2025
Created by Amanda Morton, amorton@protectemployer.com

Interactive
https://public.flourish.studio/visualisation/22037837/
Source query:
https://www.shodan.io/search?query=cloud.region%3Ausgovvirginia+port%3A5432
SQL Browser

| *SQL Monthly summary* | *Products* | Number of times Azure Gov IPs observed | Unique IPs per month | *data* |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 2025-Jan Total | MS-SQL Server and Browser, MySQL, PostgreSQL | 227 | 93 | responded with "no password supplied" |
| 2025-Feb Total | MS-SQL Server and Browser, MySQL, PostgreSQL | 266 | 102 | responded with "no password supplied" |
| 2025-Mar Total | MS-SQL Server and Browser, MySQL, | 612 | 86 | responded with "no password suppl |

|  |  |  |  |  |
|---|---|---|---|---|
|  | PostgreSQL |  |  | ied" |
| **Grand Total** |  | **1105** | **157** |  |

The responses received from these SQL database management servers indicate that simple SQL authentication (username-password) is being used, rather than the far more secure Azure AD token-based authentication.

Drilling down further, we found over 40 instances of SQL Browser on Azure Gov Cloud networks. This is especially alarming because it means the server is listening for connections from **outside the government network.**

The **SQL Server Browser service** listens on UDP port **1434** and responds to requests with instance details like **server name, instance name, and TCP port**, effectively **advertising available SQL instances** on the host. This makes it easy for attackers to **discover and target** SQL database services. It's essentially a **directory service for your database**, which is a bad idea to expose publicly.

| *SQL Browser (port 1434) monthly summary* | *product* | *region* | *port* | Number of times observed | Unique IPs per month |
|---|---|---|---|---|---|
| 2025-Jan Total | SQLBrowser | usgovvirginia | 1434 | 9 | 4 |
| 2025-Feb Total | SQLBrowser | usgovvirginia | 1434 | 19 | 7 |
| 2025-Mar Total | SQLBrowser | usgovvirginia | 1434 | 13 | 7 |
| **Grand T** |  |  |  | **41** | **10** |

| | | | | | |
|---|---|---|---|---|---|
| **otal** | | | | | |

There is no  reason to use simple username/password SQL authentication when Azure token-based authentication is already set up for you. Azure authentication is far more secure and does not cost more time to set up. Whoever configured the SQL databases for this sort of public access would have received many layers of warnings that sensitive data should not be exposed like this."

or something like: "It is straightforward to brute force a password for a SQL database authenticated only by username/password. On a home computer, one could run a program to brute force such a password in about a day. A foreign adversary with a quantum computer would need just 10 or 15  minutes. There is no valid reason to configure these endpoints in such a vulnerable way, leaving the data ripe for exfiltration.**Remote Access: Blueprint for Nation-State Intrusion**

| *RDPMonthlysummary* | *AzureGovCloudregions* | CountofRDPobservations | UniquenumberofIPaddresses |
|---|---|---|---|
| 2025-FebTotal | usgovusgovvirginiausgovtexasusdodeastusgovarizonausdodcentral | 373 | 373 |
| 2025-MarT | | 198 | 198 |

| otal | | | |
|---|---|---|---|
| **GrandTotal** | | **571** | **571** |

Critical remote access protocols were simultaneously exposed across multiple U.S. federal cloud regions. These include:

1. Microsoft Endpoint Mapper (135) – Enumerates services running on remote machines.
2. SMB (445) – Used for file sharing; allows for credential theft or lateral movement.
3. WinRM (5985/5986) – Remote command execution and scripting.
4. RDP (3389) – Full graphical desktop access.

The simultaneous exposure of remote access and management protocols:

- SMB (445) user roles and credentials
- WinRM (5985/5986) command execution and remote management
- Remote Desktop Protocol (3389)  full graphical remote access
- Microsoft Endpoint Mapper (135) what services are running and where

When exposed together, these protocols don't just increase the attack surface—they offer a step-by-step blueprint for intrusion.

Nation-state actors such as China and Russia are highly capable of exploiting these vulnerabilities. They may begin by querying the Endpoint Mapper on port 135 to **enumerate** accessible services, identifying where critical endpoints and remote services reside. From there, they could exploit SMB (445) to perform **credential harvesting** via techniques like NTLM relay or pass-the-hash attacks, using misconfigurations or outdated protocols. Once they acquire valid credentials, they can **escalate** their access using WinRM to issue remote commands or scripts—often stealthily, without triggering basic monitoring. Finally, RDP (3389) can be used for hands-on-keyboard access, allowing attackers to **move laterally**, access sensitive data, or deploy malware directly within the environment.

This sequence would allow attackers to skip several stages of the MITRE ATT&CK framework and move quickly towards data exfiltration or penetrating previously uncompromised networks. When all of these doors are open on a single external-facing government server, the system becomes more than just vulnerable; it becomes a strategic, high-value intelligence asset for adversaries.

## Security Assistance Technical Order Distribution System

Of particular note is continuous exposure of Department of Defense servers that access the Security Assistance Technical Order Distribution System, or SATODS. This system, managed by the Air Force, is responsible for requisitioning foreign military aid to US allies. If compromised, attackers would have access to the amount, type, location, and timing of military aid supporting critical US partners

| *RDPSATODSMonthlysummary* | *IP* | *ports* | *cloud.region* | Relationship |
|---|---|---|---|---|
| 2025-Jan | 62.11.100.105 | 3389 | usgovvirginia | SATODS,USAirForce |
| | 62.11.97.15 | 3389 | usgovvirginia | SATODS,USAirForce |
| 2025-F | 20.141 | 3389 | usgovv | SATODS |

| | | | | |
|---|---|---|---|---|
| eb | .44.221 | | irginia | , USA Air Force |
| | 62.10.108.118 | 3389 | usgovvirginia | SATODS, USA Air Force |
| | 62.10.70.153 | 3389 | usgovvirginia | SATODS, USA Air Force |
| | 62.11.100.105 | 3389 | usgovvirginia | SATODS, USA Air Force |
| | 62.11.96.174 | 80,3389 | usgovvirginia | SATODS, USA Air Force |
| | 62.11.96.233 | 3389 | usgovvirginia | SATODS, USA Air Force |
| | 62.11.97. | 3389 | usgovvirgi | SATODS, USA |

|  |  |  |  |  |
|---|---|---|---|---|
|  | 15 |  | nia | irForce |
| 2025-Mar | 62.11.100.105 | 3389 | usgovvirginia | SATODS, US Air Force |
|  | 62.11.96.174 | 80, 3389 | usgovvirginia | SATODS, US Air Force |
|  | 62.11.97.15 | 3389 | usgovvirginia | SATODS, US Air Force |
|  |  |  |  | **7 Total Unique IPs** |

## Nuclear Cybersecurity: The Most Sensitive Systems at Risk

### Nuclear Risks part 1. Russian Hosts Impersonating US Nuclear Laboratories

Autonomous systems controlled by Russian actors have been impersonating Los Alamos National Laboratory, Lawrence Livermore National Laboratory, NASA, and DHS servers in preparation for what appears to be a larger cyberattack on US nuclear and defense infrastructure.

Shodan query:
https://www.shodan.io/search?query=org%3A%22LLC+Baxet%22+hostname%3Agov

Spreadsheet:
https://docs.google.com/spreadsheets/d/1tbzxm6J_9F4rtmJsuv_Pt5Cl8NCVSKZsR5G_QU5QQJk/edit?usp=sharingA few highlights:

| date | IP address | spoofed domain |
|---|---|---|
| Jan 15, 2025 | 45.130.147 | controlban |

| | | |
|---|---|---|
| | .179 | ding.llnl.gov |
| Jan 20, 2025 | 46.17.43.235 | clinicaltrials.gov, 1linespbu.ru, s.tbcdn.cn, cmos.greencompute.org, www.tpu.ru, www.1-line.spbu.ru |

| | | |
|---|---|---|
| | | , m.intl.taobao.com, 1-line.spbu.ru, alicdn.com, tpu.ru, alikunlun.com |
| Feb 22, 2025 | 103.146.119.152 | i3rc.gsfc.nasa.gov |
| March 12, 2025 | 194.58.46.116 | dx10.lanl.gov, cmi.ed.gov |

| | | |
|---|---|---|
| March 12, 2025 | 46.17.43.235 | clinicaltrials.gov, 1linespbu.ru, s.tbcdn.cn, cmos.greencompute.org, www.tpu.ru, www.1-line.spbu.ru, m.intl.taoba |

|  |  |  |
|---|---|---|
|  |  | o.com,1-line.spbu.ru,alicdn.com,tpu.ru,alikunlun.com |

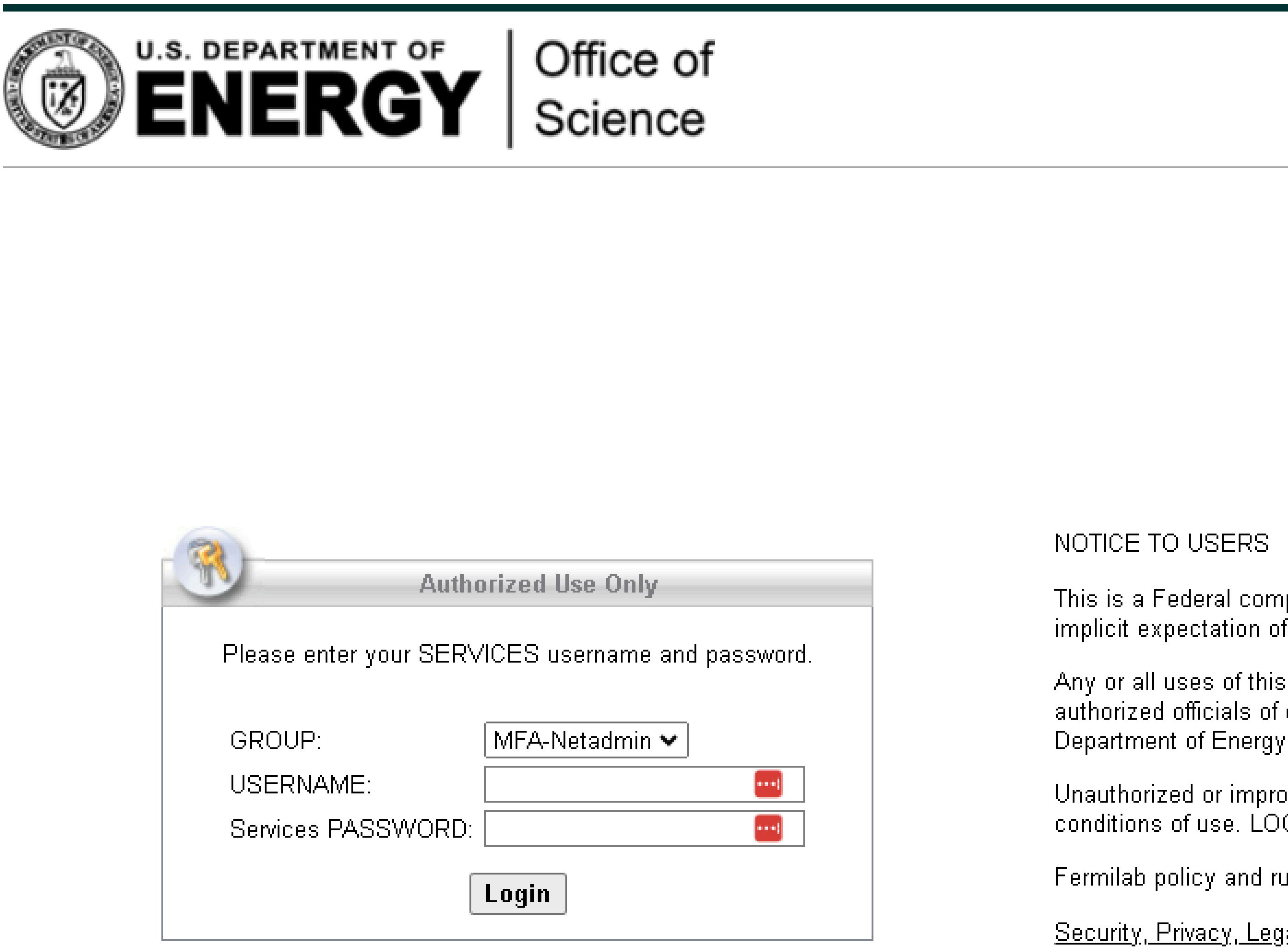
This Russian entity does not currently have valid US government TLS certificates; however, they may be staging an operation for further intrusion after obtaining certs or through other vectors of attack.

### Nuclear Risks part  2: Vulnerable Nuclear Site Logins With No Encryption, Bare IP addresses

VPN login web portals belonging to the National Nuclear Security Administration and nuclear laboratories were found accessible over plain HTTP. A simple Man-in-the-Middle attack is all that separates our nation's nuclear weapons intelligence from America's enemies.

### Key Observations:

- **Fermilab VPN Portal**: Public login page to Department of Energy's Office of Science Fermilab network management systems. https://www.shodan.io/host/131.225.251.10Hostname v-netmgr-fcc2-1-inside.fnal.gov has no public DNS records, indicating a previously internal hostname.



U.S. DEPARTMENT OF ENERGY | Office of Science

Authorized Use Only

Please enter your SERVICES username and password.

GROUP: MFA-Netadmin

USERNAME:

Services PASSWORD:

NOTICE TO USERS

This is a Federal comp
implicit expectation of

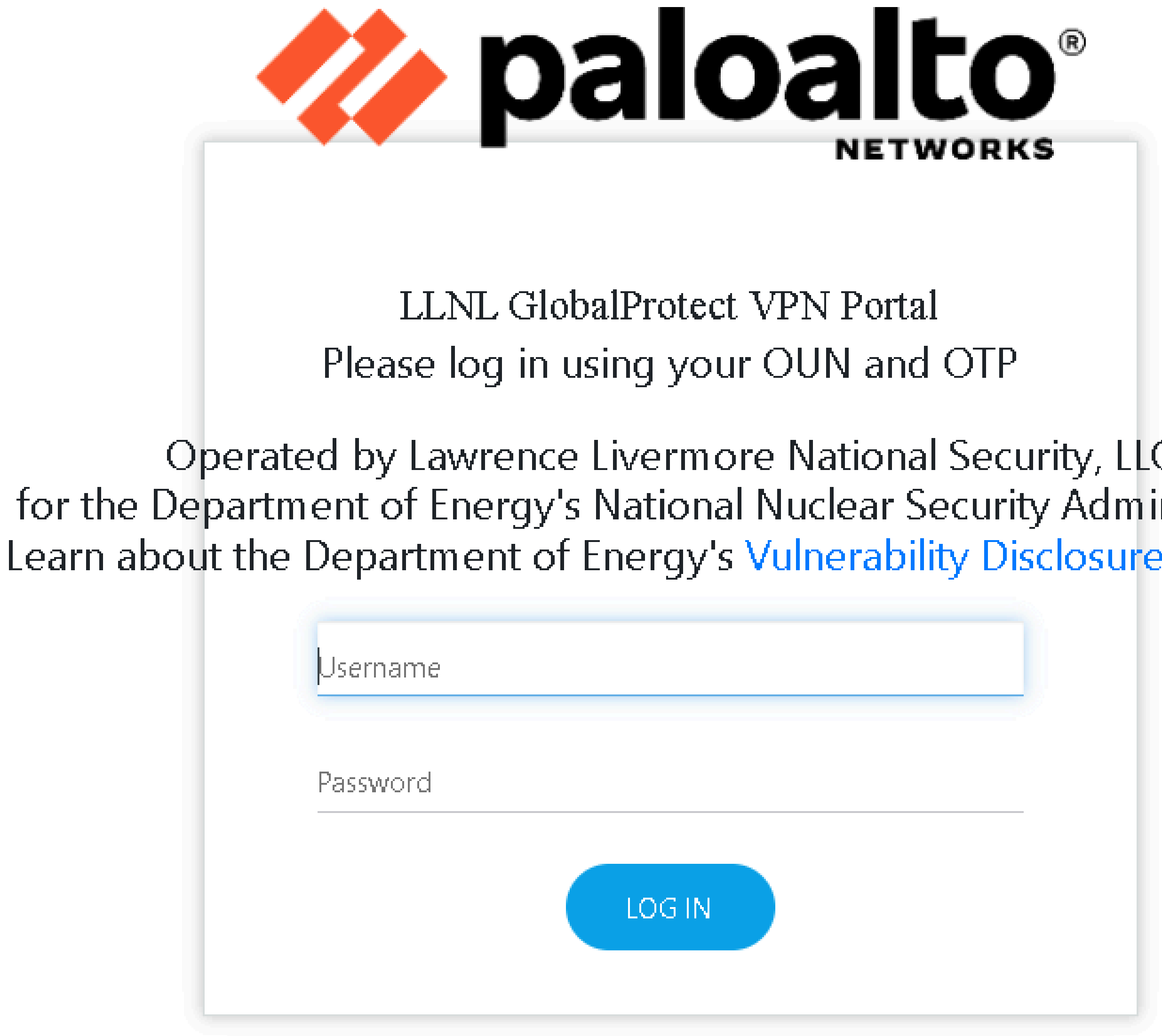
Any or all uses of this
authorized officials of
Department of Energy

Unauthorized or impro
conditions of use. LOG

Fermilab policy and ru

Security, Privacy, Leg

- **Lawrence Livermore National Lab (NNSA)**:

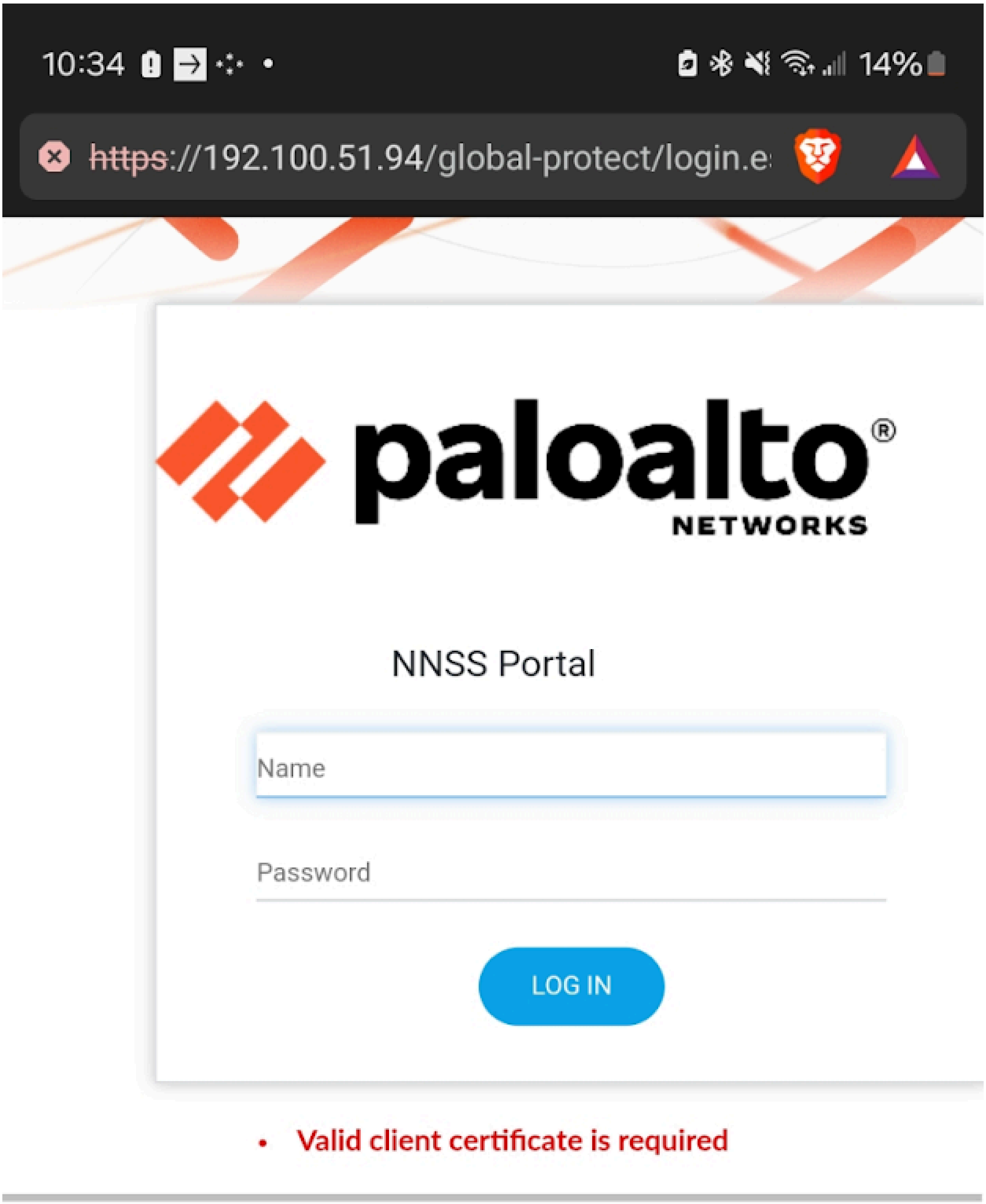


LLNL GlobalProtect VPN Portal
Please log in using your OUN and OTP

Operated by Lawrence Livermore National Security, LL
for the Department of Energy's National Nuclear Security Admi
Learn about the Department of Energy's Vulnerability Disclosure

- https://www.shodan.io/host/198.124.226.2
- GlobalProtect login exposed over plain HTTP.
- **Nevada National Security Site (NNSS)**

:



NNSS Portal

Name

Password

- Valid client certificate is required

- Password reset option available over plain HTTP, with no client-side verification that original password is correct.
- https://www.shodan.io/host/192.100.51.94

These systems are core to **nuclear material tracking**, **facility management**, and **weapons stewardship**, and their exposure means **adversaries could gain insights into operational systems or credentials**.

- Anonymous LDAP access to DOE PKI infrastructure
- https://www.shodan.io/host/205.254.131.127

LDAP (Lightweight Directory Access Protocol) services tied to **certs.energy.gov** and other .doe.gov subdomains were openly accessible on **port 389**, without encryption or authentication. This is dangerous because:

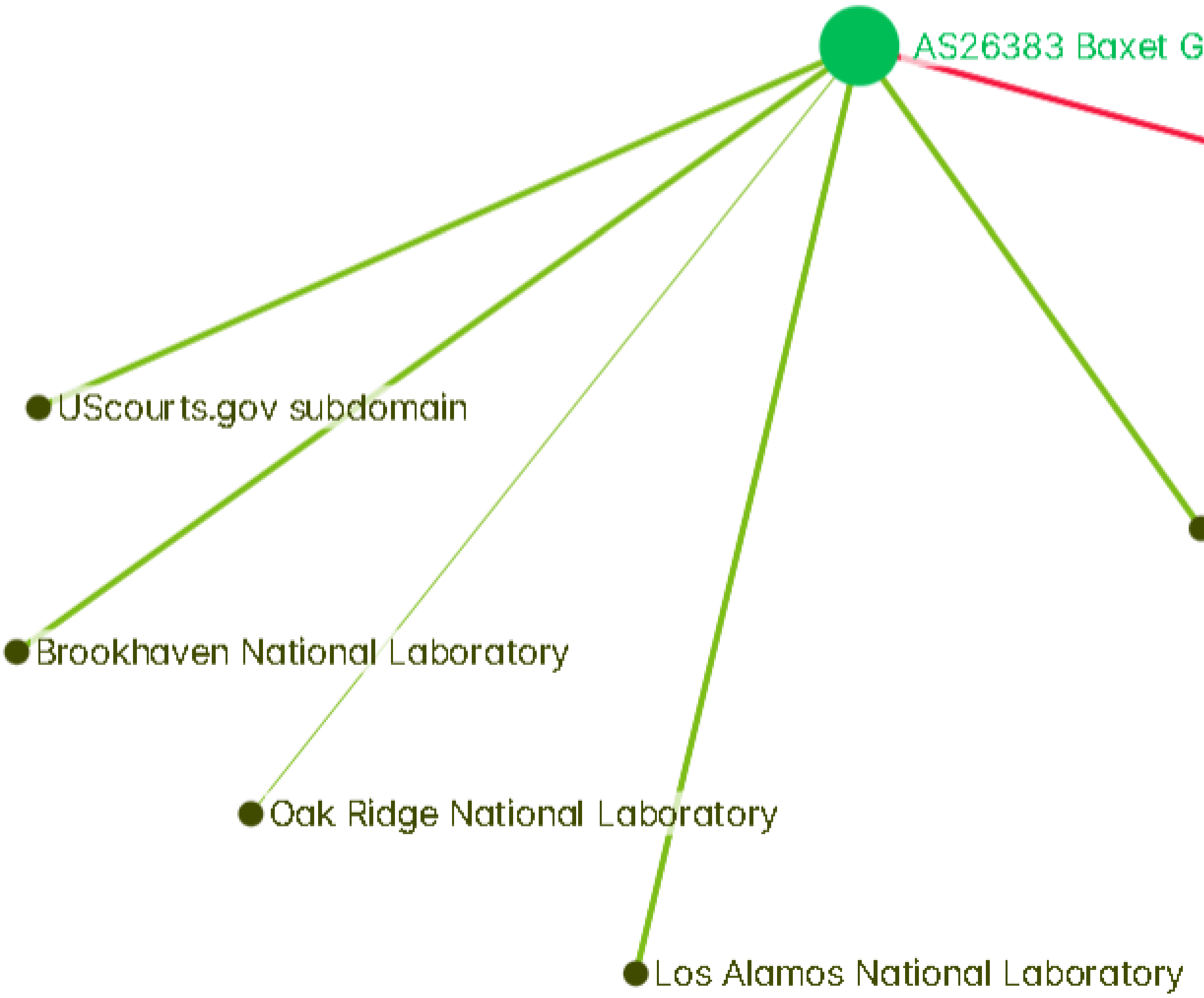
- **Anonymous Binding Enabled**: Anyone can connect and pull directory data—names, usernames, systems, departments—without credentials.
- **No TLS Encryption**: All traffic, including queries and responses, is sent in cleartext.
- **PKI Exposure Risk**: LDAP supports certificate discovery. This could be used to:
- Map the federal certificate infrastructure (PKI).
- Discover public key thumbprints.
- Support impersonation attacks if TLS certs or smartcard trust anchors are compromised.
- **Supported Controls**: Allow for paginated **directory pulls, sorting, and even unauthenticated attribute discovery.**

In short: this is like **handing out a partially redacted phonebook of a top-secret facility—only it's digital, browsable, and sometimes includes passwords**.

In summary, the exposed services' open databases, RDP/WinRM access, and disabled security controls created an environment where once the adversaries obtained some foothold or insider help, little impeded their progress. Each of these is a serious issue (rated High to Critical severity), and together they represent a systemic failure of basic security practices.

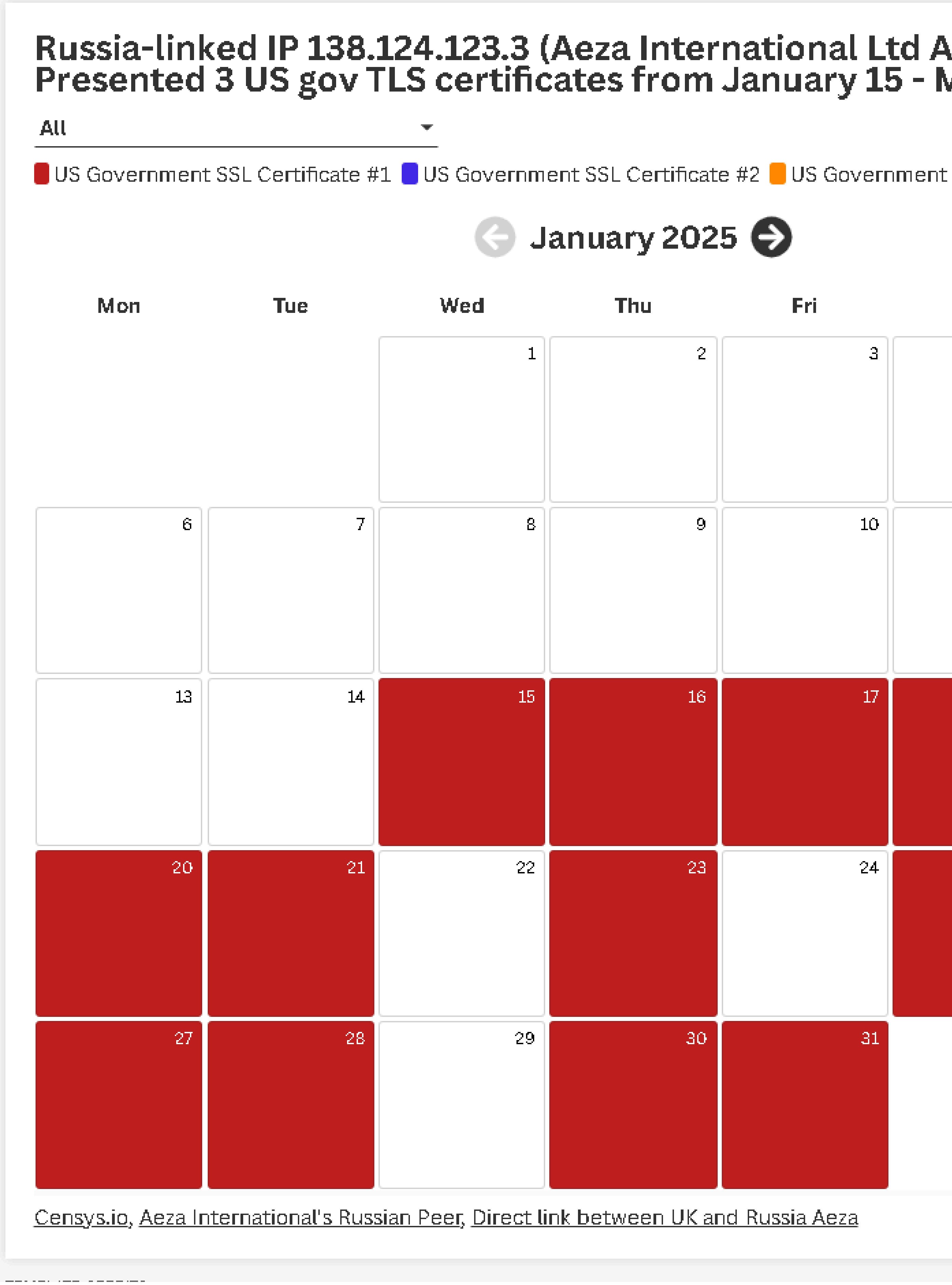
## ***Attribution - Aeza/Stark Industries (seen with real 400yaahc.gov cert) and Baxet (spoofing US gov domains without certs) are all ultimately headquartered in Russia***

5. Stark Industries and Aeza International are likely controlled by the same entity in Russia.
   A. Stark Industries and Aeza Group Limited, a now-dissolved predecessor to Aeza International LTD, are registered to the same address in the UK, **71-75 Shelton Street, Covent Garden, London**.
   B. IP address 138.124.123.3 was transferred from Stark Industries (AS44477) to Aeza International (AS210644 known to spread malware) approx. 12/21/2024. Source: **1-Russia-Aeza-3-US-Gov-Certs.xlsx**https://drive.proton.me/urls/2NRBSZS360#QPjVY41y0vL
6. Russia's LLC Baxet (AS51659) shares connection with Aeza/Stark via peer Melbikomas UAB (AS56630)


AS26383 Baxet G
UScourts.gov subdomain
Brookhaven National Laboratory
Oak Ridge National Laboratory
Los Alamos National Laboratory

View full interactive graph here:https://graphcommons.com/graphs/671b8cb6-77e7-4a6a-b18a-7f8f4e97b131

138.124.123.3 Presented 3 Unique US Gov TLS certs from Jan 15 - March 5, 2025
Interactive calendar:
https://public.flourish.studio/visualisation/22323648/



## Russia-linked IP 138.124.123.3 (Aeza International Ltd A
## Presented 3 US gov TLS certificates from January 15 - M

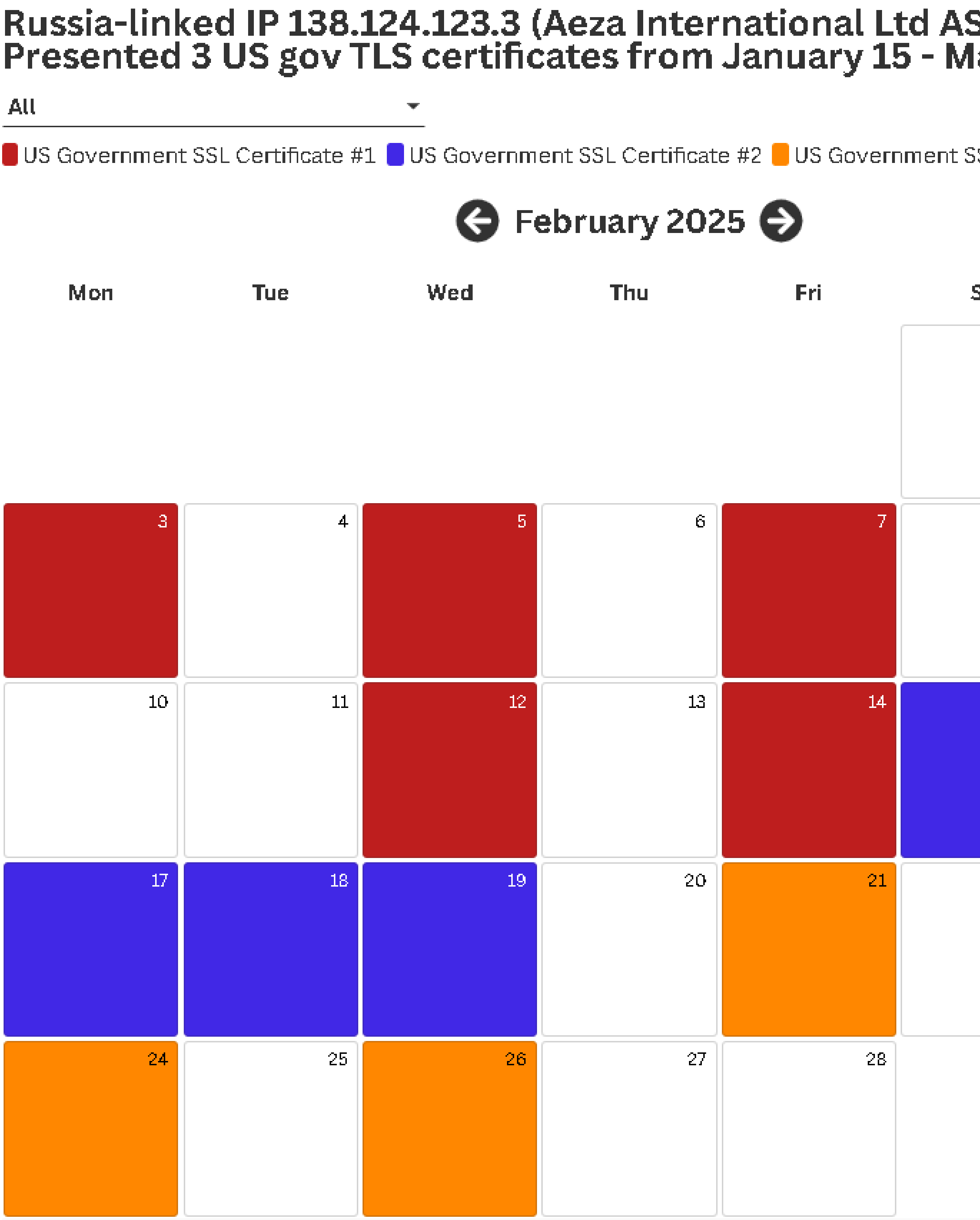
All

🟥 US Government SSL Certificate #1 🟦 US Government SSL Certificate #2 🟧 US Government

January 2025

| Mon | Tue | Wed | Thu | Fri |
|---|---|---|---|---|
|  |  | 1 | 2 | 3 |
| 6 | 7 | 8 | 9 | 10 |
| 13 | 14 | 15 🟥 | 16 🟥 | 17 🟥 |
| 20 🟥 | 21 🟥 | 22 | 23 🟥 | 24 |
| 27 🟥 | 28 🟥 | 29 | 30 🟥 | 31 🟥 |

Censys.io, Aeza International's Russian Peer, Direct link between UK and Russia Aeza



## Russia-linked IP 138.124.123.3 (Aeza International Ltd AS
## Presented 3 US gov TLS certificates from January 15 - Ma

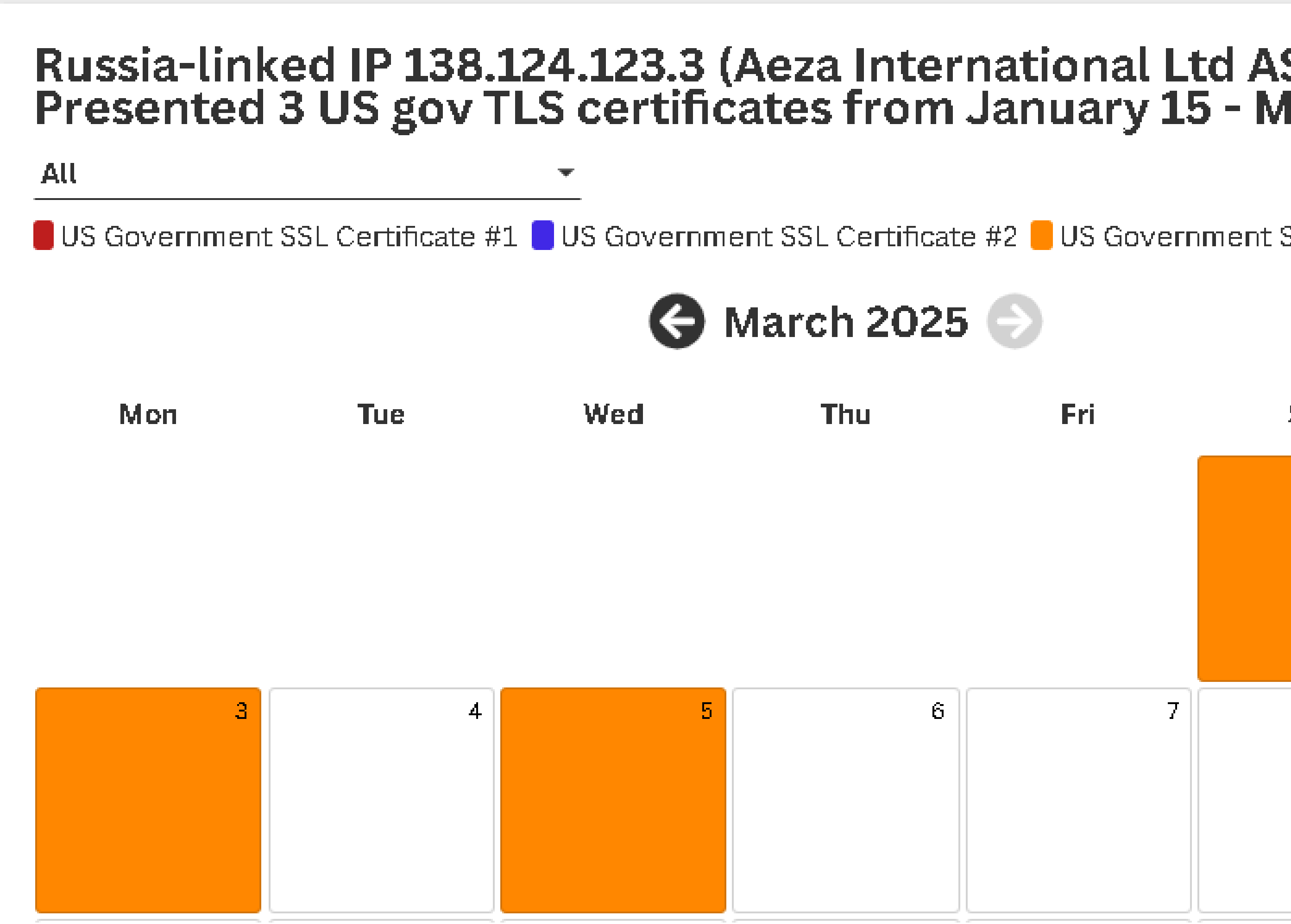
All ▾

🟥 US Government SSL Certificate #1 🟦 US Government SSL Certificate #2 🟧 US Government SS

← February 2025 →

| Mon | Tue | Wed | Thu | Fri | S |
|---|---|---|---|---|---|
| | | | | | |
| 3 🟥 | 4 | 5 🟥 | 6 | 7 🟥 | |
| 10 | 11 | 12 🟥 | 13 | 14 🟥 | 🟦 |
| 17 🟦 | 18 🟦 | 19 🟦 | 20 | 21 🟧 | |
| 24 🟧 | 25 | 26 🟧 | 27 | 28 | |

Censys.io, Aeza International's Russian Peer, Direct link between UK and Russia Aeza



## Russia-linked IP 138.124.123.3 (Aeza International Ltd AS
## Presented 3 US gov TLS certificates from January 15 - M

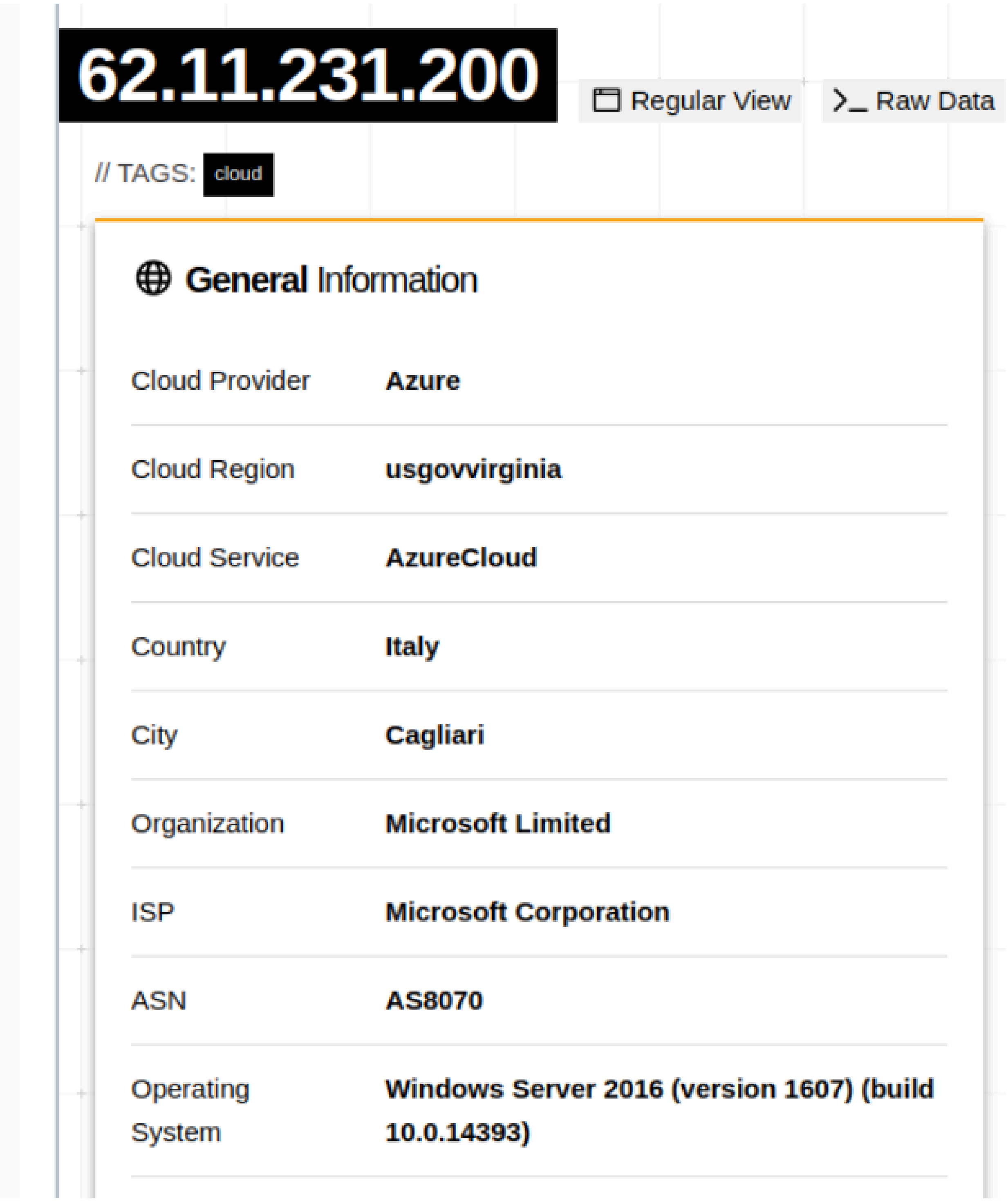
All

🟥 US Government SSL Certificate #1 🟦 US Government SSL Certificate #2 🟧 US Government S

March 2025

| Mon | Tue | Wed | Thu | Fri |
|---|---|---|---|---|
| | | | | |
| 🟧 3 | 4 | 🟧 5 | 6 | 7 |

Department of Defense / Air Force vulnerabilities
***62.11.231.200 usgovvirginia "ASGMTStage"***

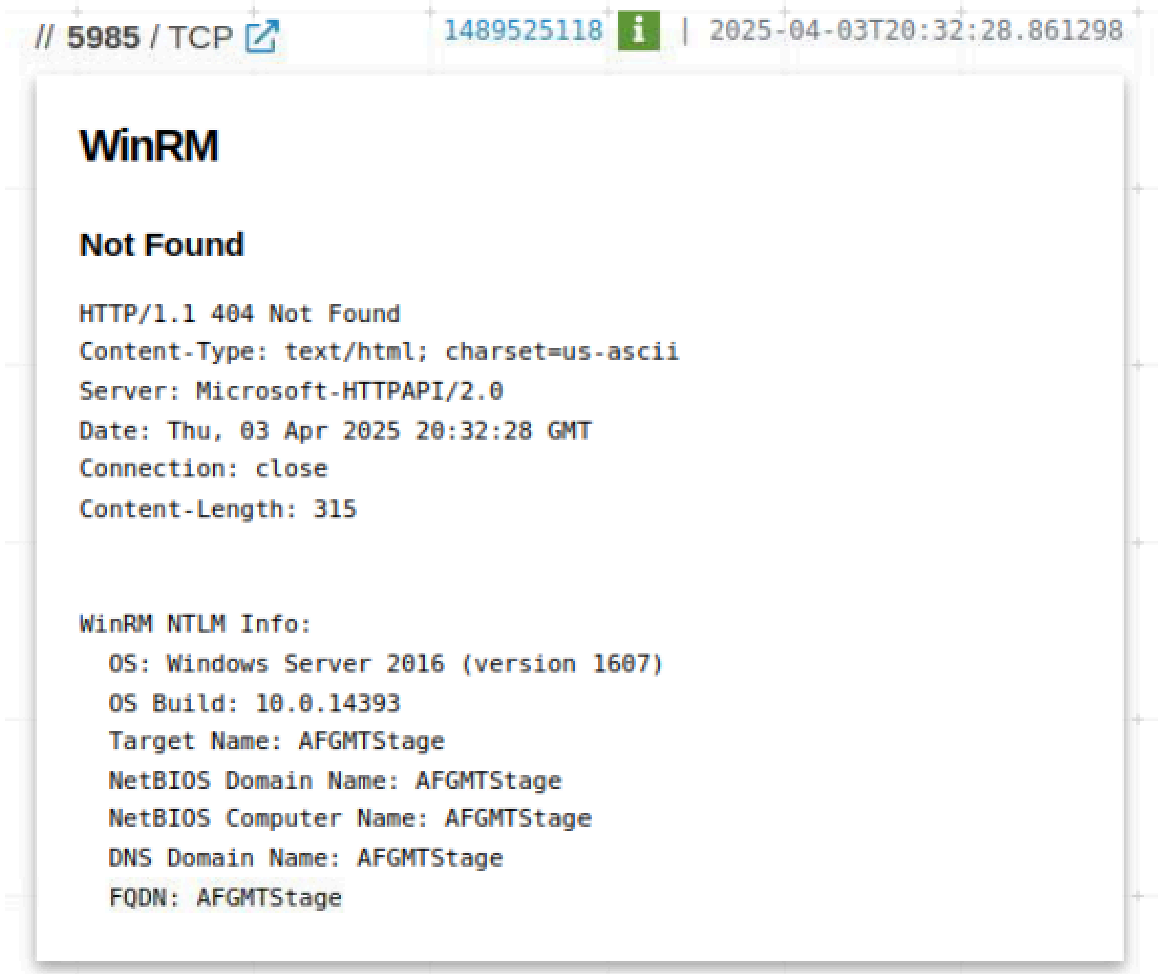


# 62.11.231.200

// TAGS: cloud

## General Information

| | |
|---|---|
| Cloud Provider | **Azure** |
| Cloud Region | **usgovvirginia** |
| Cloud Service | **AzureCloud** |
| Country | **Italy** |
| City | **Cagliari** |
| Organization | **Microsoft Limited** |
| ISP | **Microsoft Corporation** |
| ASN | **AS8070** |
| Operating System | **Windows Server 2016 (version 1607) (build 10.0.14393)** |



// **5985** / TCP

1489525118 | 2025-04-03T20:32:28.861298

**WinRM**

**Not Found**

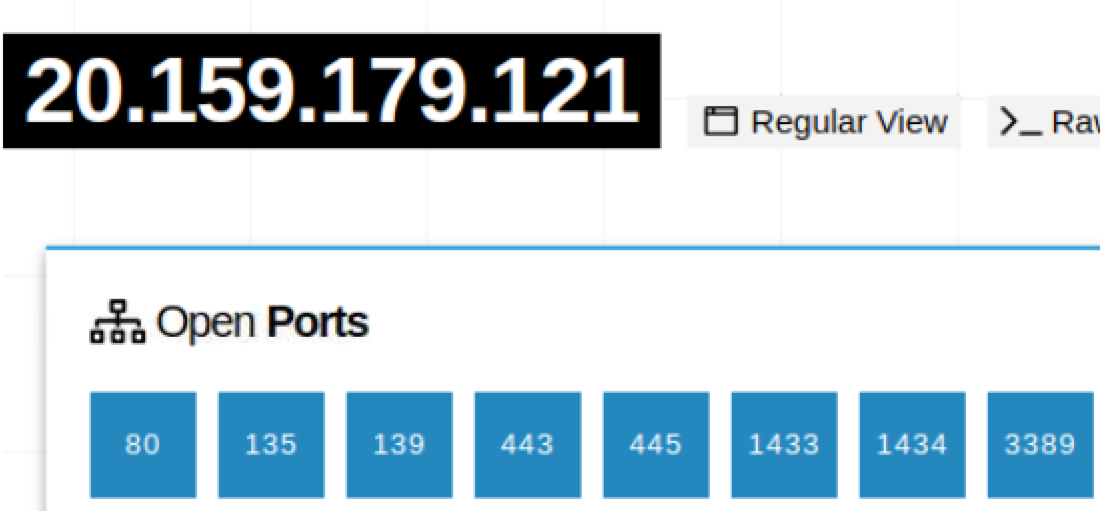
```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Thu, 03 Apr 2025 20:32:28 GMT
Connection: close
Content-Length: 315


WinRM NTLM Info:
  OS: Windows Server 2016 (version 1607)
  OS Build: 10.0.14393
  Target Name: AFGMTStage
  NetBIOS Domain Name: AFGMTStage
  NetBIOS Computer Name: AFGMTStage
  DNS Domain Name: AFGMTStage
  FQDN: AFGMTStage
```

***52.126.129.193  AFG-NE-SFTP-2***

https://www.shodan.io/host/52.126.129.193

```
WinRM NTLM Info:
  OS: Windows Server 2016 (version 1607)
  OS Build: 10.0.14393 same build as IP 62.11.231.200
  Target Name: AFG-NE-SFTP-2
  NetBIOS Domain Name: AFG-NE-SFTP-2
  NetBIOS Computer Name: AFG-NE-SFTP-2
  DNS Domain Name: AFG-NE-SFTP-2
  FQDN: AFG-NE-SFTP-2
SSL Certificate
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            57:fb:0f:84:1c:c0:bd:8b:4b:9e:4d:a2:09:1e:9b:6c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=afgnestage.usgovtexas.cloudapp.usgovcloudapi.net
        Validity
            Not Before: Jun 19 14:06:11 2024 GMT
```

**Focusing on Just One Example 20.159.179.121**



20.159.179.121

Regular View

>_ Ra

Open Ports

80 135 139 443 445 1433 1434 3389

https://www.shodan.io/host/20.159.179.121/history

IP address 20.159.179.121 belongs to the usgovvirginia region on Azure Gov Cloud. This system exposes multiple high-risk services to the internet–database, remote management, web, and RPC services, all publicly accessible and running on outdated software, makes this an extremely attractive and vulnerable target.More importantly, the server name "MCM" (Microsoft Configuration Manager) indicates that this server is likely a **central management node** that controls a fleet of government machines. If attackers compromised the control plane, they would likely obtain admin credentials, service account secrets, and the ability to push malware to all connected servers.

### 1. Port 1433/tcp – Microsoft SQL Server

- SQL Server 2016 (13.0.6455.2) – **outdated**
- Accessible over the internet — a direct entry point into backend data

### 2. Port 1434/udp – SQL Server Browser Service

- Allows SQL instance discovery — a goldmine for attackers
- Open UDP services also risk being abused in **amplification attacks**

### 3. Port 3389/tcp – Remote Desktop Protocol (RDP)

- Windows 10 / Server 2016 (Build 14393) — **unpatched, vulnerable**
- Uses NTLM authentication — **obsolete and vulnerable to relay attacks**
- Full domain info leaked:
- 081915MYAVDLAB, FQDN: **MCM**.081915MyAVDlab.com

### 4. Port 80/tcp – HTTP Web Service

- Public-facing web server— **no SSL/TLS** (plain HTTP)
- Likely hosted admin interfaces, dashboards, or apps tied to the SQL backend
- No WAF or reverse proxy observed — could expose vulnerable web apps
- Potential entry point for:
- SQL injection (if tied to DB)
- Session hijacking
- Exploits via old CMS or frameworks

### 5. Port 135/tcp – Microsoft RPC (Remote Procedure Call)

- Used for DCOM and network service binding — highly sensitive
- Frequently exploited for:
- **Lateral movement** (e.g. via SMB, WMI)
- **Privilege escalation**
- **Remote code execution (RCE)**