3/25/2025 New China w Treasury cert data and Russia-linked IP with usa.gov cert

My friend pulled ALL the data for the IPs of highest concern for the past year. So, it's a lot. But we can focus on Jan-March.

Aggregated in 90 day chunks

MEAT'S BACK ON THE MENU BOYS

Russia-Baxet-lanl-nuke-self-signed-194.58.46.116_csv
Russian (see Baxet section below) host presenting itself as a LANL SMTP server and other times hijacking cmi.ed.gov, a subdomain not used since 2020

Russia-83.149.30.186_csv
The Russian IP contacted during a Voldemort raid

China-8.219.87.97_csv
The Chinese IP observed with *.treas.gov SSL certs on Feb 11, 2025

The original evidence I saw, now gone from Censys but the above csv should capture it

first-seen-shodan	last-seen-shodan	last-seen-censys	ip	as
2025-01-18 17:22:56	2025-02-24 13:57:38	Feb 23, 2025 09:43 UTC	166.123.10.142	Treasury AS13506
2025-01-18 15:46:49	2025-02-23 23:26:21	Feb 24, 2025 02:13 UTC	164.95.10.142	Treasury AS13506
2025-01-25 8:55:47	2025-02-10 5:07:35	Feb 23, 2025 02:32 UTC	166.123.10.143	Treasury AS13506
2025-02-04 1:50:40	2025-02-23 1:11:42	Feb 24, 2025 13:40 UTC	164.95.10.143	Treasury AS13506
2025-02-18 11:12:21	**2025-02-20 22:26:18**	**Feb 23, 2025 23:20 UTC**	**8.219.87.97**	**ALIBABA-CN-NET AS45102**
2025-01-14 14:49:59	2025-01-25 8:59:07	0	8.219.87.97	ALIBABA-CN-NET AS45102
2025-01-22 0:05:15	2025-02-02 1:54:09	0	8.219.87.97	ALIBABA-CN-NET AS45102

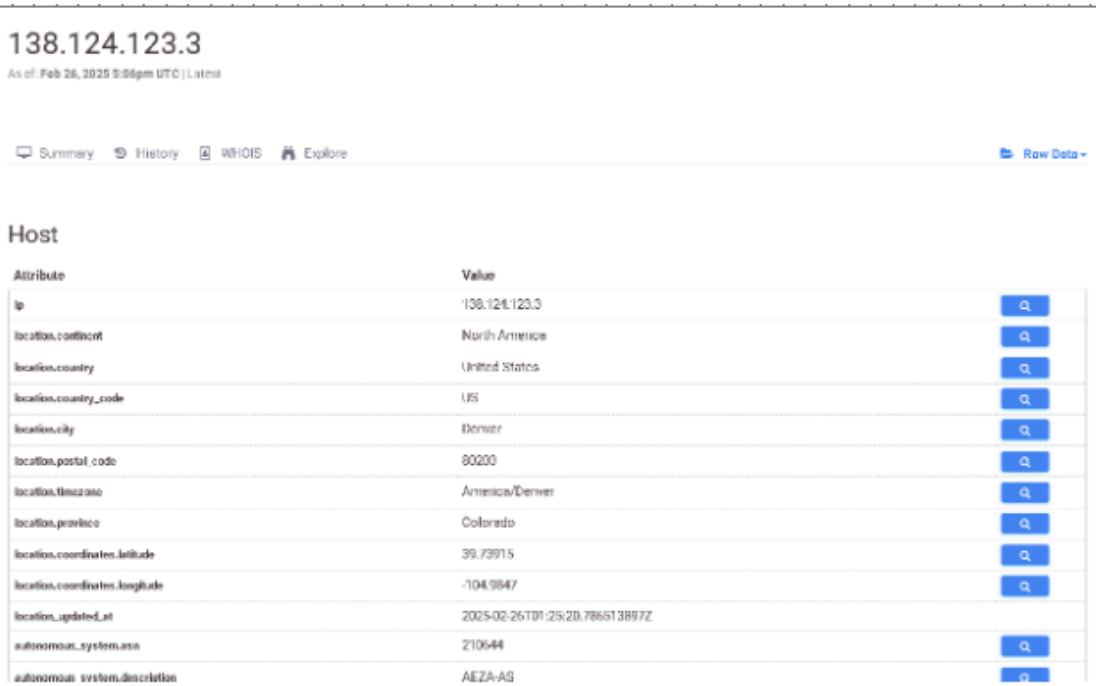
Ok I prob should've done a better job of highlighting the important bits. This was all collected from the Chinese IP's SSL certs when I saw it. We should be able to cross-reference this in above set of CSVs.

services/1/scan_time	2025-02-11T06:13:15.884Z
services/1/tls/version_selected	TLSv1_2
services/1/tls/cipher_selected	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
services/1/tls/fingerpri	**68e11f5c117a0f4b99a664a9c3485471c27f5982f849f667db11320d371bb7d4**

nt_sha256	
services/1/tls/presented_chain/0/fingerprint_sha256	13efb39a2f6654e8c67bd04f4c6d4c90cd6cab5091bcedc73787f6b77d3d3fe7
services/1/tls/presented_chain/0/subject_dn	C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2012 Entrust\, Inc. - for authorized use only, CN=Entrust Certification Authority - L1K
services/1/tls/presented_chain/0/issuer_dn	C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2009 Entrust\, Inc. - for authorized use only, CN=Entrust Root Certification Authority - G2
services/1/cert/fingerprint_sha256	68e11f5c117a0f4b99a664a9c3485471c27f5982f849f667db11320d371bb7d4
services/1/cert/fingerprint_sha1	66a024dee4beab960e4f5b11f69965a6eb5590ef
services/1/cert/fingerprint_md5	2e1a433baae63529fc1457bea668b5ba
services/1/cert/tbs_fingerprint_sha256	ce3782bdebf8f87c548b64cb2022d386b23ebcf524e62731fa808bf86bdbd48b
services/1/cert/tbs_no_ct_fingerprint_sha256	8878aa1b8ddbf72eb829e1d7be4f7e3f96c504e933144849368da024b29e4a1d
services/1/cert/spki_fingerprint_sha256	385ea6b0a62abf898e1fbf62d7f363ca1f8e5814039f143fc6ebadf15bb8a596
services/1/cert/parent_spki_fingerprint_sha256	23238969ff8cbc9948ec58ef5c81d9b81e7b060e48e7424a88bdf2f5f69602c8
services/1/cert/parsed/version	3
services/1/cert/parsed/serial_number/0	157408799883116944857734434314233964 64
services/1/cert/parsed/issuer_dn	C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2012 Entrust\, Inc. - for authorized use only, CN=Entrust Certification Authority - L1K
services/1/cert/parsed/issuer/common_name/0	Entrust Certification Authority - L1K
services/1/cert/parsed/issuer/country/0	US
services/1/cert/parsed/issuer/organization/0	Entrust, Inc.
services/1/cert/parsed/issuer/organizational_unit/0	See www.entrust.net/legal-terms
services/1/cert/parsed/issuer/organizational_unit/1	(c) 2012 Entrust, Inc. - for authorized use only
services/1/cert/parsed/subject_dn	C=US, ST=District of Columbia, L=Washington, O=United States Department of Treasury, CN=*.treasury.gov

services/1/cert/parsed/subject/common_name/0	*.treasury.gov
services/1/cert/parsed/subject/country/0	US
services/1/cert/parsed/subject/locality/0	Washington
services/1/cert/parsed/subject/province/0	District of Columbia
services/1/cert/parsed/subject/organization/0	United States Department of Treasury
services/1/cert/parsed/subject_key_info/key_algorithm/name	RSA
services/1/cert/parsed/subject_key_info/key_algorithm/oid	1.2.840.113549.1.1.1
services/1/cert/parsed/subject_key_info/rsa/exponent	65537
services/1/cert/parsed/subject_key_info/rsa/modulus	d78dcd9f15fc8917a0883cf1a46539d911cc2c351b5483a104e862e6c20c4fa34dcff93ccd7b828bcb294813f46915df136e84bfebbf1d4de792b9c3bee0ca5d65455d26048efed590798c129e4439d247f27bcc8b2a1ef132e8da2b291df76cb5237f35c3a36f473f725e3074c0918a746c5ab6c037c68d9482531f6bb68260779b1cf7d0b29247118c60d6bd7dfaf2d1d2f155ff21272267e4ad516a22d21e406125321a2267c32db3c6c62a08cd7e2e043662e2ea5832f2d2155599fbeac119a23c7c36d82eb35bb303fcb582ba930a8772ad6fc56360b08edb35edb3b59f2254bb69e496fa05b4ab46668b1b11f6b20ce17eaeddd2d14223e6944a8455db
services/1/cert/parsed/subject_key_info/rsa/length	2048
services/1/cert/parsed/subject_key_info/fingerprint_sha256	91abc3a1ee6c66e428f5d170a40f82a5e449e5867059718341858508473333e3b
services/1/cert/parsed/validity_period/not_before	2024-10-04T10:11:49.000Z
services/1/cert/parsed/validity_period/not_after	2025-11-03T10:11:48.000Z
services/1/cert/parsed/validity_period/length_seconds	34127999

Russia 138.124.123.3 with usa.gov fedidcard.gov and more cert



138.124.123.3

As of: Feb 26, 2025 5:06pm UTC | Latest

Summary History WHOIS Explore Raw Data

Host

Attribute	Value
ip	138.124.123.3
location.continent	North America
location.country	United States
location.country_code	US
location.city	Denver
location.postal_code	80203
location.timezone	America/Denver
location.province	Colorado
location.coordinates.latitude	39.73915
location.coordinates.longitude	-104.9847
location_updated_at	2025-02-26T01:25:20.786513897Z
autonomous_system.asn	210644
autonomous_system.description	AEZA-AS

TLS

Handshake

Version Selected TLSv1_3

Cipher Selected TLS_AES_256_GCM_SHA384

Certificate

Fingerprint 95e04bc4a9ab640d5e85a21f00053375246aad4619493de092c98af09f56f9c

Subject CN=400yaahc.gov

Issuer C=US, O=Let's Encrypt, CN=R10

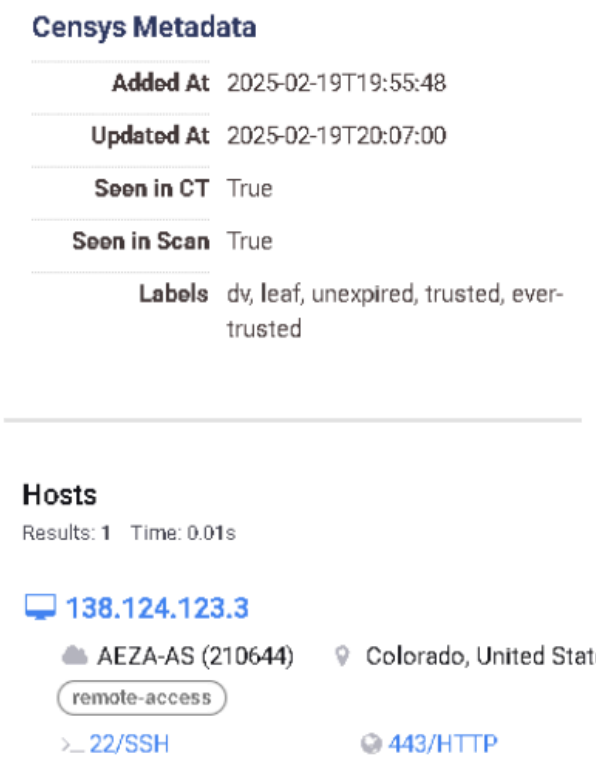
Names 400yaahc.gov, consumeraction.gov, fedidcard.gov, firstgov.gov, forms.gov, fpisc.gov, gobiernousa.gov, gsa.gov, info.gov, kids.gov, m.gsa.gov, pbrb.gov, permitting.gov, us.gov, usa.gov, usagov.gov, workplace.gsa.gov, www.fedidcard.gov

Fingerprint

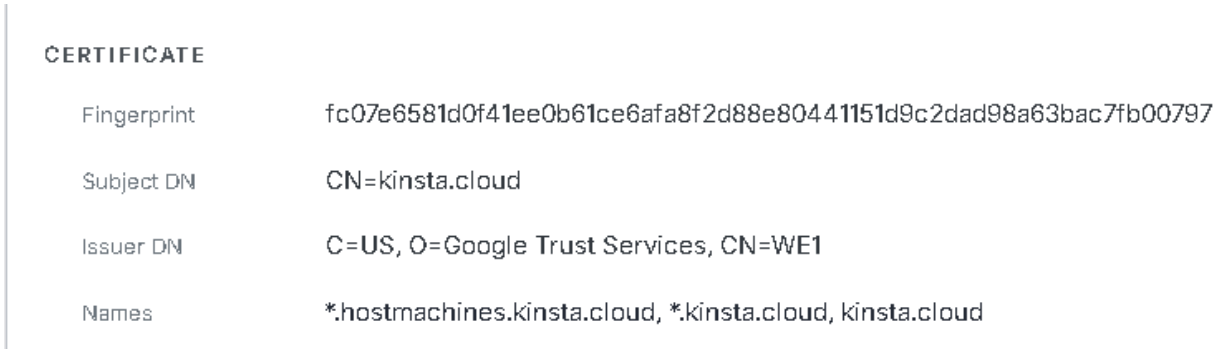
JARM 14d14d00014d14d00042d42d0000008eafd3f5048d753a6a294a6ae97b840d

JA3S 15af977ce25de452b96affa2addb1036

JA4S t130200_1302_a56c5b993250



https://crt.sh/?id=16738559834
It's not on Censys anymore bearing the gov cert, but now it has a kinsta.cloud C



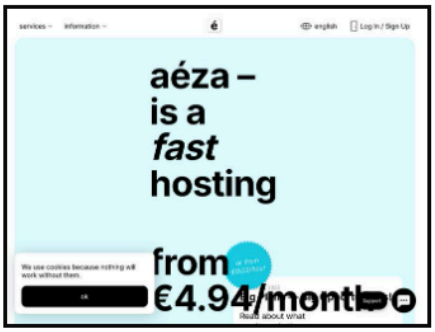
Maybe coincidence but DOGE also used kinsta to develop doge.gov before it went live

While Aeza International Limited AS210644 is technically registered in the UK, it has Aeza Group LLC (Russia) as its upstream and they have the same exact website design

	AS216246	Aeza Group LLC
	AS210644	Aéza International Limited

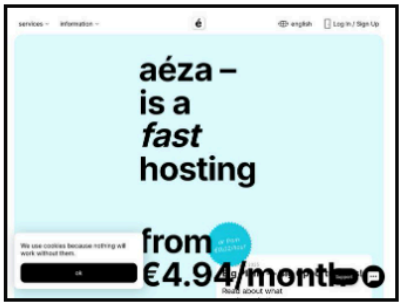
Aéza International Limited

AS Number **210644**
Website **https://aeza.net**



Aeza Group LLC

AS Number **216246**
Website **http://aeza.net**

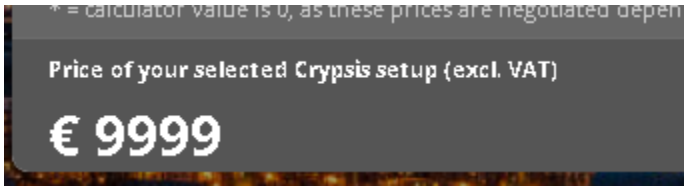


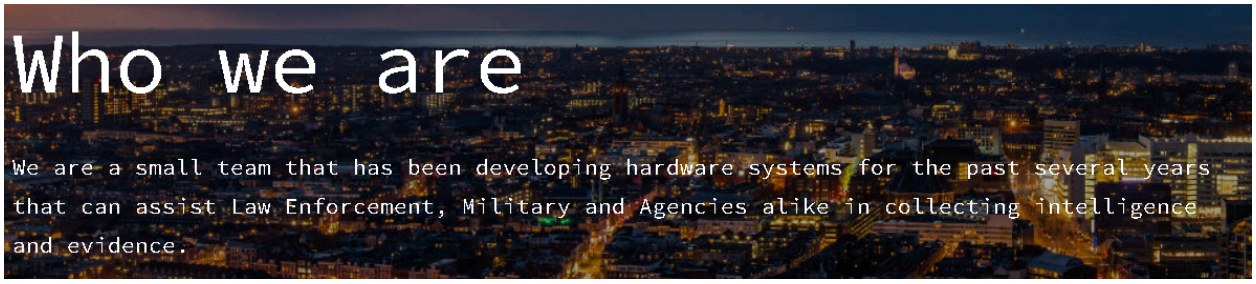
And when you take a look at a random TOR relay hosted by Aeza AS210644, they all seem to be in Russia
https://nusenu.github.io/OrNetStats/w/as_number/AS210644.html
https://bgp.tools/prefix/77.221.156.0/23#dns

Nickname	Authenticated Relay Operator ID or ContactInfo (unverified)	Bandwidth	IP Address	AS Name	Country	Flags	First Seen
cozybeardev (31)	email:tor[]shadowbrokers...	293 Mbit/s	77.221.157.237	AEZA INTERNATIONAL LTD			2024-05-04
cozybeardev (31)	shadowbrokers.eu	288 Mbit/s	79.137.202.92	AEZA INTERNATIONAL LTD			2023-02-17
cozybeardev (31)	shadowbrokers.eu	261 Mbit/s	79.137.198.213	AEZA INTERNATIONAL LTD			2023-05-18
prsv (274)	email:admin[]prsv.ch...	257 Mbit/s	138.124.93.159	AEZA INTERNATIONAL LTD			2025-02-09
cozybeardev (31)	email:tor[]shadowbrokers...	239 Mbit/s	77.221.152.105	AEZA INTERNATIONAL LTD			2024-07-24
cozybeardev (31)	shadowbrokers.eu	229 Mbit/s	94.228.169.70	AEZA INTERNATIONAL LTD			2023-06-15

I've looked into this guy cozybeardev, he's either a) a crypto hacker bro who tried to market a custom keylogger and remote access hacking device to intelligence and gave up, or b) Russian intel took him off the market and he's paid handsomely to do spy stuff in Europe and his TOR relay family ranks in the top 50 or so in the world for bandwidth, while operating 4 exit nodes in Russia.

This isn't about him necessarily but thought I would slake your curiosity so we don't get distracted.





https://web.archive.org/web/20230411113006/https://menura.org/#whoweare
https://web.archive.org/web/20230411113006/http://www.menura.org/#crypsis
https://github.com/RedBulletTooling/KEYVILBOARD

Motivation

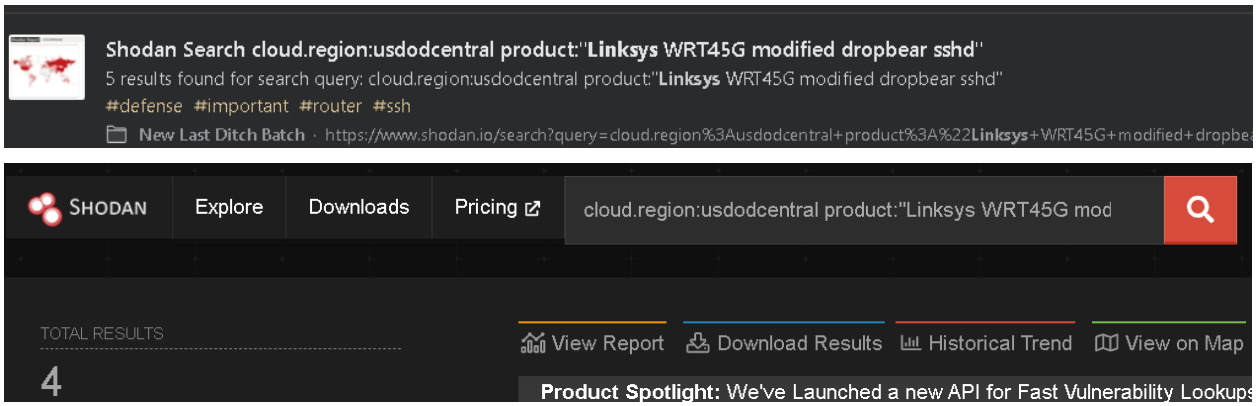
We would hate to see the knowledge that we build up gone to waste, given we decided to halt this product. This product has not been as commercially viable as we had hoped. But we have put time, effort and a decent chunk of money into this project to create something that hasn't been replicated since. Our goal with publicizing this project is that goal of it's creation will be reached. To prevent harms to those who can't protect themselves. May that be terrorism, child exploitation or other crimes. If you work for an organisation that has these same goals and have a need, contact us. We are happy to help.

What is Crypsis

Crypsis is a hardware keylogger that communicates using a NFR9160 module. By doing so we can do very advanced methods of communicating covertly, aswell as propper implementation of encryption and other security measures. Apart from the hardware the server is dockerized, meaning it's modular and highly adjustable.

3/24/2025 findings
https://www.shodan.io/search?query=cloud.region%3Ausgovvirginia+product%3A%22Kubernetes%22

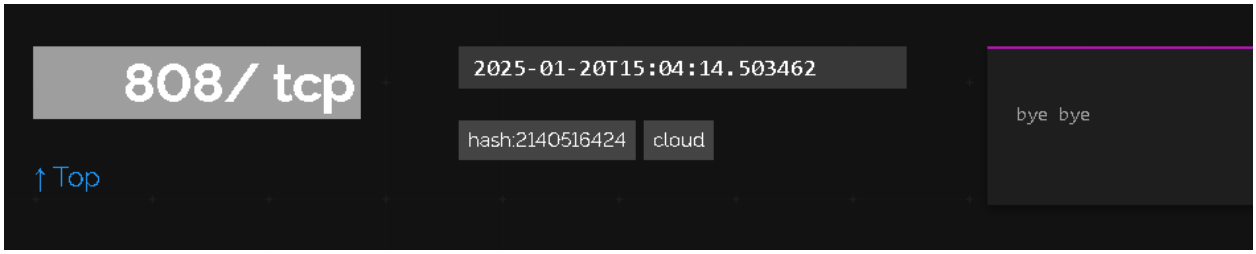
USDOD
usdodcentral



Linksys Router with port 22
https://www.shodan.io/search?query=cloud.region%3Ausdodcentral+product%3A%22Linksys+WRT45G+modified+dropbear+sshd%22

52.182.53.254
52.182.95.249
52.182.49.190
52.182.49.155

This 52.182.49.155 is particularly interesting…On 1/20, it had a custom message in its response header on port 808. Custom firmware?

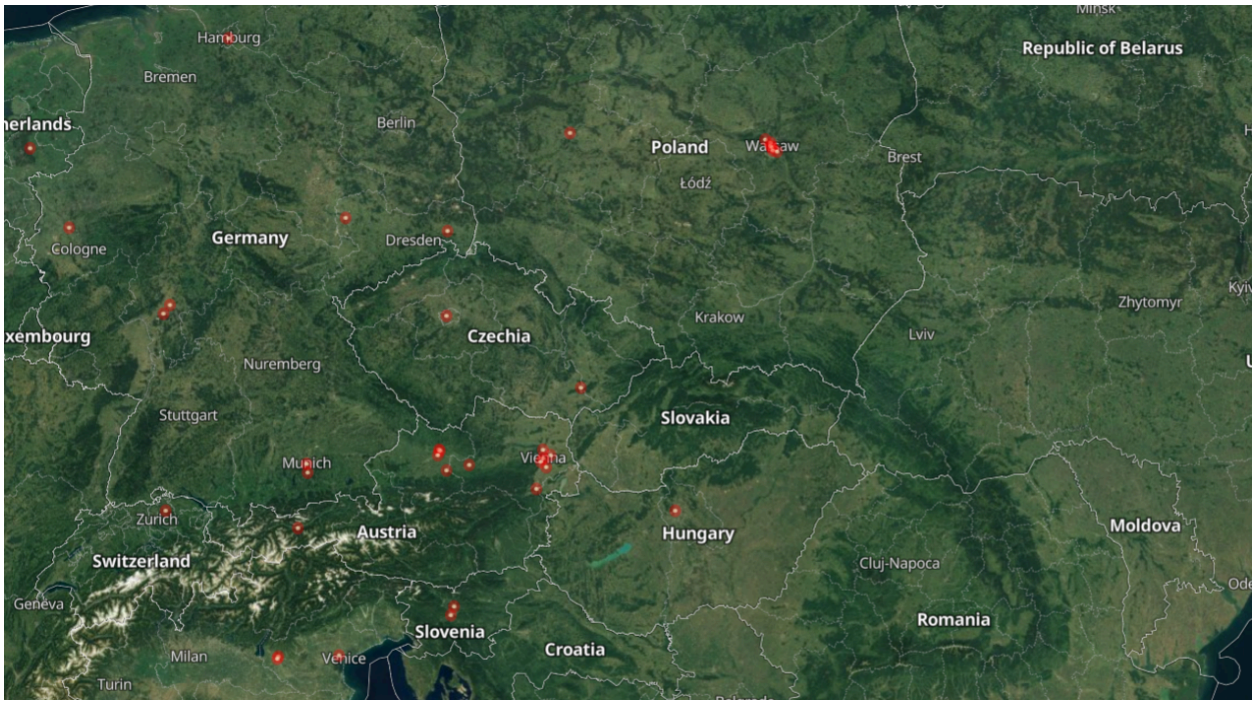


usdodeast

https://www.shodan.io/search?query=cloud.region%3Ausdodeast+product%3A%22Linksys+WRT45G+modified+dropbear+sshd%22

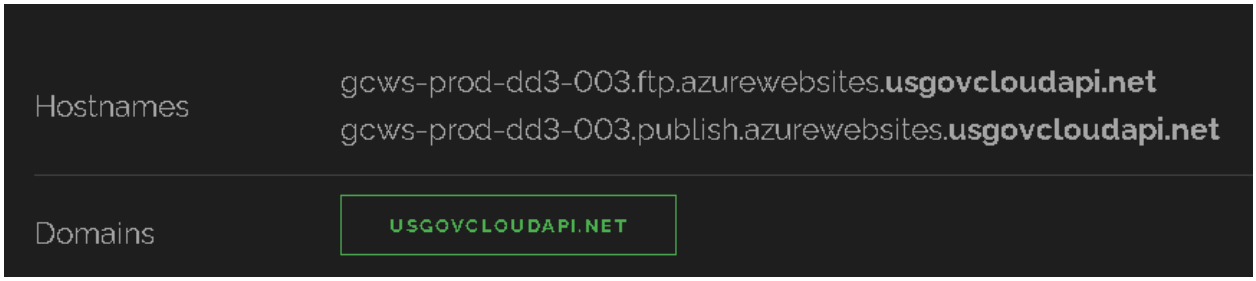
52.181.166.132
Same message on 2/10

So, when we pivot to that hash to find other devices with bye bye on port 808, we get a fair amount in east Europe/Balkans



Bye Bye
https://maps.shodan.io/#46.06520124147803/36.13990730778441/4/satellite/hash:2140516424

Usdodcentral FTP
https://www.shodan.io/search?query=cloud.region%3Ausdodcentral+product%3A%22Microsoft+ftpd%22
An example:
https://www.shodan.io/host/52.182.49.24



IIS port 443 first seen 1/29

FTP
2025-03-10T20:48:27.472091
2025-03-06T03:58:27.985768
2025-01-27T01:20:52.367332
2025-01-15T19:50:43.879138

More PostgreSQL database endpoints identified–usgovarizona

https://docs.google.com/spreadsheets/d/1omvkU9ZjT-Qty7hgWwSWwuv8wMl8VYyWXJhr95MaibQ/edit?usp=sharing

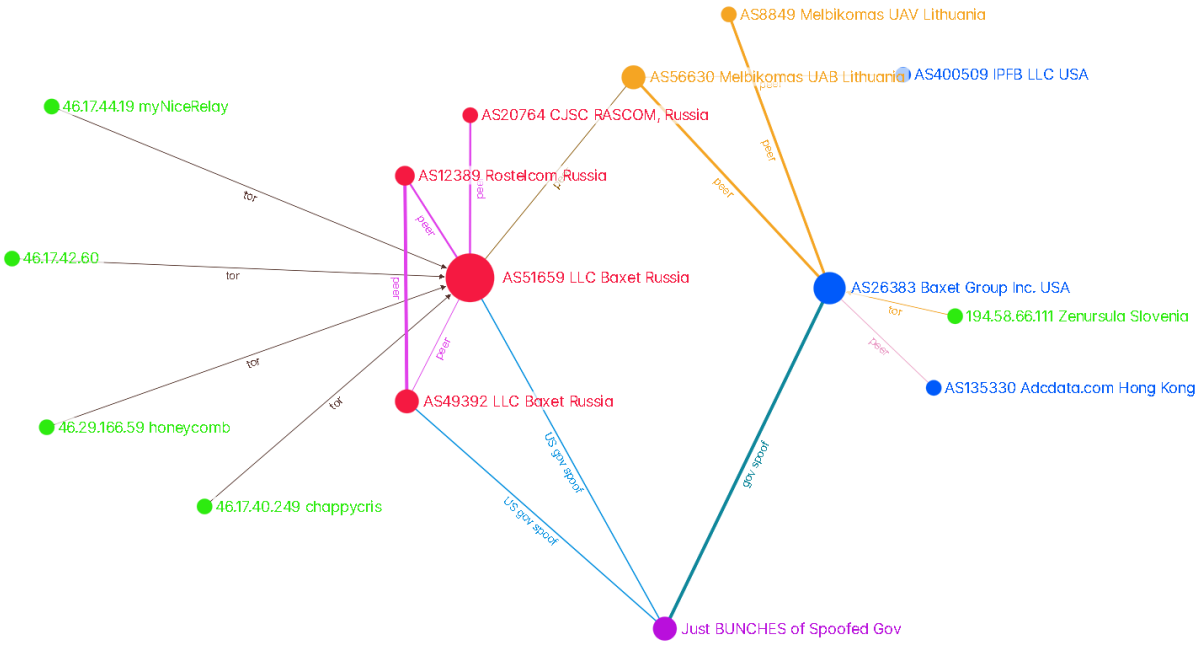
Baxet Russia masquerading as various US gov servers

High level overview of connections between Russian and US (with Euro IP ranges) “Baxet” ASNs

Snapshot of nuclear or dhs related spoofed sites/mail servers

timestamp - Mon	ip_str	port	asn	hostnames
Jan	166.1.22.248	22	AS26383	icons.ornl.gov
Feb	166.1.22.248	22	AS26383	icons.ornl.gov
		80	AS26383	icons.ornl.gov, icons.ornl.gov
		111	AS26383	icons.ornl.gov
		8181	AS26383	icons.ornl.gov
				icons.ornl.gov, icons.ornl.gov
	194.58.46.11(	22	AS26383	dx10.lanl.gov, cmi.ed.gov
				dx10.lanl.gov, cmi.ed.gov, cmi.ed.gov
				dx10.lanl.gov, cmi.ed.gov, dx10.lanl.gov
		25	AS26383	dx10.lanl.gov, cmi.ed.gov, dx10.lanl.gov
		80	AS26383	dx10.lanl.gov, cmi.ed.gov
				dx10.lanl.gov, cmi.ed.gov, dx10.lanl.gov
		111	AS26383	dx10.lanl.gov, cmi.ed.gov, cmi.ed.gov
				dx10.lanl.gov, cmi.ed.gov, dx10.lanl.gov
		1234	AS26383	dx10.lanl.gov, cmi.ed.gov, dx10.lanl.gov
		8181	AS26383	dx10.lanl.gov, cmi.ed.gov, dx10.lanl.gov
	194.87.82.24(	25	AS26383	yahoo.com, ca.my.yahoo.com, hk.rd.yahoo.com, sevp.ice.dhs.gov, ddl.f
Mar	166.1.22.248	22	AS26383	icons.ornl.gov
	194.58.46.11(	22	AS26383	dx10.lanl.gov, cmi.ed.gov
				dx10.lanl.gov, cmi.ed.gov, cmi.ed.gov
		111	AS26383	dx10.lanl.gov, cmi.ed.gov, cmi.ed.gov
	194.87.82.24(	22	AS26383	yahoo.com, ca.my.yahoo.com, hk.rd.yahoo.com, sevp.ice.dhs.gov, ddl.f

https://graphcommons.com/graphs/8d13c71f-7288-46b6-a65c-f1b8af07223f



Query: org:"LLC Baxet" hostname:gov
Covering ASNs AS51659 and AS49392
https://www.shodan.io/search?query=org%3A%22LLC+Baxet%22+hostname%3Agov

Spreadsheet of past 90 days for this query
https://drive.proton.me/urls/DK95YFNM1W#FmLisaIXpXO2

Query: asn:AS26383 hostname:gov
Registered in Delaware, USA
https://www.shodan.io/search?query=asn%3AAS26383+hostname%3Agov

Spreadsheet
https://drive.proton.me/urls/C0ZFJSY2A0#lEJ8Cc0j2zIe

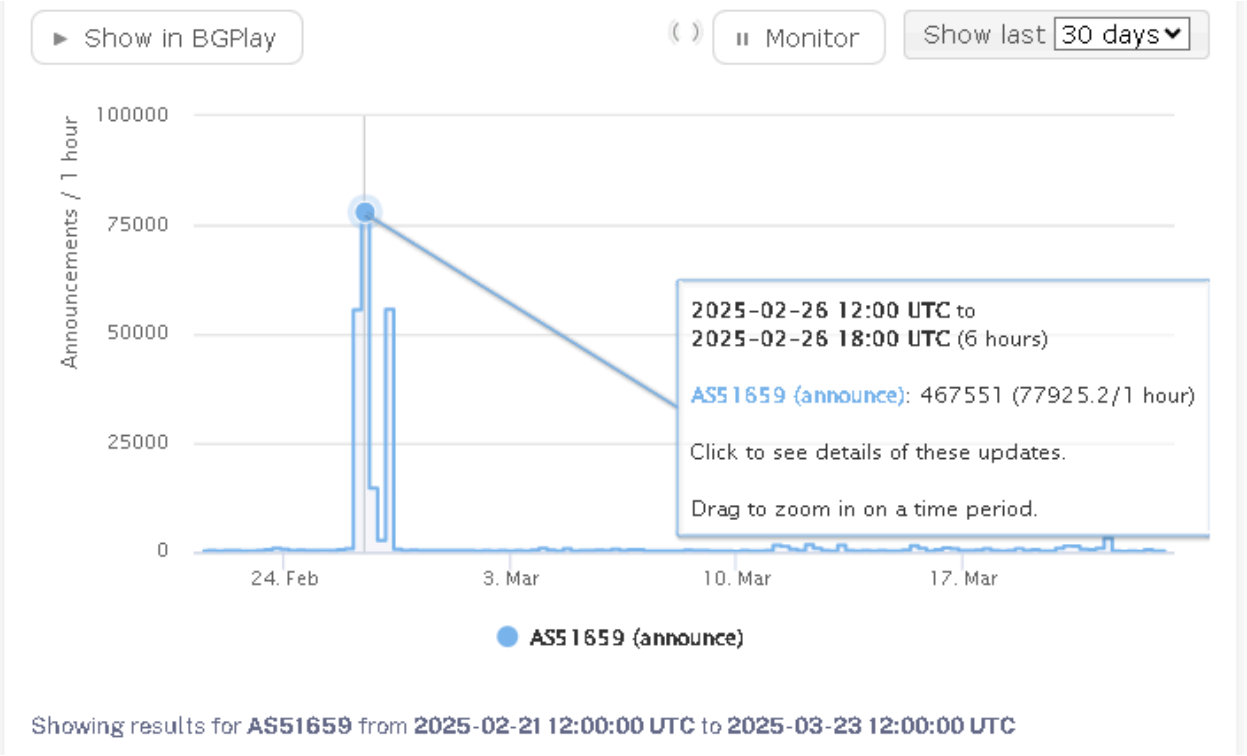
AS51659 LLC Baxet Russia
https://bgp.he.net/AS51659#_peers

Peers with
AS49392 LLC Baxet Russia
https://bgp.he.net/AS49392#_peers

AS26383 Baxet Group Inc. and also without a . USA
https://bgp.he.net/AS26383#_peers
https://opencorporates.com/companies/us_de/7627330

BAXET GROUP INC.

Company Number	7627330
Incorporation Date	26 September 2019 (over 5 years ago)
Company Type	Domestic Corporation
Jurisdiction	Delaware (US)
Registered Address	New Castle, DE United States
Agent Name	INCORP SERVICES, INC
Agent Address	919 NORTH MARKET STREET, SUITE 950 - WILMINGTON DE 19801
Directors / Officers	INCORP SERVICES, INC, agent



Tor relays

Home :: AS51659

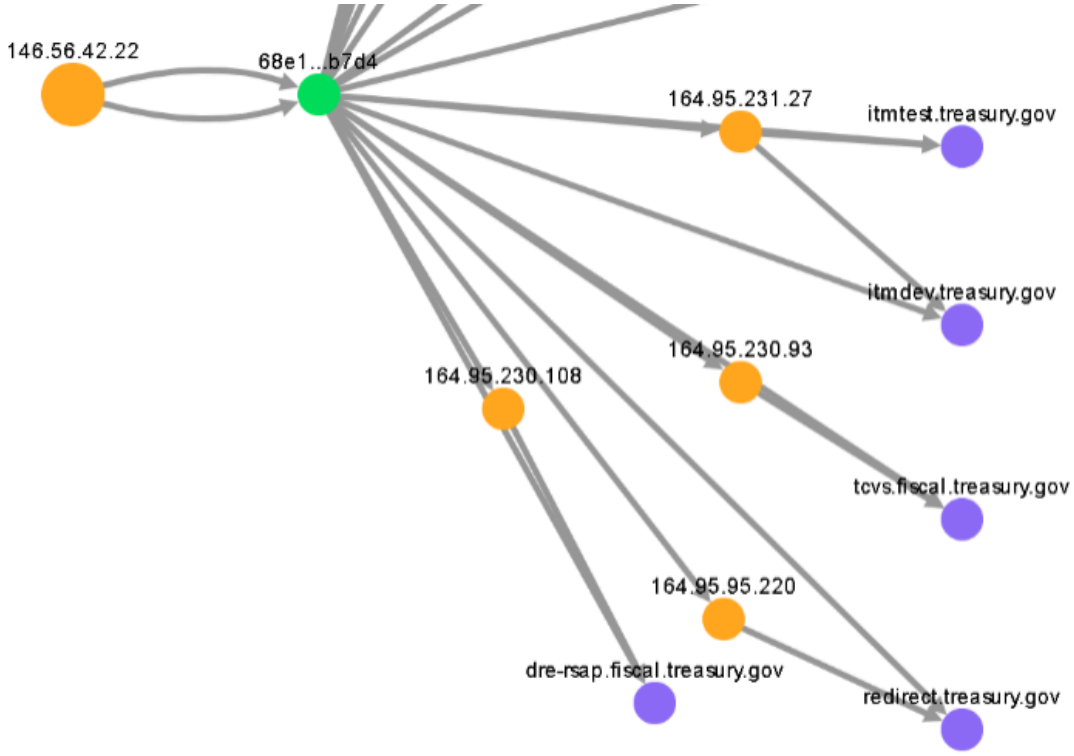
AS51659 (LLC Baxet)is responsible for ~544 Mbit/s of traffic, with 10 middle relays.

Nickname	Authenticated Relay Operator ID or ContactInfo (unverified)	Bandwidth	IP Address	AS Name	Country	Flags	First Seen
myNiceRelay (2)	volunteerhappy@firemail.de	85 Mbit/s	46.17.44.19	LLC Baxet			2024-12-09
chappycris (2)	barongarrison@firemail.de	69 Mbit/s	46.17.40.249	LLC Baxet			2025-01-29
chappycris (2)	barongarrison@firemail.de	68 Mbit/s	46.17.40.249	LLC Baxet			2025-01-29
honeycomb (2)	azaleawindsurf@firemail.de	65 Mbit/s	46.29.166.59	LLC Baxet			2025-02-18
hawk (2)	katerinagrow@firemail.de	63 Mbit/s	46.17.42.60	LLC Baxet			2025-01-14
honeycomb (2)	azaleawindsurf@firemail.de	55 Mbit/s	46.29.166.59	LLC Baxet			2024-11-12
hawk (2)	katerinagrow@firemail.de	51 Mbit/s	46.17.42.60	LLC Baxet			2025-01-14
Zensursula (23)	cp_tor [] mailfence dot com	51 Mbit/s	194.87.69.60	LLC Baxet			2024-01-27
myNiceRelay (2)	volunteerhappy@firemail.de	38 Mbit/s	46.17.44.19	LLC Baxet			2025-03-11
cc	none	0 Mbit/s	195.133.5.179	LLC Baxet			2025-03-21

Treasury IPs with same cert that Chinese alibaba ip had

Spreadsheet here
Sorry I had trouble pulling the actual certs but I searched by fingerprint
https://drive.proton.me/urls/3TAZEKZQ7M#8p85hIijq0h4

First, the Chinese IP is gone and replaced with two South Korean hosts
146.56.42.22



152.67.204.133

Fingerprint 68e11f5c117a0f4b99a664a9c3485471c27f5982f849f667db11320d371bb7d4

*.treasury.gov

Certificate | Trust | ZLint | PEM

Basic Information

Subject DN	C=US, ST=District of Columbia, L=Washington, O=United States Department of Treasury, CN=*.treasury.gov
Issuer DN	C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2012 Entrust\, Inc. - for authorized use only, CN=Entrust Certification Authority - L1K
Serial Number	Decimal: 157408799883116944857734434314233964 64 Hex: 0xbd7954d62875cd032f34d61550dca70
Validity Period	2024-10-04T10:11:49 **to** 2025-11-03T10:11:48 (394 days, 23:59:59)
All Names	*.bpd.treas.gov *.fiscal.treasury.gov *.fms.treas.gov *.publicdebt.treas.gov *.treas.gov *.treasury.gov treas.gov treasury.gov
Labels	ov, leaf, trusted, unexpired, ever-trusted,

Fingerprint

SHA-256	68e11f5c117a0f4b99a664a9c3485471c27f5982f849f667db11320d371bb7d4
SHA-1	66a024dee4beab960e4f5b11f69965a6eb5590ef
MD5	2e1a433baae63529fc1457bea668b5ba

Censys Metadata

Added At	2024-10-23T02:44:43
Updated At	2025-03-12T18:19:38
Seen in CT	True
Seen in Scan	True
Labels	ov, leaf, trusted, unexpired, ever-trusted

When I Censys search for “same key and subject” it shows another more recent cert, with no known hosts associated at this time

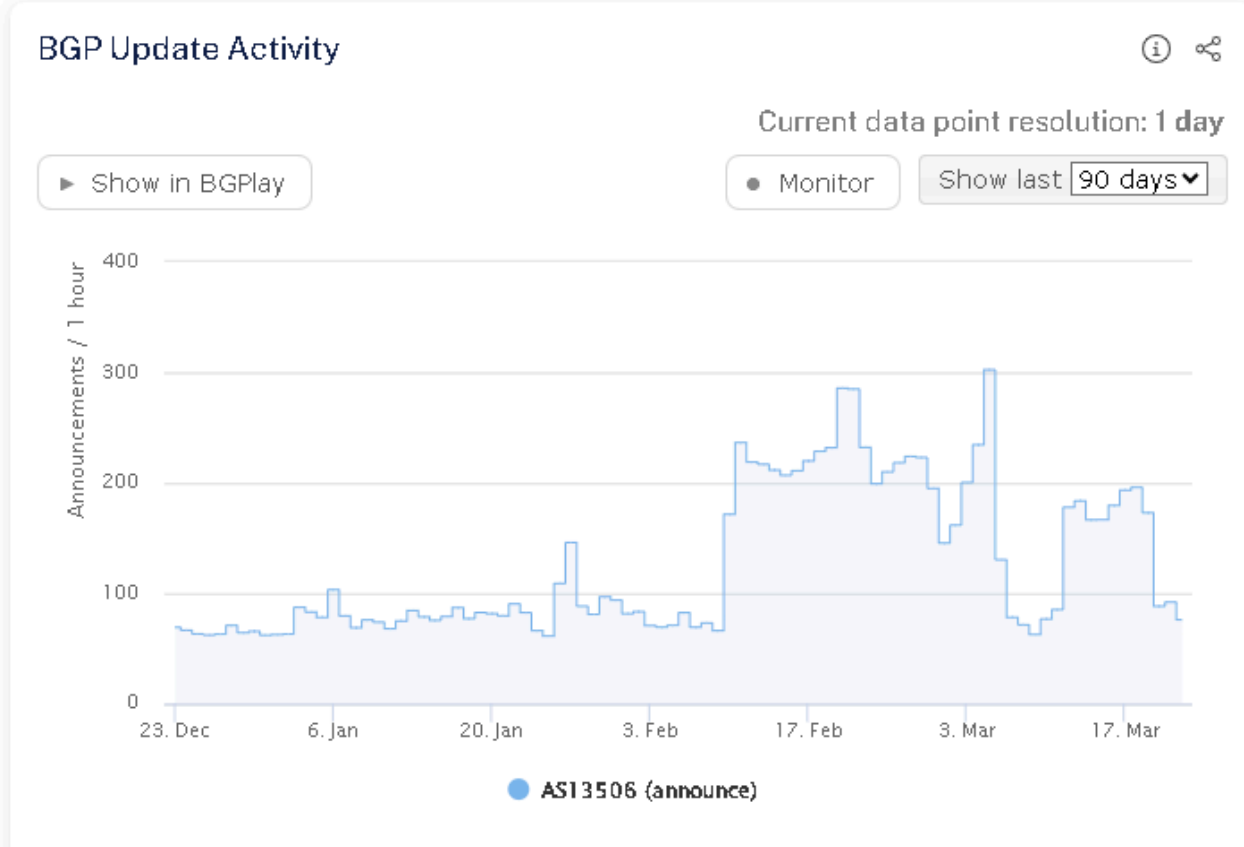
B0f2526a05d0fa76cfef84781ff42533d7e0e57c96fc9c7205fd8041e4b5d3c3

Added At 2024-03-13T22:16:43
Updated At 2025-03-15T12:37:09

https://crt.sh/?q=b0f2526a05d0fa76cfef84781ff42533d7e0e57c96fc9c7205fd8041e4b5d3c3

It really could be an artifact of Oracle's AS, just adding so we don't miss anything.

Treasury AS routing spikes
Last 90 days
https://stat.ripe.net/resource/AS13506#tab=routing



Looking at previous 90 days of BGP updates
On Feb 10, the rate of Treasury AS 13506 announcements per day more than doubled, from 1586 day previous to 4116 on Feb 10
and 5675 Feb 11
And 6857 on Feb 20
And 7257 on March 5

Compare to DOGE timeline: January 31, top Treasury official resigns over DOGE data requests
https://thehill.com/homenews/administration/5119996-david-lebryk-retirement-treasury-doge-musk/
Feb 4, News Breaks: DOGE staffer Marko Elez Has Full Admin Privileges at Treasury
https://www.wired.com/story/elon-musk-associate-bfs-federal-payment-system/
Feb 17, Gavin Kliger prepares to access IRS data
https://www.washingtonpost.com/business/2025/02/16/doge-irs-access-taxpayer-data/
https://abcnews.go.com/Politics/elon-musks-doge-asks-access-irs-taxpayer-data/story?id=118883475
Feb 25, Acting IRS commissioner Doug O'Donnell Resigns, replaced by Tom Krause CEO of Cloud Software Group

https://www.irs.gov/newsroom/krause-to-serve-as-acting-irs-commissioner-odonnell-retires-after-distinguished-career#:~:text=O'Donnell%2C%20the%20IRS%20Deputy,of%20the%20nation's%20tax%20agency.

Starlink / SpaceX

Fresh data
shodan_starlink-AS-14593-SQLBrowser-1434.csv
https://drive.proton.me/urls/W416VV388G#qb2SgzirARe7
Pulled from
https://www.shodan.io/search?query=asn%3A%22AS14593%22+product%3A%22SQL+Server+Browser+Service%22
Query: asn:"AS14593" product:"SQL Server Browser Service"

52.166.151.221
https://www.shodan.io/host/52.166.151.221
Related hostname b6474429cbdd.database.azure.com has no DNS records
Only time seen Shodan 3/22/25
2025-03-22T20:06:45.330939

spacex-pgdb-qa.postgres.database.azure.com first seen on 52.166.151.221 on 3/12/25
Compare this to the Azure China postresql database below that has “3-16” in the name but first seen 3-10 and last seen 3-19. They named the endpoint in advance knowing it would come 3-16 perhaps? Speculation.

IP Addresses	Organization	First Seen	Last Seen	Duration Seen
52.166.151.221	Microsoft Corporation	2025-03-12 (12 days)	2025-03-23 (today)	11 days
13.95.128.208	Microsoft Corporation	2024-07-14 (8 months)	2025-03-12 (12 days)	8 months
40.68.125.32	Microsoft Corporation	2024-05-08 (11 months)	2024-07-14 (8 months)	2 months

13.73.180.59	Microsoft Corporation	2023-12-15 (1 year)	2024-05-08 (11 months)	5 months
13.73.180.146	Microsoft Corporation	2023-10-15 (1 year)	2023-12-15 (1 year)	2 months

34.254.253.243
Seem to be country names. I thought Starlink wasn't in Russia?
India, China, Turkey, Russia, Ukraine
https://securitytrails.com/list/ip/34.254.253.243
https://www.shodan.io/domain/link-spacex.com

Domain	Rank
in.link-spacex.com	
in.c.link-spacex.com	
c.link-spacex.com	
manager.ru.c.link-spacex.com	
turkiye.c.link-spacex.com	
in-manage.c.link-spacex.com	
ec2-34-254-253-243.eu-west-1.compute.amazonaws.com	
phantom.link-spacex.com	
ua.c.link-spacex.com	
ru.c.link-spacex.com	
ru-manage.c.link-spacex.com	

manage.c.link-spacex.com

143.105.0.103
customer.ashnvax2.pop.starlinkisp.net

Ashburn, Virginia is where AWS datacenter is. Note “x” at end of name, special Musk signifier perhaps?
Only observed once each, 3/11 SMB, 3/13 port 1434 SQL Browser
https://www.shodan.io/host/143.105.0.103
No DNS history
https://securitytrails.com/domain/customer.ashnvax2.pop.starlinkisp.net/history/a

Okay, so Amazon partners with SpaceX through Project Kuiper

https://www.aboutamazon.com/what-we-do/devices-services/project-kuiper
Okay, but here’s the weird part. SpaceX’s Starlink is a *competitor* to Amazon’s project. They only *launch* Amazon’s satellite, not provide actual links from Starlink’s own satellites. Starlink has *their own* network of ground stations supporting their infrastructure.

But for some reason, Starlinkisp.net has set up some new subdomains clearly matching the locations of Amazon data centers. I just checked a few randomly, they don’t have DNS records or Shodan observations

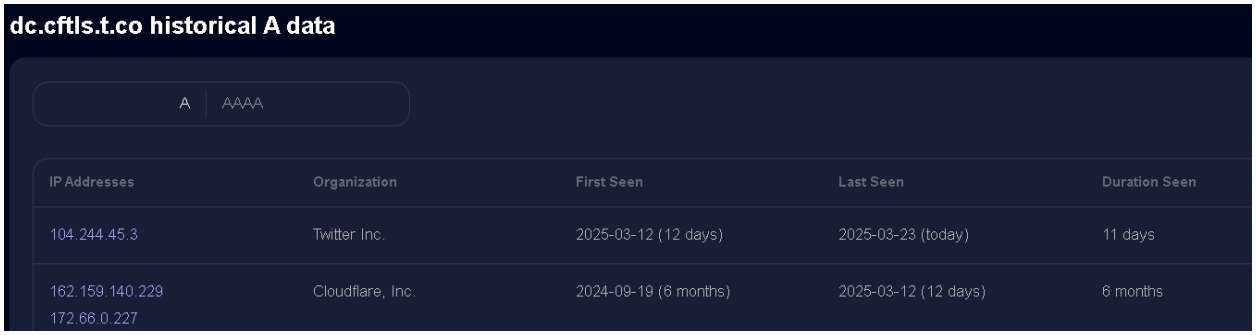
Check it out. I also included “tor” bc what’s up with that?

https://www.shodan.io/domain/starlinkisp.net

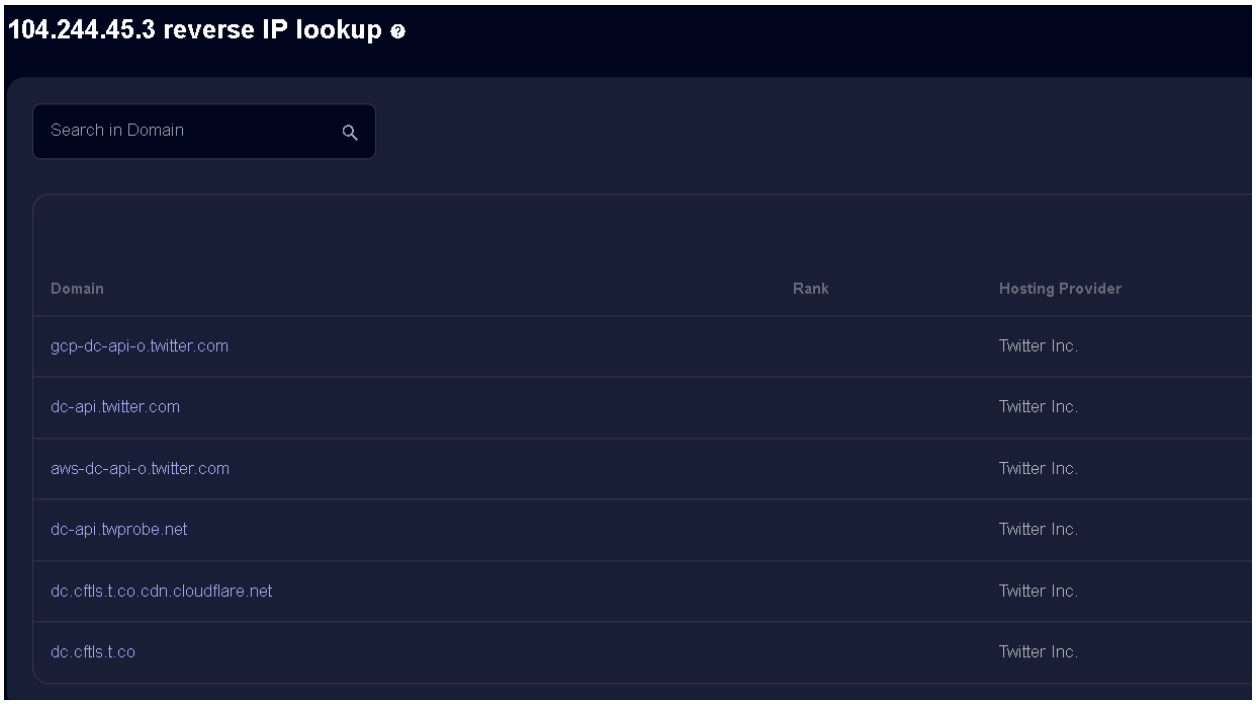
rchntxx9-sdc-tor10a	A	10.141.238.30
rchntxx9-sdc-tor11a	A	10.141.238.33
rchntxx9-sdc-tor11b	A	10.141.238.34
rchntxx9-sdc-tor14b	A	10.141.238.43
rchntxx9-sdc-tor3a	A	10.141.238.9
rchntxx9-sdc-tor4a	A	10.141.238.12
rdmdwax3-agg-rtr1	A	172.22.1.10
rdmdwax3-agg-rtr2	A	172.22.2.10
rdmdwax3-agg-rtr3	A	172.22.3.10

rdmdwax3-edg-rtr1 A 172.22.1.20
rdmdwax3-edg-rtr2 A 172.22.2.20
rdmdwax3-gws-swc1 A 172.22.1.70
rdmdwax3-iot-fwl1 A 135.129.59.234
rdmdwax3-li-fwl1 A 135.129.59.247
rdmdwax3-mgt-fwl1 A 135.129.59.244
rdmdwax3-mgt-fwl1 AAAA 2620:134:b003:ff00::1
rdmdwax3-mgt-fwl1-oob A 206.224.95.20
rdmdwax3-mgt-fwl2 A 206.224.90.4
rdmdwax3-mgt-fwl2 AAAA 2620:134:b003:ff03::1
rdmdwax3-mgt-fwl2-oob A 206.224.95.21
rdmdwax3-mgt-fwl200 A 206.224.91.4

Twitter



104.244.45.3 Moved from cloudflare to twitter on 3/12/25



https://securitytrails.com/list/ip/104.244.45.3

Azure China

pgflexibletest03-16.postgres.database.chinacloudapi.cn
Named it 3-16 for some reason but first seen 3-10, last seen 3-19. Expecting something?

https://securitytrails.com/domain/pgflexibletest03-16.postgres.database.chinacloudapi.cn/history/a

IP Addresses	Organization	First Seen	Last Seen	Duration Seen
143.64.220.107	Shanghai Blue Cloud Technology Co.,Ltd	2025-03-10 (14 days)	2025-03-19 (5 days)	9 days

Queries to run

asn:"AS8075" hostname:spacex
Spacex hosts on Azure Cloud (hosts some gov, but plenty are non gov)

New data
shodan_starlink-AS-14593-SQLBrowser-1434.csv
https://drive.google.com/file/d/1vO83zV4d81CPDMrH83mx2kJyMibSnmkB/view?usp=sharing