Starlink n doge

Starlink business info

https://en.wikipedia.org/wiki/Starlink

- Starlink Services, LLC (a wholly-owned subsidiary of SpaceX)
- Active since 2019; 6 years ago Paying customers since Oct 26, 2020; 4 years ago[2] [2]

DoD, OIG review of Musk clearances in Dec 2024

From NY Times Oct 20/21, 2024

By Eric Lipton lipton@nytimes.com

David A. Fahrenthold Signal 202-309-5010

Aaron Krolik
and Kirsten Grind Signal (347) 417-1874

Published Oct. 20, 2024Updated Oct. 21, 2024

Kirsten Grind

Elon Musk and his rocket company, SpaceX, have repeatedly failed to comply with federal reporting protocols aimed at protecting state secrets, including by not providing some details of his meetings with foreign leaders, according to people with knowledge of the company and internal documents.

Concerns about the reporting practices — and particularly about Mr. Musk, who is SpaceX's chief executive — have triggered at least three federal reviews, eight people with knowledge of the efforts said. The Defense Department's Office of Inspector General opened a review into the matter this year, and the **Air Force and the Pentagon's Office of the Under Secretary of Defense for Intelligence and Security (NOTE: SEE RAINDROP FOR USDIS VULNS)** separately initiated reviews last month, the people said.

The Air Force also recently denied Mr. Musk a high-level security access, citing potential security risks associated with the billionaire. Several allied nations, including Israel, have also expressed concerns that he could share sensitive data with others, according to defense officials. Internally, SpaceX has a team that is expected to ensure compliance with the government's national security rules. Some of those employees have complained to the Defense Department's Office of Inspector General and other agencies about the lax reporting, which goes back to at least 2021, four people with knowledge of the company said. SpaceX was awarded at least $10 billion in federal contracts with the Pentagon and NASA from 2019 to 2023, making it a major contractor.

But since at least 2021, Mr. Musk and SpaceX have not adhered to those reporting requirements, the people with knowledge of SpaceX said. He and his team have not provided some details of his travel — such as his full itineraries — and some of his meetings with foreign leaders, they said. He has also not reported his use of drugs, which is required even with a prescription, they said.

It is unclear why Mr. Musk did not report some of this information to the government, especially since he sometimes posts on X about matters that he does not relay to the Defense Department. It is also unclear if Mr. Musk instructed SpaceX to not report the information. No federal agency has accused him of disclosing classified material.
Still, "to have someone who has major contracts with the government who would be in a position to pass along — whether deliberately or inadvertently — secrets is concerning," said Senator Jeanne Shaheen, Democrat of New Hampshire and a member of the Senate Committees on Armed Services and Foreign Relations.
Last month, Ms. Shaheen asked the Air Force and the Defense Department's Office of Inspector General to investigate whether Mr. Musk was having inappropriate communications with foreign leaders, including President Vladimir V. Putin of Russia.
The Air Force and the Pentagon's Office of the Under Secretary of Defense for Intelligence and Security initiated their reviews in response to questions from Ms. Shaheen and another lawmaker. On Friday, a day after The New York Times asked the secretary of the Air Force, Frank Kendall, about the matter, he responded to Ms. Shaheen, saying federal privacy laws prohibited him from discussing Mr. Musk's case.

DoD contracts

https://www.nbcnews.com/tech/security/musk-xai-was-added-late-pentagon-grok-defense-department-rcna219488

Research in progress

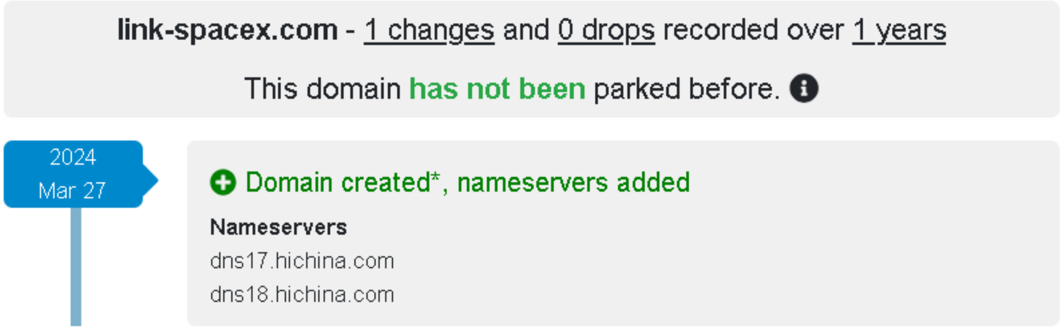
Musk's gov email

erm71@who.eop.gov

General research

https://en.wikipedia.org/wiki/Starlink

link-spacex.com



link-spacex.com - 1 changes and 0 drops recorded over 1 years

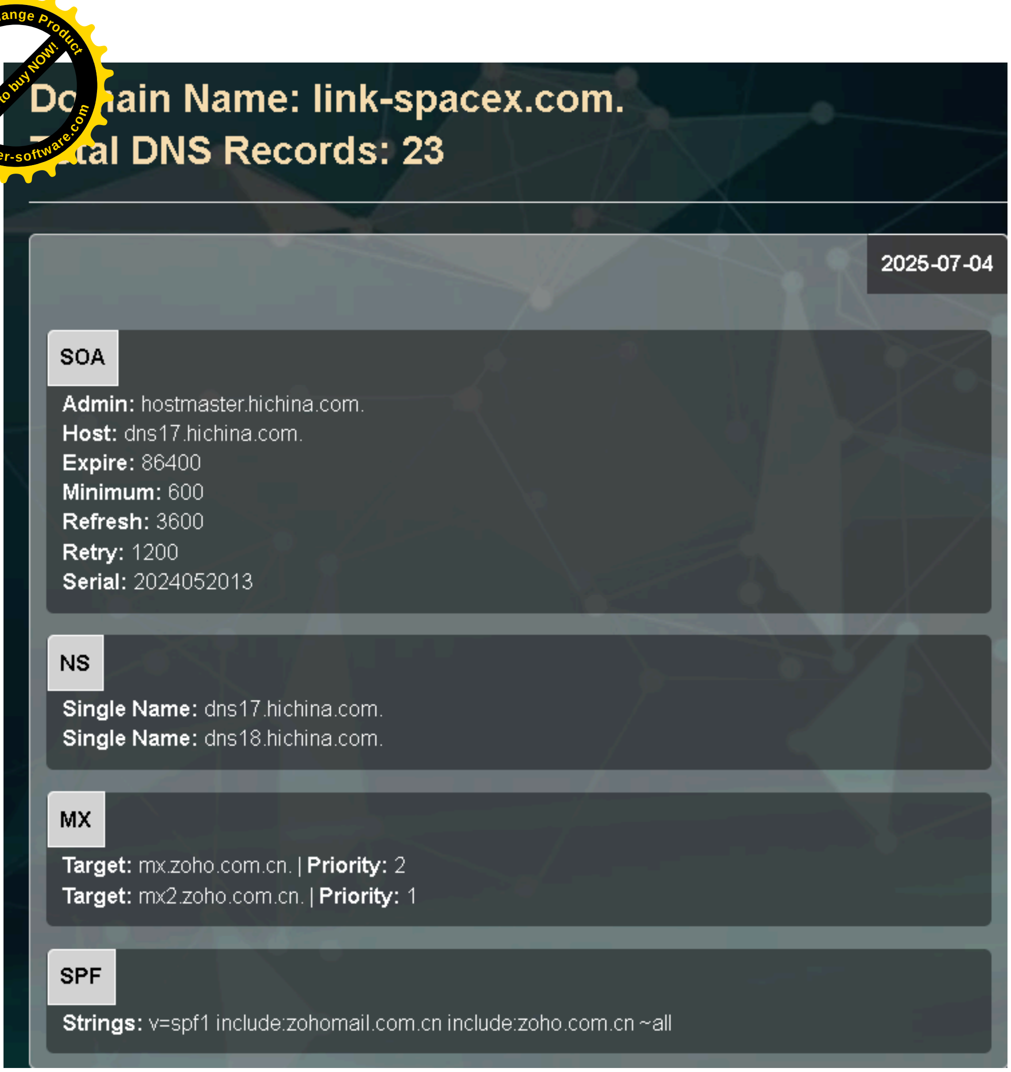
This domain has not been parked before.

2024
Mar 27

Domain created*, nameservers added

Nameservers
dns17.hichina.com
dns18.hichina.com

https://completedns.com/dns-history/



Domain Name: link-spacex.com.
Total DNS Records: 23

2025-07-04

SOA

Admin: hostmaster.hichina.com.
Host: dns17.hichina.com.
Expire: 86400
Minimum: 600
Refresh: 3600
Retry: 1200
Serial: 2024052013

NS

Single Name: dns17.hichina.com.
Single Name: dns18.hichina.com.

MX

Target: mx.zoho.com.cn. | **Priority:** 2
Target: mx2.zoho.com.cn. | **Priority:** 1

SPF

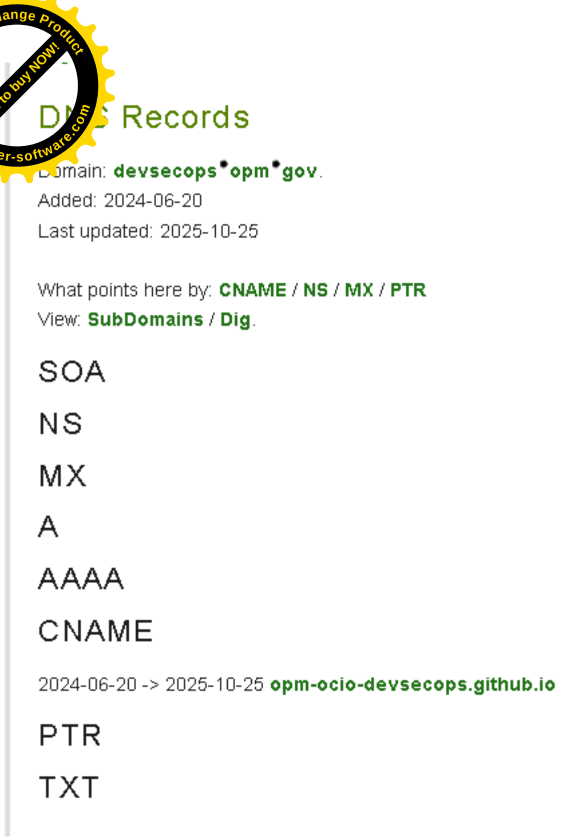
Strings: v=spf1 include:zohomail.com.cn include:zoho.com.cn ~all

https://whoisfreaks.com/tools/dns/history/lookup/link-spacex.com?type=all

From HackerTarget

Same IP ru.pre.link-spacex.com
3.252.209.80

ec2-3-252-209-80.eu-west-1.compute.amazonaws.com
pre.link-spacex.com
manage.pre.link-spacex.com
ru.pre.link-spacex.com
turkiye.pre.link-spacex.com
ua.pre.link-spacex.com



DNS Records

Domain: devsecops•opm•gov.
Added: 2024-06-20
Last updated: 2025-10-25

What points here by: CNAME / NS / MX / PTR
View: SubDomains / Dig.

SOA

NS

MX

A

AAAA

CNAME

2024-06-20 -> 2025-10-25 opm-ocio-devsecops.github.io

PTR

TXT

https://dnshistory.org/dns-records/devsecops.opm.gov
CNAME
2024-06-20 -> 2025-10-25 opm-ocio-devsecops.github.io

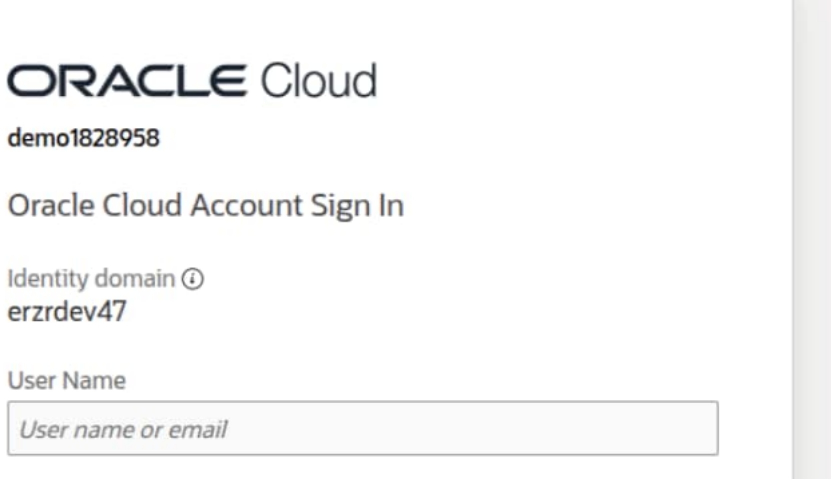
Pivoting from DOGE.gov records

Chain of thought overview

doge[.]gov --> SPF records pitc.gov --> found an old Biden site with 46eop in domain, so tried searching 47eop on urlscan.io

found salesforce infra with47eop--dev47se

https://www.shodan.io/search?query=dev47



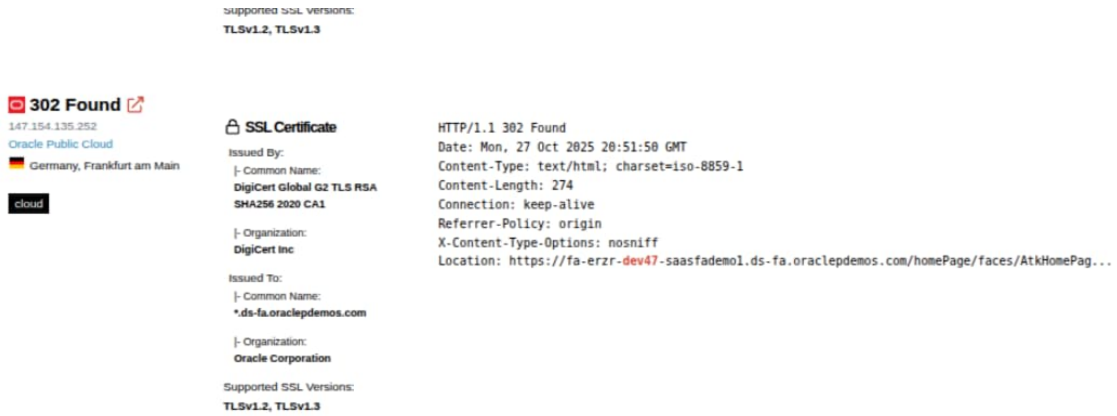
ORACLE Cloud

demo1828958

Oracle Cloud Account Sign In

Identity domain ⓘ
erzrdev47

User Name
User name or email



Supported SSL Versions:
TLSv1.2, TLSv1.3

302 Found
147.154.135.252
Oracle Public Cloud
Germany, Frankfurt am Main
cloud

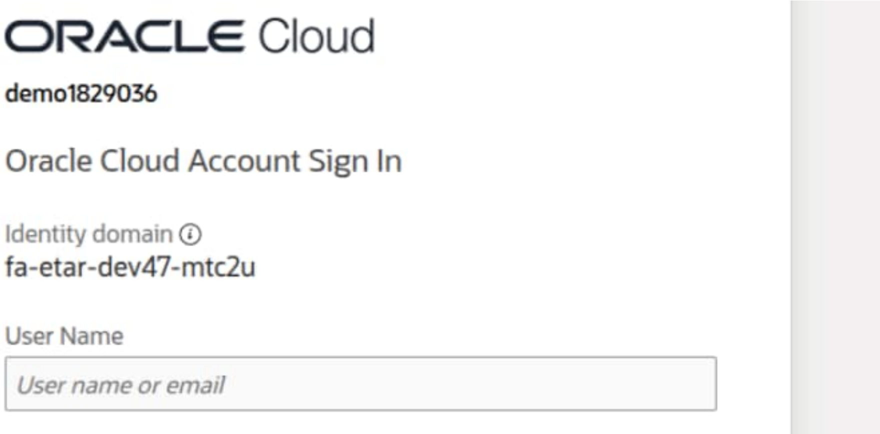
SSL Certificate
Issued By:
|- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1
|- Organization:
DigiCert Inc
Issued To:
|- Common Name:
*.ds-fa.oraclepdemos.com
|- Organization:
Oracle Corporation
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 302 Found
Date: Mon, 27 Oct 2025 20:51:50 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 274
Connection: keep-alive
Referrer-Policy: origin
X-Content-Type-Options: nosniff
Location: https://fa-erzr-dev47-saasfademo1.ds-fa.oraclepdemos.com/homePage/faces/AtkHomePag...
```

Only server in Germany 147.154.135.252, Oracle Public Cloud

https://idcs-ab57fef8b46846a698602fa495b34f38.identity.oraclecloud.com/ui/v1/signin

and



ORACLE Cloud

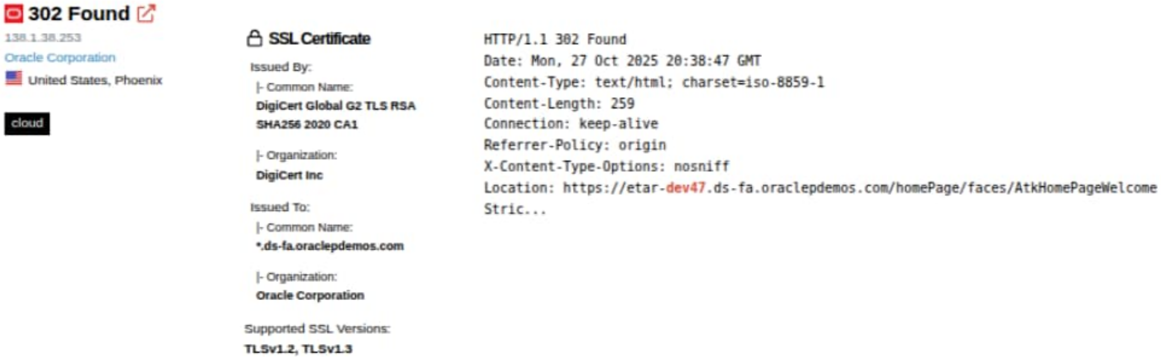
demo1829036

Oracle Cloud Account Sign In

Identity domain ⓘ
fa-etar-dev47-mtc2u

User Name
User name or email

https://idcs-9e08e9fa03664f4fa1f9c50c36b5b6b4.identity.oraclecloud.com/ui/v1/signin

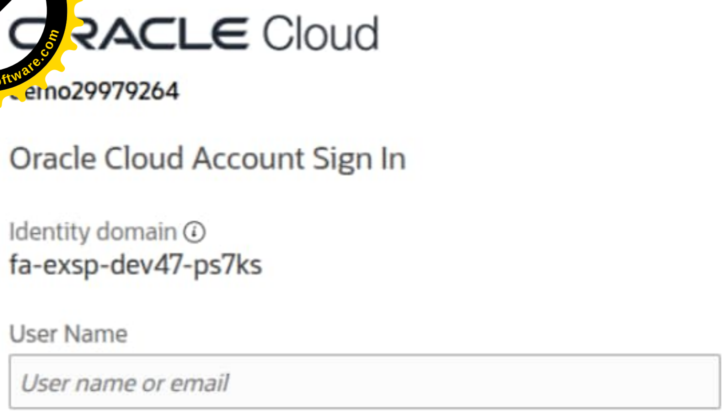


302 Found
138.1.38.253
Oracle Corporation
United States, Phoenix
cloud

SSL Certificate
Issued By:
|- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1
|- Organization:
DigiCert Inc
Issued To:
|- Common Name:
*.ds-fa.oraclepdemos.com
|- Organization:
Oracle Corporation
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 302 Found
Date: Mon, 27 Oct 2025 20:38:47 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 259
Connection: keep-alive
Referrer-Policy: origin
X-Content-Type-Options: nosniff
Location: https://etar-dev47.ds-fa.oraclepdemos.com/homePage/faces/AtkHomePageWelcome
Stric...
```

3rd one:



demo29979264

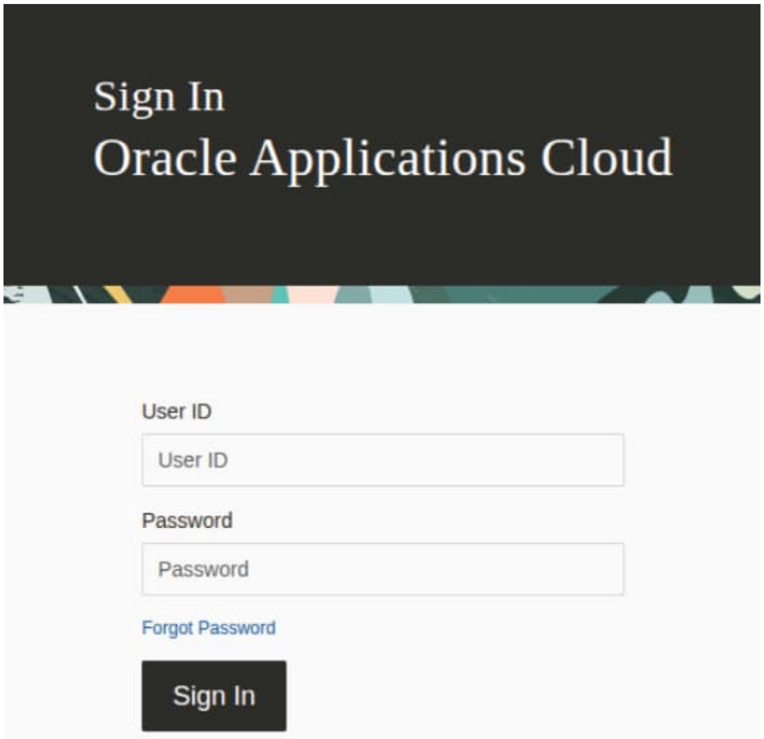
Oracle Cloud Account Sign In

Identity domain ⓘ
fa-exsp-dev47-ps7ks

User Name

https://idcs-b2fc90e89fda44619f53029f2791754a.identity.oraclecloud.com/ui/v1/signin
https://192.29.103.105/

aaand



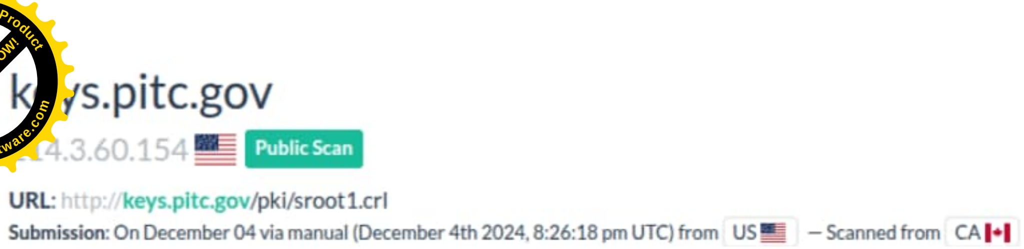
Sign In
Oracle Applications Cloud

https://edtc-dev47.login.us2.oraclecloud.com/oam/server/obrareq.cgi?
encquery%3D1s2vr%2FAOgMM%2B8935t7loatCcYWwVUPHQIsh4k0QMKrbQgbULz%2Bxj1ir1FHm6WtaUebYoAofUSRSd4fEAWyIZO1ICn4tPkzhZr04
Context=1.006G%5E4EB9M02vHT6yBbe6G00801Q0004Xw%3BkXjE

https://whoisfreaks.com/tools/dns/history/lookup/doge.gov?type=all

Strings: v=spf1 include:spf.mail.dmz.pitc.gov ~all
whats pitc.gov? its not a reachable domain...

URLscan.io:



keys.pitc.gov

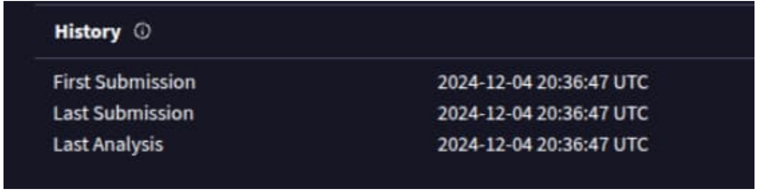
214.3.60.154 🇺🇸

URL: http://keys.pitc.gov/pki/sroot1.crl

Submission: On December 04 via manual (December 4th 2024, 8:26:18 pm UTC) from US 🇺🇸 — Scanned from CA 🇨🇦

Hm, keys and a CRL…? December 4, 2024 eh?

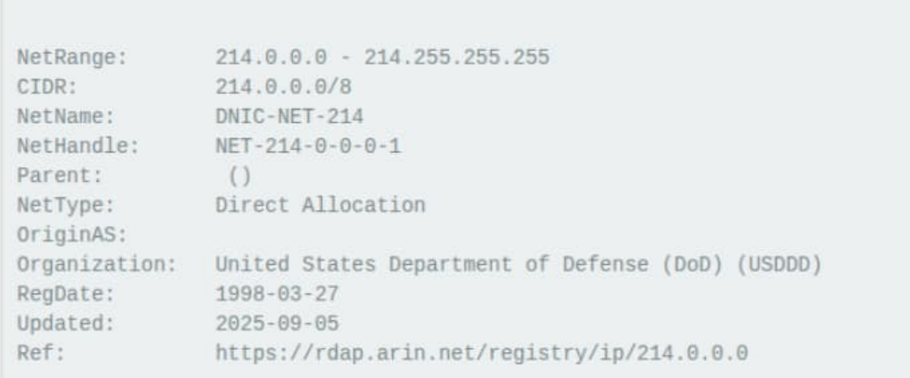
VirusTotal says



History

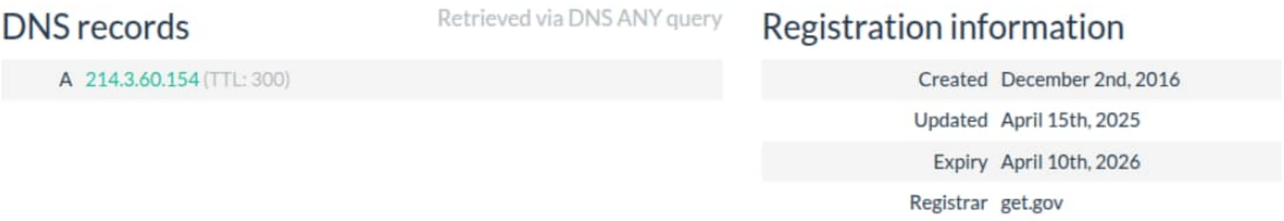
First Submission	2024-12-04 20:36:47 UTC
Last Submission	2024-12-04 20:36:47 UTC
Last Analysis	2024-12-04 20:36:47 UTC

WHOIS



```
NetRange:       214.0.0.0 - 214.255.255.255
CIDR:           214.0.0.0/8
NetName:        DNIC-NET-214
NetHandle:      NET-214-0-0-0-1
Parent:          ()
NetType:        Direct Allocation
OriginAS:
Organization:   United States Department of Defense (DoD) (USDDD)
RegDate:        1998-03-27
Updated:        2025-09-05
Ref:            https://rdap.arin.net/registry/ip/214.0.0.0
```

AS27064 DoD



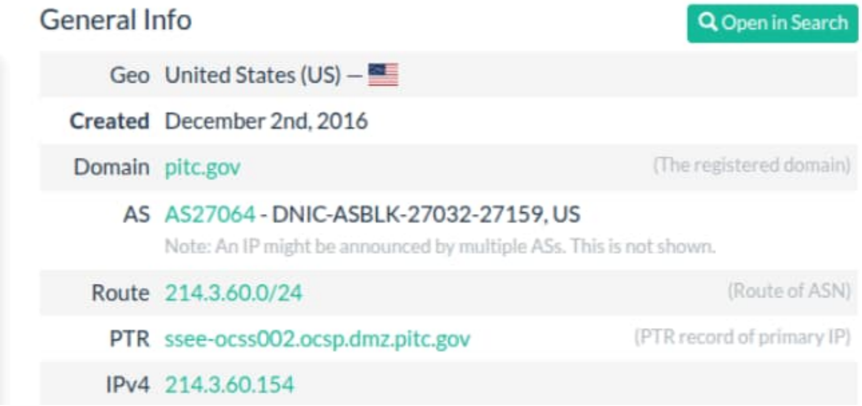
DNS records Retrieved via DNS ANY query

A	214.3.60.154 (TTL: 300)

Registration information

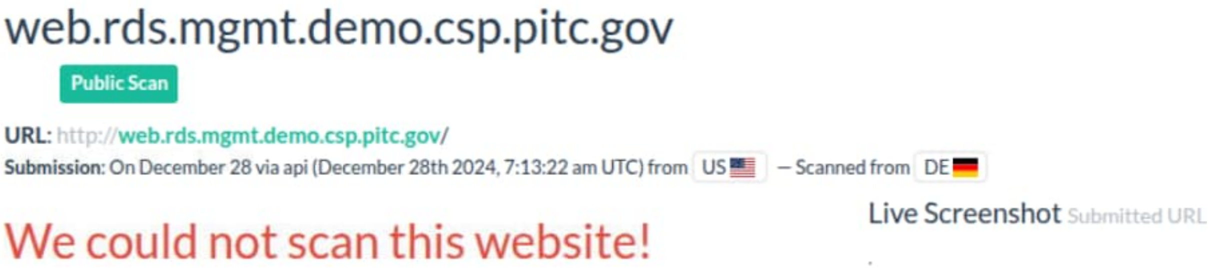
Created	December 2nd, 2016
Updated	April 15th, 2025
Expiry	April 10th, 2026
Registrar	get.gov

Interesting, created Dec 2, 2016, and Keys.pitc.gov was scanned Dec 4, 2024, both incoming trump admins



General Info

Geo	United States (US) — 🇺🇸
Created	December 2nd, 2016
Domain	pitc.gov (The registered domain)
AS	AS27064 - DNIC-ASBLK-27032-27159, US Note: An IP might be announced by multiple ASs. This is not shown.
Route	214.3.60.0/24 (Route of ASN)
PTR	ssee-ocss002.ocsp.dmz.pitc.gov (PTR record of primary IP)
IPv4	214.3.60.154



web.rds.mgmt.demo.csp.pitc.gov

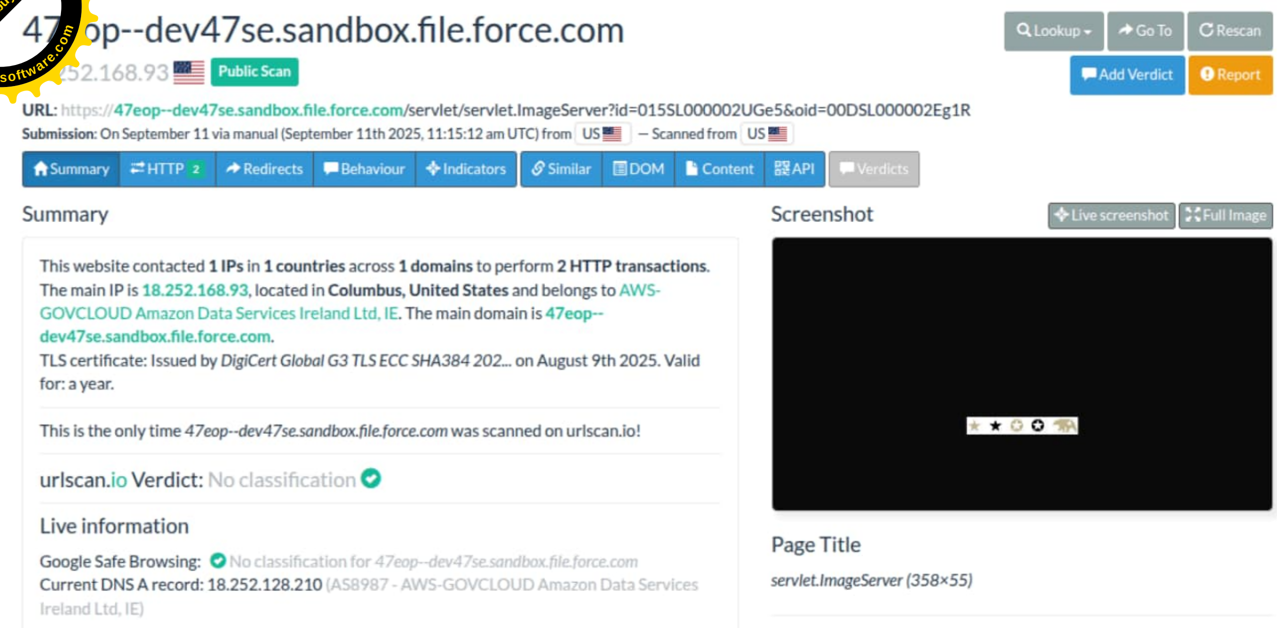
URL: http://web.rds.mgmt.demo.csp.pitc.gov/

Submission: On December 28 via api (December 28th 2024, 7:13:22 am UTC) from US 🇺🇸 — Scanned from DE 🇩🇪

Live Screenshot Submitted URL

We could not scan this website!

URLScan.io search for 47eop found this Sept 11, 2025 icon set that seems to be Cali, and who else?



47 op--dev47se.sandbox.file.force.com

52.168.93 🇺🇸 Public Scan

URL: https://47eop--dev47se.sandbox.file.force.com/servlet/servlet.ImageServer?id=015SL000002UGe5&oid=00DSL000002Eg1R
Submission: On September 11 via manual (September 11th 2025, 11:15:12 am UTC) from US 🇺🇸 — Scanned from US 🇺🇸

Summary

This website contacted **1 IPs** in **1 countries** across **1 domains** to perform **2 HTTP transactions**. The main IP is 18.252.168.93, located in **Columbus, United States** and belongs to AWS-GOVCLOUD Amazon Data Services Ireland Ltd, IE. The main domain is 47eop--dev47se.sandbox.file.force.com.
TLS certificate: Issued by *DigiCert Global G3 TLS ECC SHA384 202...* on August 9th 2025. Valid for: a year.

This is the only time *47eop--dev47se.sandbox.file.force.com* was scanned on urlscan.io!

urlscan.io **Verdict:** No classification ✓

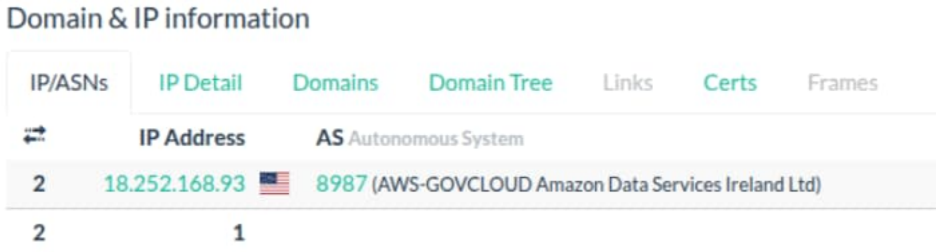
Live information

Google Safe Browsing: ✓ No classification for *47eop--dev47se.sandbox.file.force.com*
Current DNS A record: 18.252.128.210 (AS8987 - AWS-GOVCLOUD Amazon Data Services Ireland Ltd, IE)

Screenshot

Page Title

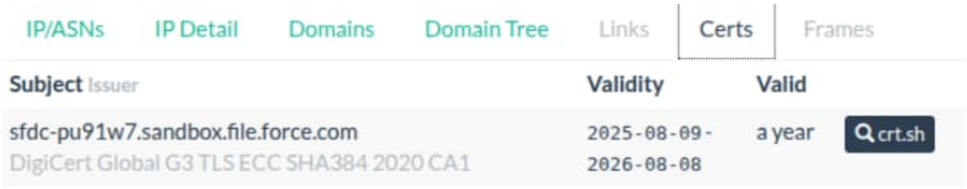
servlet.ImageServer (358×55)



Domain & IP information

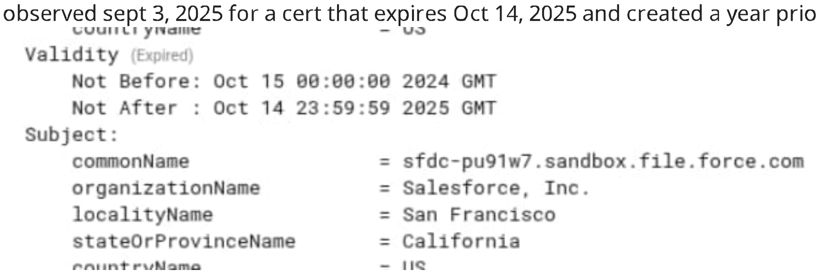
⇄	IP Address	AS Autonomous System
2	18.252.168.93 🇺🇸	8987 (AWS-GOVCLOUD Amazon Data Services Ireland Ltd)
2	1	

General
Full URL
https://47eop--dev47se.sandbox.file.force.com/servlet/servlet.ImageServer?id=015SL000002UGe5&oid=00DSL000002Eg1R
Protocol
H2
Security
TLS 1.3, , AES_128_GCM
Server
18.252.168.93 Columbus, United States, ASN8987 (AWS-GOVCLOUD Amazon Data Services Ireland Ltd, IE),
Reverse DNS
ec2-18-252-168-93.us-gov-east-1.compute.amazonaws.com
Software
/
Resource Hash
117529c565d4d8000c904bf118607ed58a67b9b325b51b28783ae0a5317ce80c



Subject Issuer	Validity	Valid	
sfdc-pu91w7.sandbox.file.force.com DigiCert Global G3 TLS ECC SHA384 2020 CA1	2025-08-09 - 2026-08-08	a year	crt.sh

https://crt.sh/?id=20762619642
observed sept 3, 2025 for a cert that expires Oct 14, 2025 and created a year prior



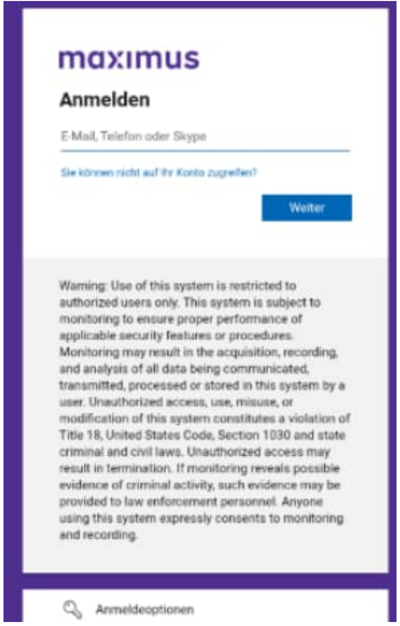
```
    countryName               = US
Validity (Expired)
    Not Before: Oct 15 00:00:00 2024 GMT
    Not After : Oct 14 23:59:59 2025 GMT
Subject:
    commonName                = sfdc-pu91w7.sandbox.file.force.com
    organizationName          = Salesforce, Inc.
    localityName              = San Francisco
    stateOrProvinceName       = California
    countryName               = US
```

DoD AS8987 strange stuff

[illegible]geoaxis.gs.mil
214.28.196.150

Maximus...CSI?

Found this stumbling through on https://urlscan.io/asn/AS8987



maximus

Anmelden

E-Mail, Telefon oder Skype
Sie können nicht auf Ihr Konto zugreifen?
Weiter

Warning: Use of this system is restricted to authorized users only. This system is subject to monitoring to ensure proper performance of applicable security features or procedures. Monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed or stored in this system by a user. Unauthorized access, use, misuse, or modification of this system constitutes a violation of Title 18, United States Code, Section 1030 and state criminal and civil laws. Unauthorized access may result in termination. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to law enforcement personnel. Anyone using this system expressly consents to monitoring and recording.

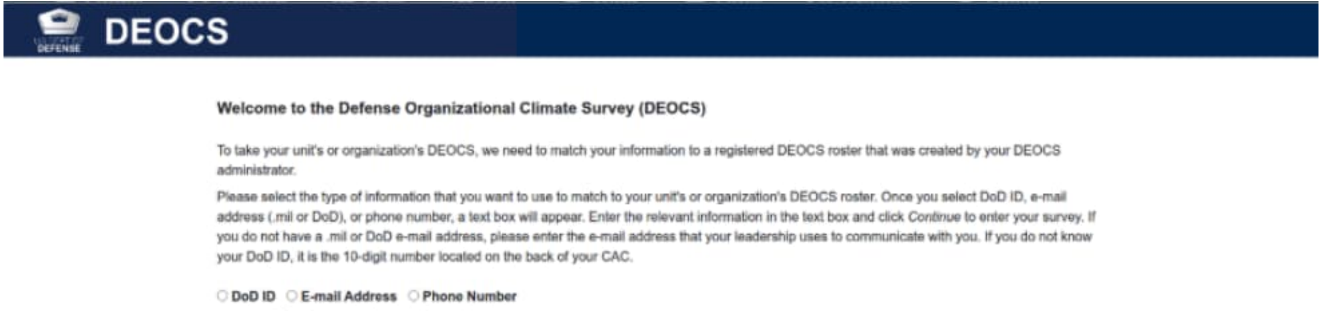
: https://maximuscsi.my.salesforce-setup.com/
MAXIMUS??? CSI, conf / sensitive info on amazon gov?
https://urlscan.io/result/019a2ce0-1396-720c-ac1a-37ed8cde8a71/#summary

More DOD

surveysdrc.com
16.64.1.211

Submitted URL: https://surveysdrc.com/DEOCS
Effective URL: https://surveysdrc.com/deocs_portal/(S(zo0wituwra0dnupggg3bejro))/EnterEmail.aspx

https://urlscan.io/result/019a271e-9cd3-759e-bf47-8856eb202182



Welcome to the Defense Organizational Climate Survey (DEOCS)

To take your unit's or organization's DEOCS, we need to match your information to a registered DEOCS roster that was created by your DEOCS administrator.

Please select the type of information that you want to use to match to your unit's or organization's DEOCS roster. Once you select DoD ID, e-mail address (.mil or DoD), or phone number, a text box will appear. Enter the relevant information in the text box and click *Continue* to enter your survey. If you do not have a .mil or DoD e-mail address, please enter the e-mail address that your leadership uses to communicate with you. If you do not know your DoD ID, it is the 10-digit number located on the back of your CAC.

○ DoD ID ○ E-mail Address ○ Phone Number

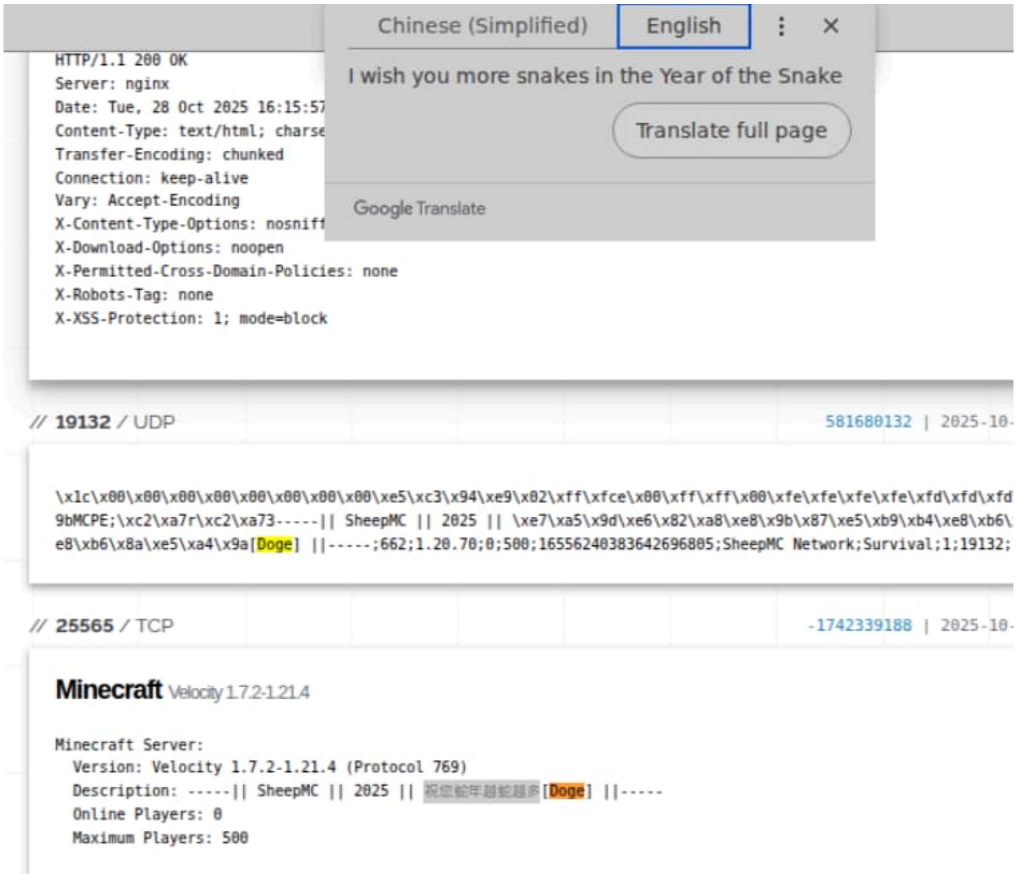
Stylometric analysis resources

https://medium.com/@callyso0414/tracing-ransomware-threat-actors-through-stylometric-analysis-and-chat-log-examination-23f0f84ab

https://github.com/Casualtek/Ransomchats

https://www.danielsoper.com/sentimentanalysis/default.aspx

Looking at "doge" shodan query



```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 28 Oct 2025 16:15:57
Content-Type: text/html; charse
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
X-Robots-Tag: none
X-XSS-Protection: 1; mode=block
```

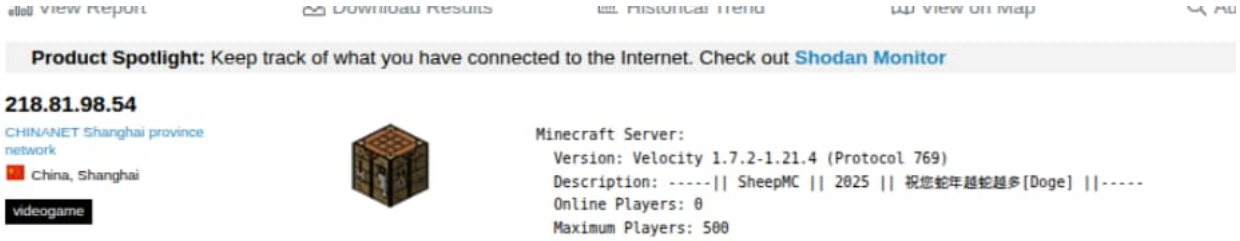
// 19132 / UDP   581680132 | 2025-10-

```
\x1c\x00\x00\x00\x00\x00\x00\x00\x00\xe5\xc3\x94\xe9\x02\xff\xfce\x00\xff\xff\x00\xfe\xfe\xfe\xfe\xfd\xfd\xfd
9bMCPE;\xc2\xa7r\xc2\xa73-----|| SheepMC || 2025 || \xe7\xa5\x9d\xe6\x82\xa8\xe8\x9b\x87\xe5\xb9\xb4\xe8\xb6\
e8\xb6\x8a\xe5\xa4\x9a[Doge] ||-----;662;1.20.70;0;500;16556240383642696805;SheepMC Network;Survival;1;19132;
```

// 25565 / TCP   -1742339188 | 2025-10-

Minecraft Velocity 1.7.2-1.21.4

```
Minecraft Server:
  Version: Velocity 1.7.2-1.21.4 (Protocol 769)
  Description: -----|| SheepMC || 2025 || 祝您蛇年越蛇越多[Doge] ||-----
  Online Players: 0
  Maximum Players: 500
```



Product Spotlight: Keep track of what you have connected to the Internet. Check out Shodan Monitor

218.81.98.54
CHINANET Shanghai province network
China, Shanghai
videogame

```
Minecraft Server:
  Version: Velocity 1.7.2-1.21.4 (Protocol 769)
  Description: -----|| SheepMC || 2025 || 祝您蛇年越蛇越多[Doge] ||-----
  Online Players: 0
  Maximum Players: 500
```

Minecraft eh??

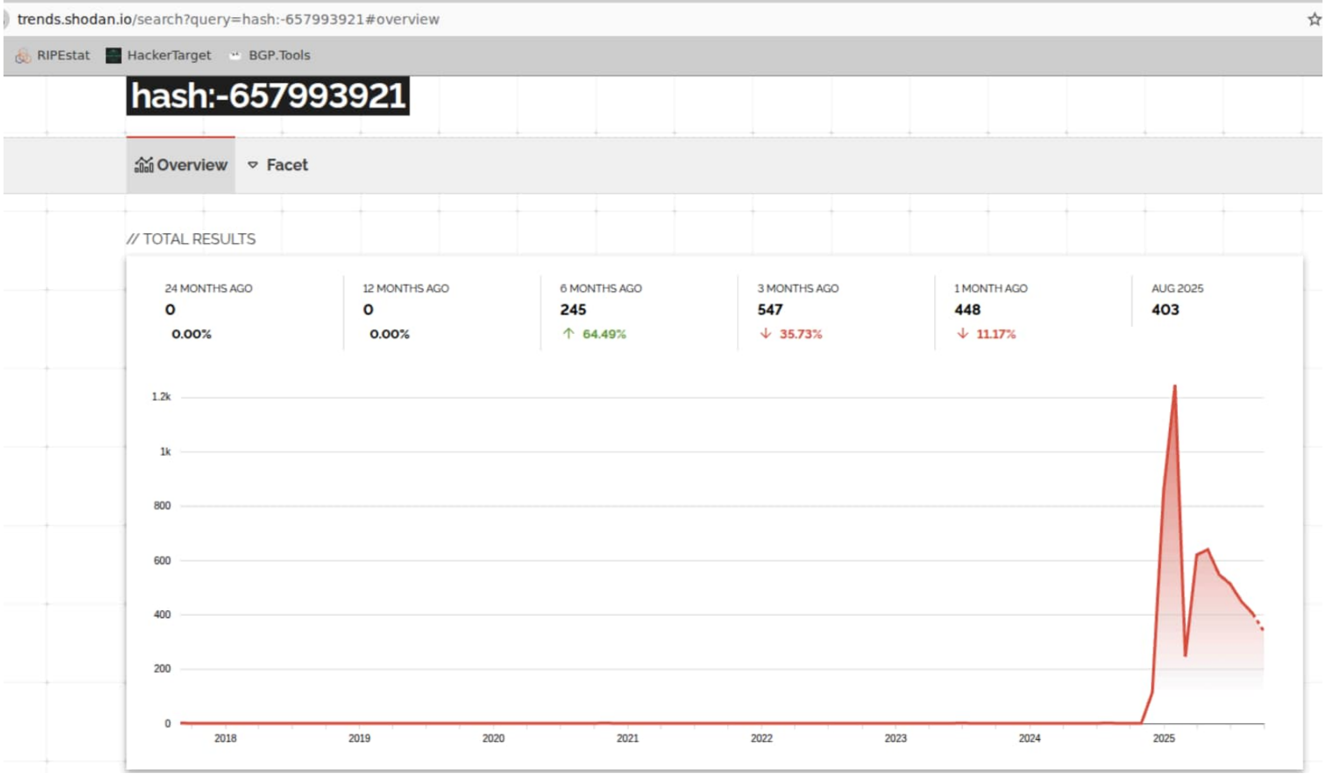
So I followed this "DOGE" chinese minecraft server via hash on the mongodb port
https://www.shodan.io/host/218.81.98.54

with a pretty specific git version
gitVersion": "18b949444cfdaa88e30b0e10243bc18268251c1f"

hash
-657993921 | 2025-10-28T18:54:44.952065

Summary of China DOGE WTF is up China and DOGE and this server Russia

follo[illegible] china doge server --> MongoDB with a specific configuration shared by servers in (descending order) China, U.S., Russia, India. [illegible]ain [illegible]., at least one provider (NatCoWeb) is linked with Russia via Russian-Ukrainian founder (Raindrop? Obsidian?)

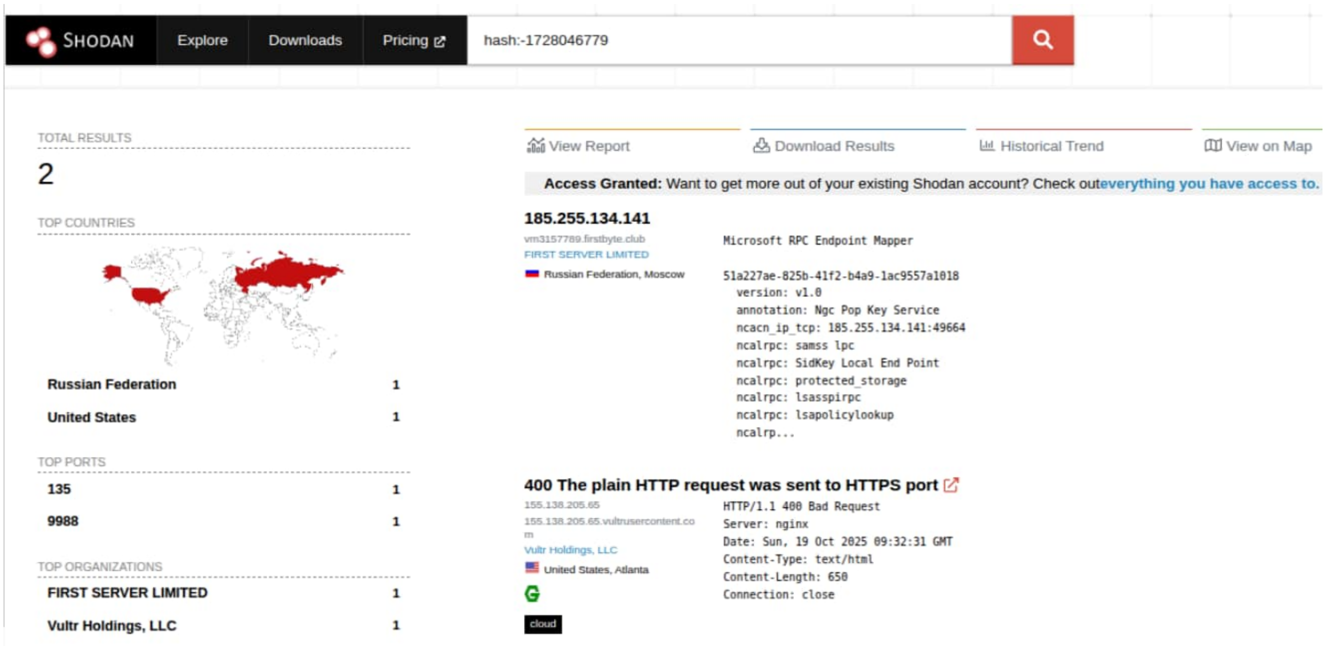

trends.shodan.io/search?query=hash:-657993921#overview

hash:-657993921

// TOTAL RESULTS

24 MONTHS AGO	12 MONTHS AGO	6 MONTHS AGO	3 MONTHS AGO	1 MONTH AGO	AUG 2025
0	0	245	547	448	403
0.00%	0.00%	↑ 64.49%	↓ 35.73%	↓ 11.17%	

DAYUM



hash:-1728046779

TOTAL RESULTS

2

TOP COUNTRIES

Russian Federation	1
United States	1

TOP PORTS

135	1
9988	1

TOP ORGANIZATIONS

FIRST SERVER LIMITED	1
Vultr Holdings, LLC	1

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

185.255.134.141
vm3157789.firstbyte.club
FIRST SERVER LIMITED
Russian Federation, Moscow

```
Microsoft RPC Endpoint Mapper

51a227ae-825b-41f2-b4a9-1ac9557a1018
  version: v1.0
  annotation: Ngc Pop Key Service
  ncacn_ip_tcp: 185.255.134.141:49664
  ncalrpc: samss lpc
  ncalrpc: SidKey Local End Point
  ncalrpc: protected_storage
  ncalrpc: lsasspirpc
  ncalrpc: lsapolicylookup
  ncalrp...
```

400 The plain HTTP request was sent to HTTPS port
155.138.205.65
155.138.205.65.vultrusercontent.com
Vultr Holdings, LLC
United States, Atlanta
cloud

```
HTTP/1.1 400 Bad Request
Server: nginx
Date: Sun, 19 Oct 2025 09:32:31 GMT
Content-Type: text/html
Content-Length: 650
Connection: close
```

Russia
185.255.134.141
2025-10-23T13:31:35.600206
vm3157789.firstbyte.club
FIRST SERVER LIMITED

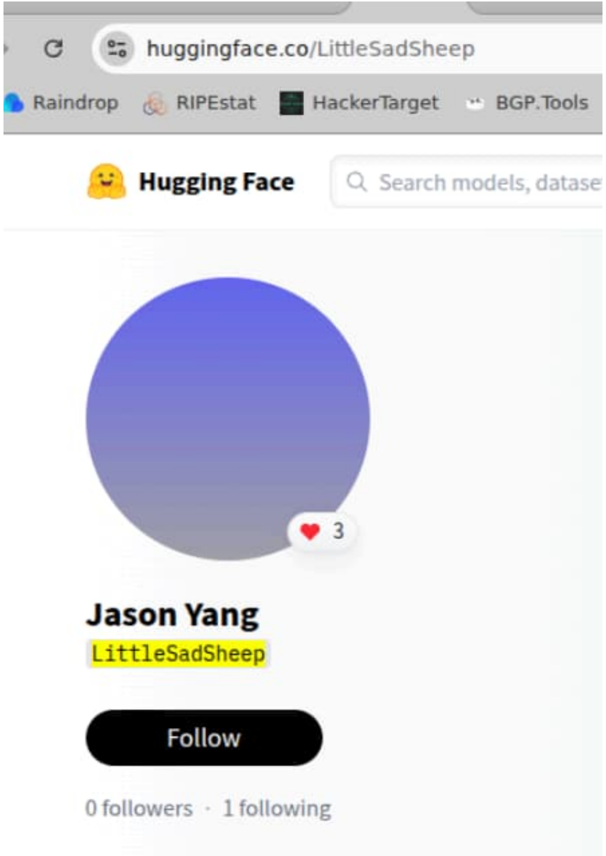
155.138.205.65
https://www.shodan.io/search?query=hash%3A-1728046779

LittleSadSheep started getting active Oct 2024....Same time as BB

https://github.com/LittleSadSheep?tab=overview&from=2024-06-01&to=2024-06-30

——笨蛋兼家里蹲服务器运维，爱吃jvav，使我的搅拌机旋转（摆烂

https://x.com/littlesadsheep



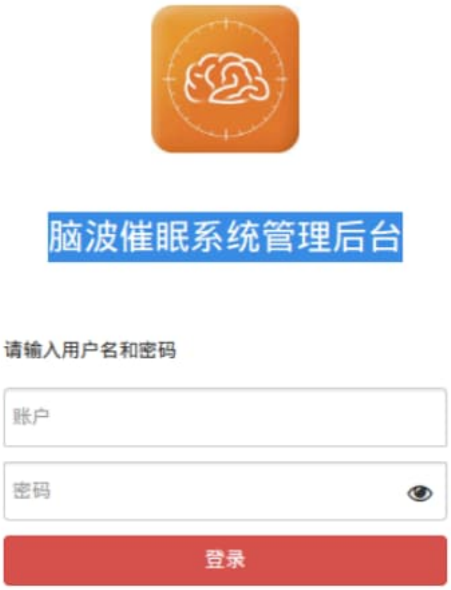
huggingface.co/LittleSadSheep

Jason Yang

LittleSadSheep

0 followers · 1 following

https://huggingface.co/LittleSadSheep/activity/likes

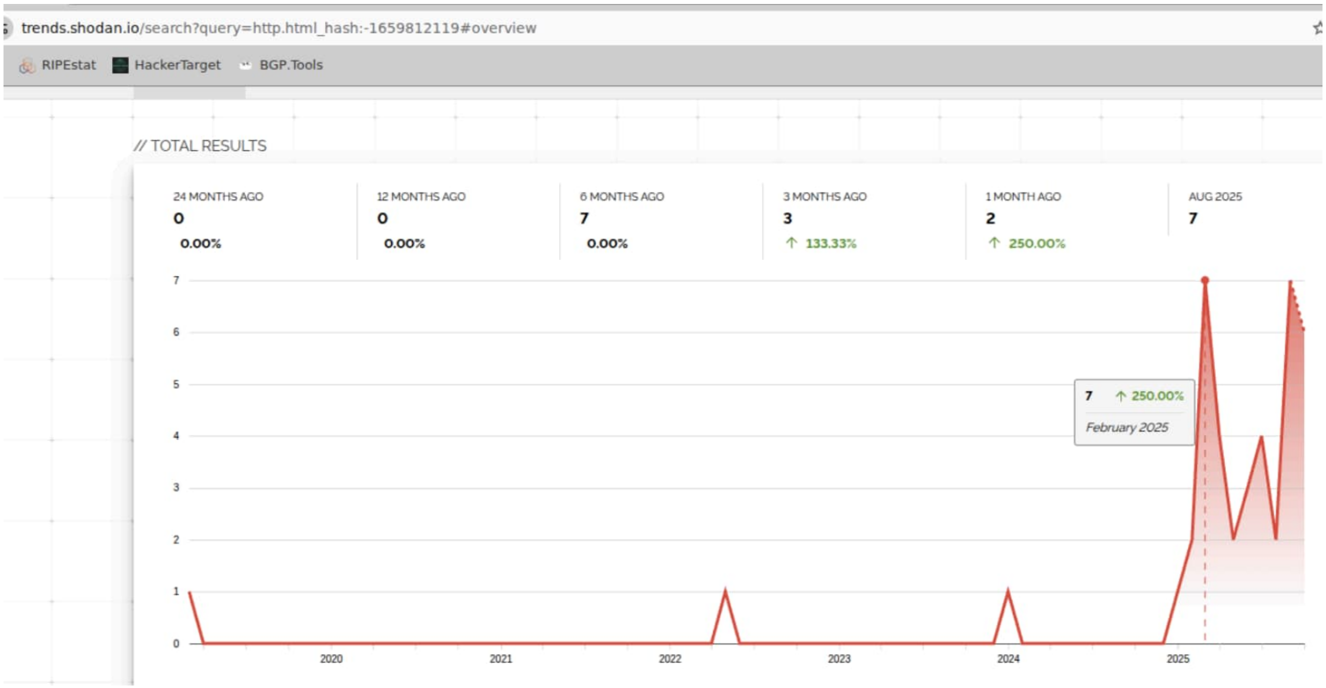


脑波催眠系统管理后台

请输入用户名和密码

http://121.43.149.127/login
from
https://www.shodan.io/search?query=doge+country%3A%22CN%22

DOGE synology disk station manager started appearing Jan 2025



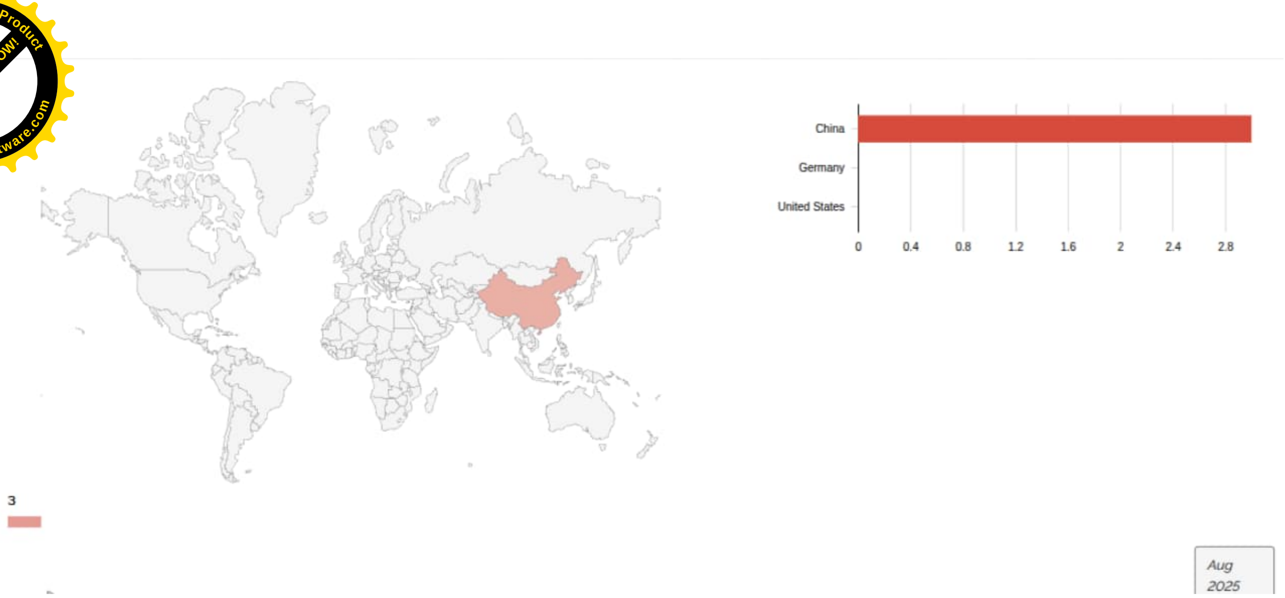
trends.shodan.io/search?query=http.html_hash:-1659812119#overview

// TOTAL RESULTS

24 MONTHS AGO	12 MONTHS AGO	6 MONTHS AGO	3 MONTHS AGO	1 MONTH AGO	AUG 2025
0	0	7	3	2	7
0.00%	0.00%	0.00%	↑ 133.33%	↑ 250.00%	

Spikes in Feb, June, August

PDF-XChange Product Click to buy NOW! www.tracker-software.com

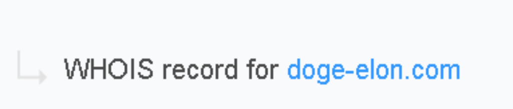


https://www.shodan.io/search?query=doge+country%3A%22CN%22

Russia MongoDB pivot from sadlittlesheep

https://www.shodan.io/host/185.255.134.141

More sus random shit

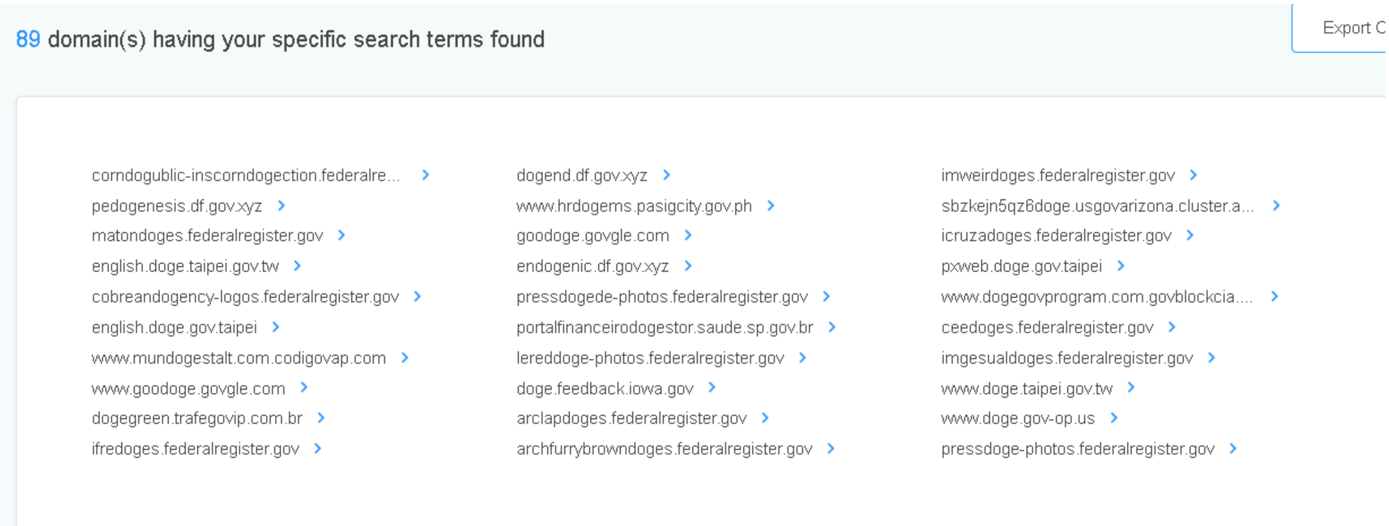


WHOIS record for doge-elon.com

registered last year Israel
remember DOGELON Trevor Nestor

WhoisXML API subdomain search

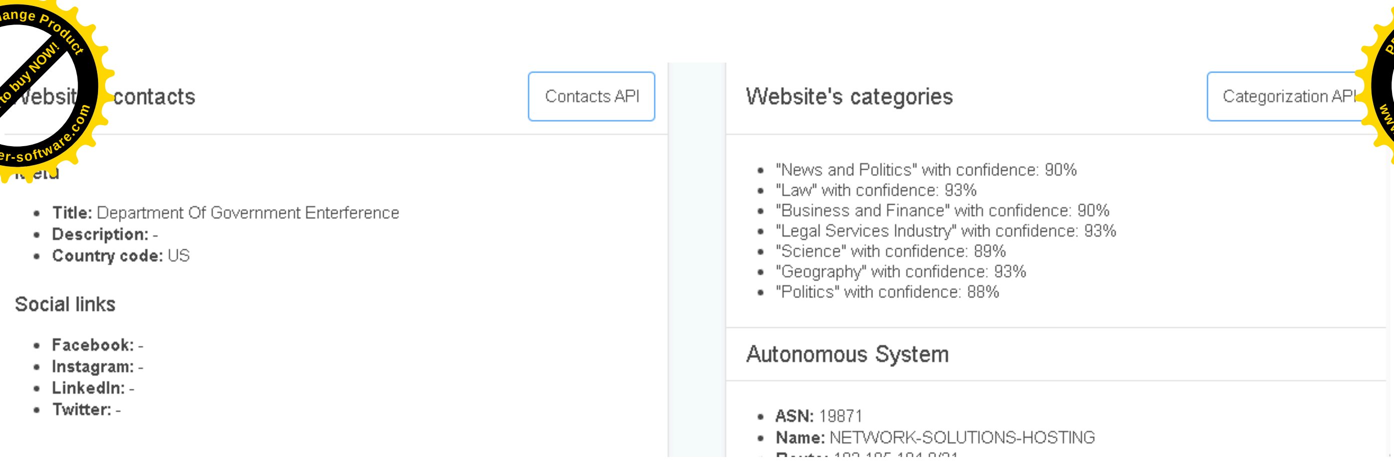
https://tools.whoisxmlapi.com/domains-subdomains-discovery



89 domain(s) having your specific search terms found

- corndogublic-inscorndogection.federalre...
- pedogenesis.df.gov.xyz
- matondoges.federalregister.gov
- english.doge.taipei.gov.tw
- cobreandogency-logos.federalregister.gov
- english.doge.gov.taipei
- www.mundogestalt.com.codigovap.com
- www.goodoge.govgle.com
- dogegreen.trafegovip.com.br
- ifredoges.federalregister.gov
- dogend.df.gov.xyz
- www.hrdogems.pasigcity.gov.ph
- goodoge.govgle.com
- endogenic.df.gov.xyz
- pressdogede-photos.federalregister.gov
- portalfinanceirodogestor.saude.sp.gov.br
- lereddoge-photos.federalregister.gov
- doge.feedback.iowa.gov
- arclapdoges.federalregister.gov
- archfurrybrowndoges.federalregister.gov
- imweirdoges.federalregister.gov
- sbzkejn5qz6doge.usgovarizona.cluster.a...
- icruzadoges.federalregister.gov
- pxweb.doge.gov.taipei
- www.dogegovprogram.com.govblockcia....
- ceedoges.federalregister.gov
- imgesualdoges.federalregister.gov
- www.doge.taipei.gov.tw
- www.doge.gov-op.us
- pressdoge-photos.federalregister.gov

https://gov-op.us/



Website's contacts

field

- **Title:** Department Of Government Enterference
- **Description:** -
- **Country code:** US

Social links

- **Facebook:** -
- **Instagram:** -
- **LinkedIn:** -
- **Twitter:** -

Website's categories

- "News and Politics" with confidence: 90%
- "Law" with confidence: 93%
- "Business and Finance" with confidence: 90%
- "Legal Services Industry" with confidence: 93%
- "Science" with confidence: 89%
- "Geography" with confidence: 93%
- "Politics" with confidence: 88%

Autonomous System

- **ASN:** 19871
- **Name:** NETWORK-SOLUTIONS-HOSTING
- **Route:** 192.185.184.0/21

Doge-related Azure Gov Cloud

sbzqxvoaonjdoge.usgovvirginia.cluster.atlas.usgovcloudapi.net
sbzdogeeg7th9mc.usgovvirginia.cluster.atlas.usgovcloudapi.net

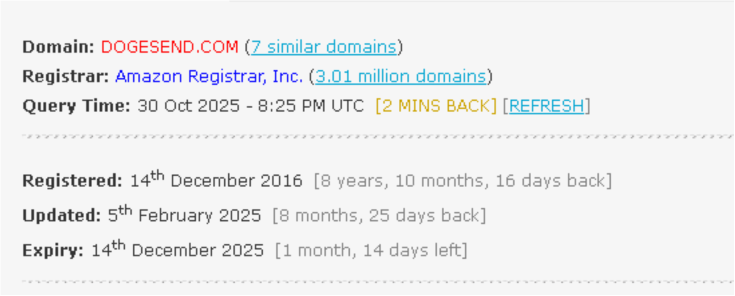
Doge-related .gov subdomains

saltydogede-photos.federalregister.gov
tixlqdogekas.edcgov.us
imfurrybrowndoges.federalregister.gov
dogesend.com.mcas-gov.us
phidogency-logos.federalregister.gov
imawatchdoges.federalregister.gov
saltydogede-photos.federalregister.gov
newonlinevdogency-logos.federalregister.gov
corndogublic-inscorndogection.federalregister.gov

spasec-usgva-devsecops-dev-rg-mysql-server-5170.mysql.database.usgovcloudapi.net

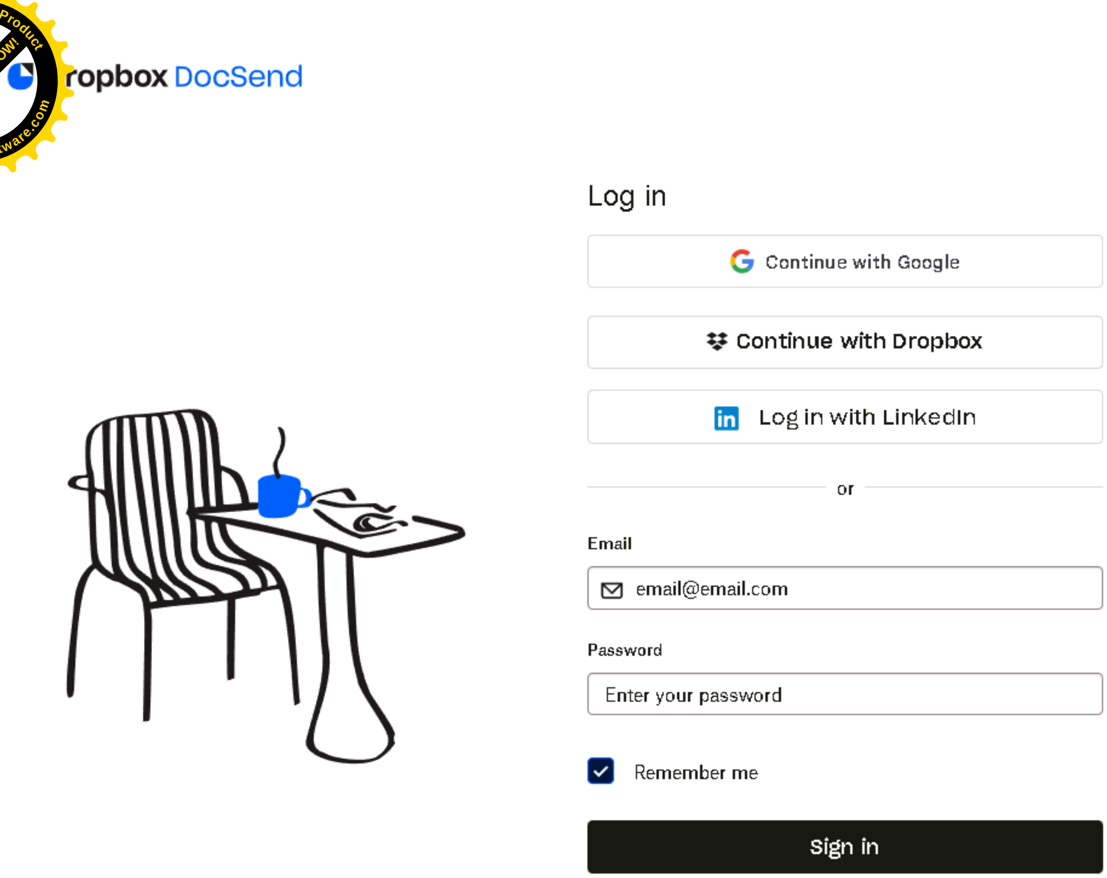
Foreign
doge.gov.taipei
english.doge.taipei.gov.tw
aidoge.southpunjab.gov.pk
www.doge21.ohio.govt.hu

https://dogesend.com/login



Domain: DOGESEND.COM (7 similar domains)
Registrar: Amazon Registrar, Inc. (3.01 million domains)
Query Time: 30 Oct 2025 - 8:25 PM UTC [2 MINS BACK] [REFRESH]

Registered: 14th December 2016 [8 years, 10 months, 16 days back]
Updated: 5th February 2025 [8 months, 25 days back]
Expiry: 14th December 2025 [1 month, 14 days left]



ropbox DocSend

Log in

Continue with Google

Continue with Dropbox

Log in with LinkedIn

or

Email

email@email.com

Password

Enter your password

☑ Remember me

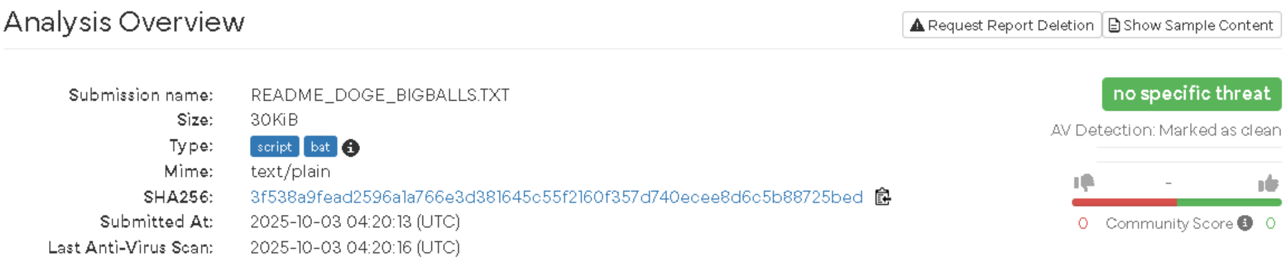
Sign in

public-ipuppydogection.federalregister.gov

Hybrid Analysis and VirusTotal DOGE related malware

When you see an email address pattern in a submission name, it typically indicates:

- **Email attachment origin**: The file was extracted from an email attachment, and the analyst included the recipient/sender address for context
- **User tracking**: The submitter tagged it with an identifier for their own organizational tracking
- **Phishing campaign indicator**: Analysts often include the targeted email address when submitting samples from phishing campaigns
-



Analysis Overview

Request Report Deletion | Show Sample Content

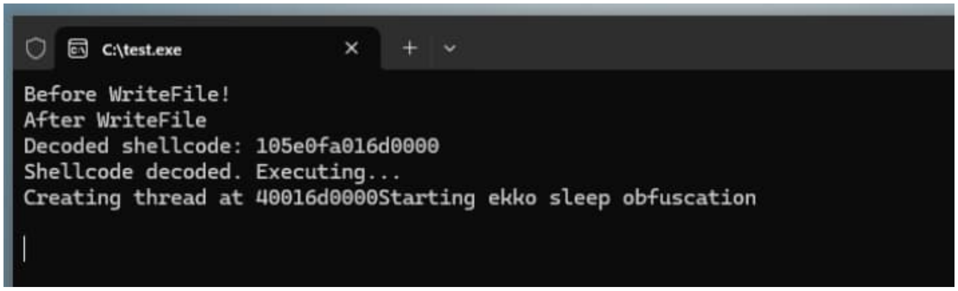
Submission name:	README_DOGE_BIGBALLS.TXT
Size:	30KiB
Type:	script bat
Mime:	text/plain
SHA256:	3f538a9fead2596a1a766e3d381645c55f2160f357d740ecee8d6c5b88725bed
Submitted At:	2025-10-03 04:20:13 (UTC)
Last Anti-Virus Scan:	2025-10-03 04:20:16 (UTC)

no specific threat

AV Detection: Marked as clean

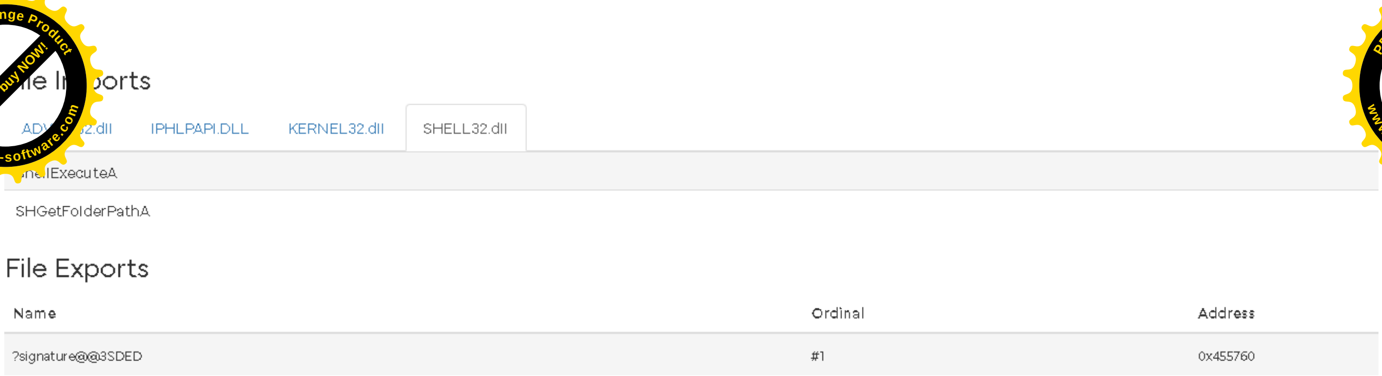
0 Community Score 0

3f538a9fead2596a1a766e3d381645c55f2160f357d740ecee8d6c5b88725bed



C:\test.exe

```
Before WriteFile!
After WriteFile
Decoded shellcode: 105e0fa016d0000
Shellcode decoded. Executing...
Creating thread at 40016d0000Starting ekko sleep obfuscation
```



File Imports

ADVAPI32.dll | IPHLPAPI.DLL | KERNEL32.dll | SHELL32.dll

ShellExecuteA

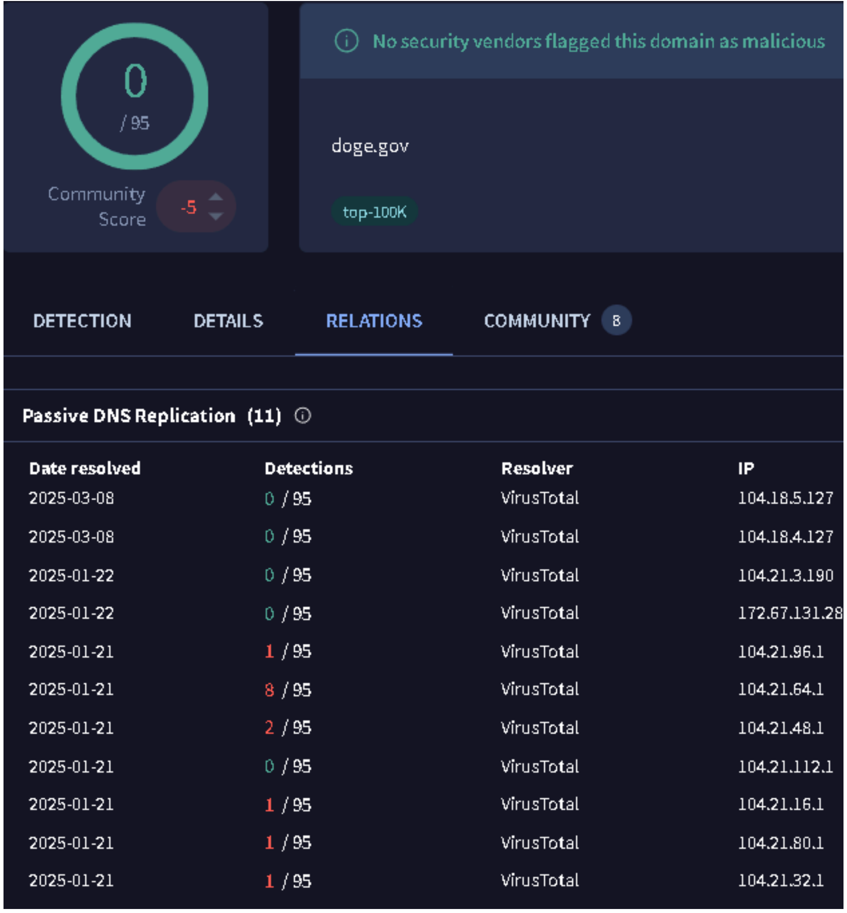
SHGetFolderPathA

File Exports

Name	Ordinal	Address
?signature@@3SDED	#1	0x455760

Why this is not the "misattributed" Big Balls ransomware campaign:

these files were submitted back in Feb 2025, far before any indicators of the ransomware



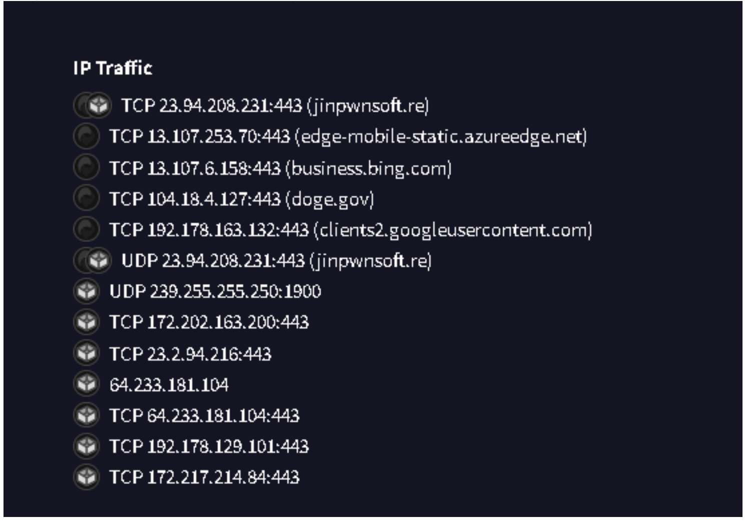
No security vendors flagged this domain as malicious

doge.gov

Passive DNS Replication (11)

Date resolved	Detections	Resolver	IP
2025-03-08	0 / 95	VirusTotal	104.18.5.127
2025-03-08	0 / 95	VirusTotal	104.18.4.127
2025-01-22	0 / 95	VirusTotal	104.21.3.190
2025-01-22	0 / 95	VirusTotal	172.67.131.28
2025-01-21	1 / 95	VirusTotal	104.21.96.1
2025-01-21	8 / 95	VirusTotal	104.21.64.1
2025-01-21	2 / 95	VirusTotal	104.21.48.1
2025-01-21	0 / 95	VirusTotal	104.21.112.1
2025-01-21	1 / 95	VirusTotal	104.21.16.1
2025-01-21	1 / 95	VirusTotal	104.21.80.1
2025-01-21	1 / 95	VirusTotal	104.21.32.1

https://www.virustotal.com/gui/file/5099e6accc82be312d14ed61572f5027138a8a313bc1a4cd703fdf48cd2c250b/behavior



IP Traffic

TCP 23.94.208.231:443 (jinpwnsoft.re)
TCP 13.107.253.70:443 (edge-mobile-static.azureedge.net)
TCP 13.107.6.158:443 (business.bing.com)
TCP 104.18.4.127:443 (doge.gov)
TCP 192.178.163.132:443 (clients2.googleusercontent.com)
UDP 23.94.208.231:443 (jinpwnsoft.re)
UDP 239.255.255.250:1900
TCP 172.202.163.200:443
TCP 23.2.94.216:443
64.233.181.104
TCP 64.233.181.104:443
TCP 192.178.129.101:443
TCP 172.217.214.84:443

DNS Resolutions

business.bing.com
Resolved Ips
13.107.6.158
clients2.googleusercontent.com
Resolved Ips
192.178.163.132
doge.gov
Resolved Ips
104.18.5.127
104.18.4.127
edge-consumer-static.azureedge.net
edge-mobile-static.azureedge.net
Resolved Ips
13.107.253.70
jinpwnsoft.re
Resolved Ips
23.94.208.231
storage.googleapis.com
bg.microsoft.map.fastly.net
Resolved Ips
199.232.210.172
199.232.214.172
redirector.gvt1.com
Resolved Ips
108.177.121.139
108.177.121.113
108.177.121.101
108.177.121.100
108.177.121.102
108.177.121.138

IP Traffic

TCP 23.94.208.231:443 (jinpwnsoft.re)

TCP 13.107.253.70:443 (edge-mobile-static.azureedge.net)

TCP 13.107.6.158:443 (business.bing.com)

TCP 104.18.4.127:443 (doge.gov)

TCP 192.178.163.132:443 (clients2.googleusercontent.com)

UDP 23.94.208.231:443 (jinpwnsoft.re)

UDP 239.255.255.250:1900

TCP 172.202.163.200:443

TCP 23.2.94.216:443

64.233.181.104

TCP 64.233.181.104:443

TCP 192.178.129.101:443

TCP 172.217.214.84:443

```
"C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc

"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument https://jinpwnsoft.re/

"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=C:\Users\
<USER>\AppData\Local\Microsoft\Edge\User Data" /prefetch:4 –monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\
<USER>\AppData\Local\Microsoft\Edge\User Data\Crashpad" --annotation=IsOfficialBuild=1 --annotation=channel= --
annotation=chromium-version=122.0.6261.129 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --
```

annotation=plat=Win64 "--annotation=prod=Microsoft Edge" --annotation=ver=122.0.2365.92 --initial-client-data=0x32c,0x330,0x334,0x328,0x33c,0x7ff8cde05fd8,0x7ff8cde05fe4,0x7ff8cde05ff0
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" –type=gpu-process --no-appcompat-clear --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
--mojo-platform-channel-handle=2060 --field-trial-handle=2064,i,252677469388152830,15530766717893881315,262144 --variations-seed-version /prefetch:2

"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" –type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=2312 --field-trial-handle=2064,i,252677469388152830,15530766717893881315,262144 --variations-seed-version /prefetch:3

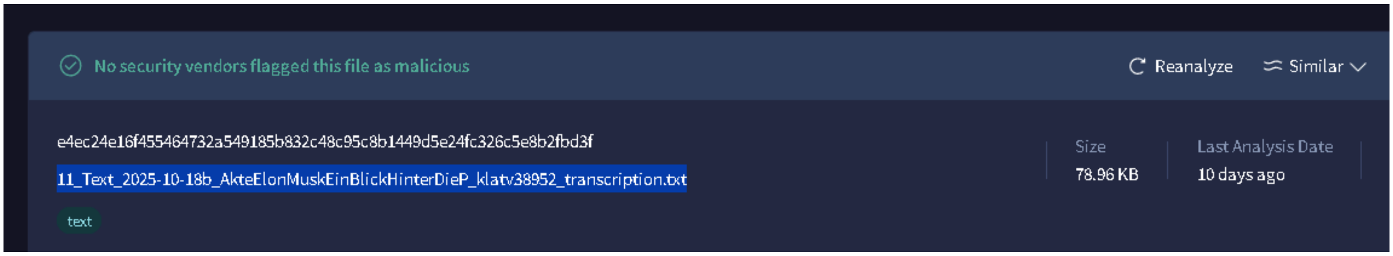
"C:\Users\<USER>\Desktop\YumeKey Tool on the Web.url"

"C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\InputApp\TextInputHost.exe" -ServerName:InputApp.AppX9jnwykgrccxc8by3hsrsh07r423xzvav.mca

"C:\Windows\system32\BackgroundTaskHost.exe" -ServerName:BackgroundTaskHost.WebAccountProvider

C:\Users\<USER>\Desktop\YumeKey Tool on the Web.url

C:\Windows\System32\RuntimeBroker.exe -Embedding



No security vendors flagged this file as malicious

e4ec24e16f455464732a549185b832c48c95c8b1449d5e24fc326c5e8b2fbd3f

11_Text_2025-10-18b_AkteElonMuskEinBlickHinterDieP_klatv38952_transcription.txt

Size: 78.96 KB

Last Analysis Date: 10 days ago

https://www.virustotal.com/gui/file/e4ec24e16f455464732a549185b832c48c95c8b1449d5e24fc326c5e8b2fbd3f

https://www.virustotal.com/gui/domain/files.doge.gov/relations
https://www.virustotal.com/graph/files.doge.gov

https://www.virustotal.com/graph/embed/gda09d19b1ccb4f45918816a6fd839f953a76913451234bf1a2b64d9f0153edd5?theme=dark

PDF that seems to be a guide to media and DOGE targets seen Feb 17, 2025

https://www.virustotal.com/gui/file/0ba697bf64aa204b95083de6db43e271587adb95da46f8f3ad937e34ac9c0569/details

base.apk contacted egov.uscis.gov

https://www.virustotal.com/gui/file/0a7a1d3163b7d9eca355e732d4438794b96983c9d2669551a3a703786e86499a/behavior

https://www.virustotal.com/gui/file/3cf6115f1f89440ba8399930e077f39ec83f82ac445cf55a8707c53a45ad97ee/details

Just sketchy, can monitor vitals and write reproductive data??

https://www.virustotal.com/gui/file/02bb3c1be5b343437bd0fd5a13ee6a21695d5d93631a9b1959317ca7a33a0934/details
Mobile Passport Control
gov.dhs.cbp.pspd.mpc-V1.2.0.apk

Alright start summarizing

1. A suspicious server located in Taiwan (China) with DOGE in the server name.
    1. Minecraft on one port, a very specific MongoDB config on another high-number port
    2. when pivoting on Shodan via MongoDB, about 400 hosts around the world have been observed with same build, version, git build, etc
    3. FIRST OBSERVATION BY SHODAN (TRENDS) - Jan 2025. China, USA, Russia within same month.

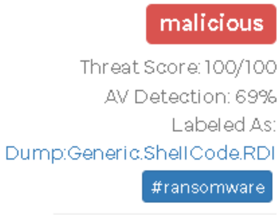
Very sketchy constellation of contacted gov sites from cloudflare 172.65.90.27

https://www.virustotal.com/gui/ip-address/172.65.90.27/relations

suckmychocolatesaltyballs.doge.gov

On October 4, 2025, the Hybrid Analysis malware detection tool received a malware sample "test.exe"

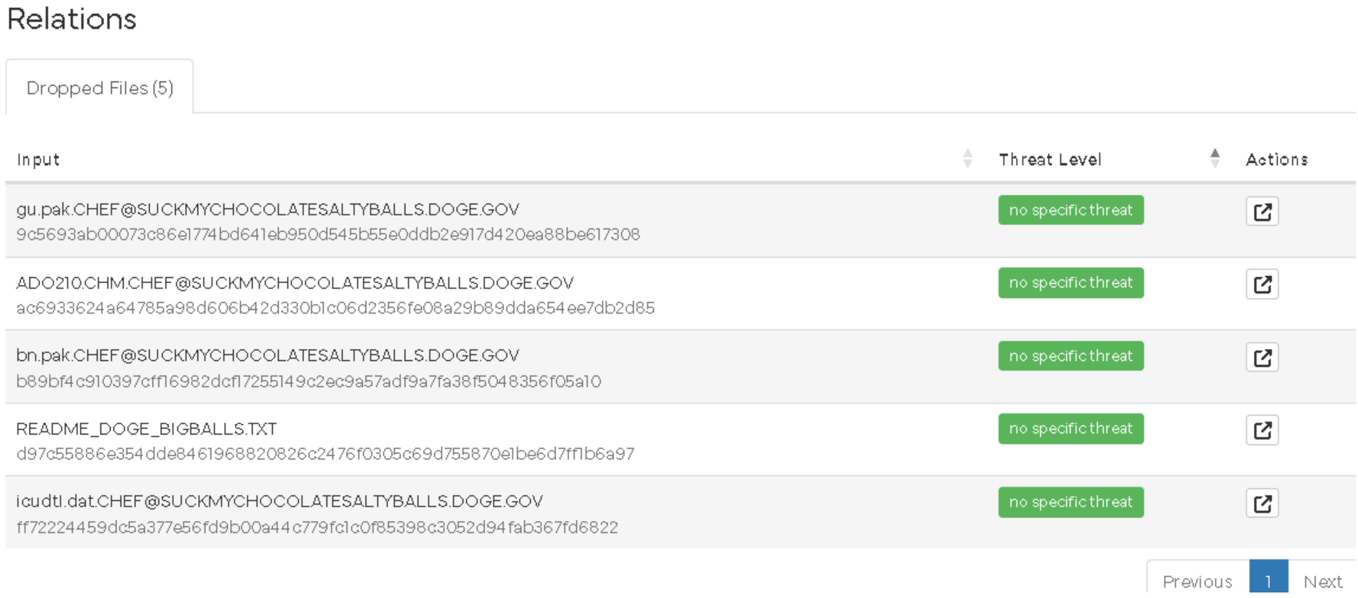
https://hybrid-analysis.com/sample/3feb7babc4040fa802fd2c8d3ce7c6fe5d64d14f8a004ee5faebbabb35bf7b18



malicious

Threat Score: 100/100
AV Detection: 69%
Labeled As:
Dump:Generic.ShellCode.RDI
#ransomware

and dropped a series of files called

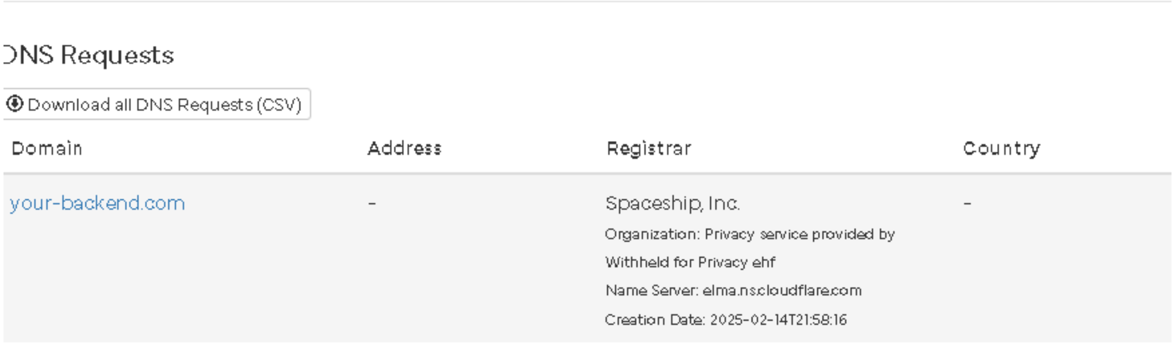


Relations

Dropped Files (5)

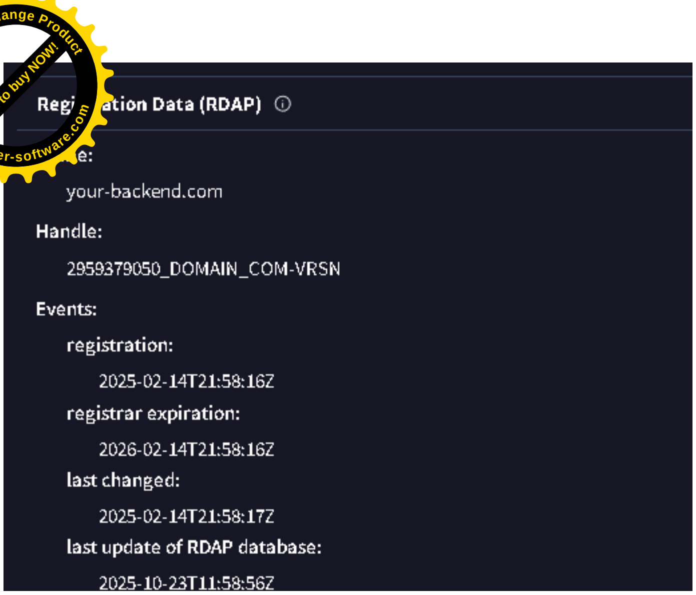
Input	Threat Level	Actions
gu.pak.CHEF@SUCKMYCHOCOLATESALTYBALLS.DOGE.GOV 9c5693ab00073c86e1774bd641eb950d545b55e0ddb2e917d420ea88be617308	no specific threat	↗
ADO210.CHM.CHEF@SUCKMYCHOCOLATESALTYBALLS.DOGE.GOV ac6933624a64785a98d606b42d330b1c06d2356fe08a29b89dda654ee7db2d85	no specific threat	↗
bn.pak.CHEF@SUCKMYCHOCOLATESALTYBALLS.DOGE.GOV b89bf4c910397cff16982dcf17255149c2ec9a57adf9a7fa38f5048356f05a10	no specific threat	↗
README_DOGE_BIGBALLS.TXT d97c55886e354dde8461968820826c2476f0305c69d755870e1be6d7ff1b6a97	no specific threat	↗
icudtl.dat.CHEF@SUCKMYCHOCOLATESALTYBALLS.DOGE.GOV ff72224459dc5a377e56fd9b00a44c779fc1c0f85398c3052d94fab367fd6822	no specific threat	↗

test.exe contacts one domain which I thought was a joke but look at reg date



DNS Requests

Domain	Address	Registrar	Country
your-backend.com	-	Spaceship, Inc. Organization: Privacy service provided by Withheld for Privacy ehf Name Server: elma.ns.cloudflare.com Creation Date: 2025-02-14T21:58:16	-

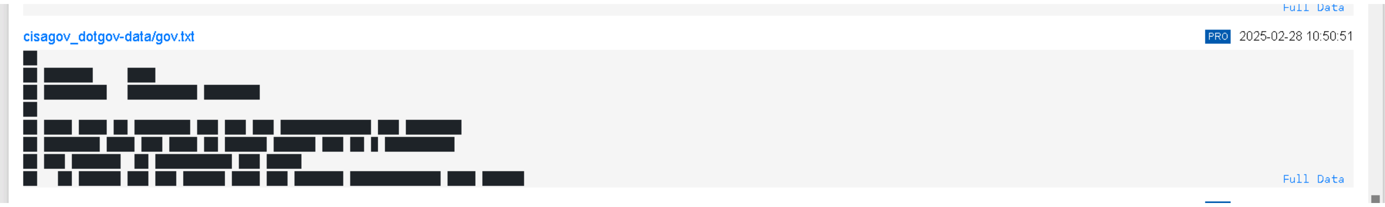


```
Registration Data (RDAP)
Name:
    your-backend.com
Handle:
    2959379050_DOMAIN_COM-VRSN
Events:
    registration:
        2025-02-14T21:58:16Z
    registrar expiration:
        2026-02-14T21:58:16Z
    last changed:
        2025-02-14T21:58:17Z
    last update of RDAP database:
        2025-10-23T11:58:56Z
```

https://magrathea.endchan.net/qrbunker/thread/161567.html

2025-09-27 06:58:52

CISA Leak found on Intelx.io, 2/28/25



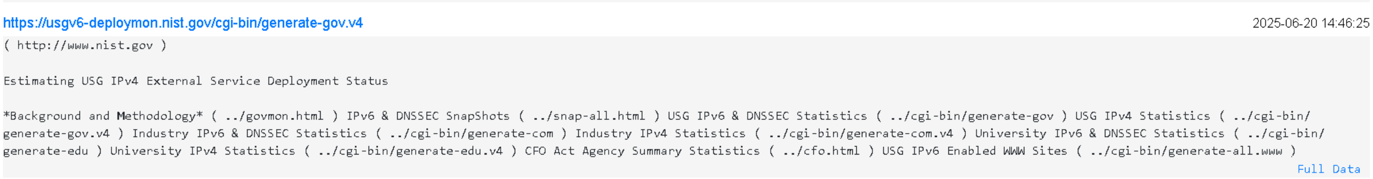
Full Data

cisagov_dotgov-data/gov.txt PRO 2025-02-28 10:50:51

[redacted]

Full Data

cisagov_dotgov-data/gov.txt



https://usgv6-deploymon.nist.gov/cgi-bin/generate-gov.v4 2025-06-20 14:46:25

```
( http://www.nist.gov )

Estimating USG IPv4 External Service Deployment Status

*Background and Methodology* ( ../govmon.html ) IPv6 & DNSSEC SnapShots ( ../snap-all.html ) USG IPv6 & DNSSEC Statistics ( ../cgi-bin/generate-gov ) USG IPv4 Statistics ( ../cgi-bin/
generate-gov.v4 ) Industry IPv6 & DNSSEC Statistics ( ../cgi-bin/generate-com ) Industry IPv4 Statistics ( ../cgi-bin/generate-com.v4 ) University IPv6 & DNSSEC Statistics ( ../cgi-bin/
generate-edu ) University IPv4 Statistics ( ../cgi-bin/generate-edu.v4 ) CFO Act Agency Summary Statistics ( ../cfo.html ) USG IPv6 Enabled WWW Sites ( ../cgi-bin/generate-all.www )
```

Full Data

Starlink and Russia article

- Starlink - Why do we care about Starlink? Andy Jenkinson-->

  Ukrainian deaths in 2022. Used a Russian talking point Zaporiphizhia to justify shutting down Starlink (WWIII!),
- then got the Verizon contract in July 2025, first day shut down Starlink

  leading to deaths in Ukraine, at a time where Ukraine was making advances.
- September 2025 - biggest attack by Russia of entire war. Another Starlink outage shutting down comms on Ukraine's entire frontline.

  Examples of Russian intel leaking?

- what is suspicious that we still don't understand?
  - link-spacex.com registered last March or May in China, ostensibly linked to Ugandan cell phone company, subdomains for Turkey, India, China, Russia, Ukraine.
  - Starlink Crimea https://bgp.he.net/AS204791#_prefixes

PDF-XChange Product
Click to buy NOW!
www.tracker-software.com

ow much $$$ Dod in contracts, a lineup of timeline

2022

2024

Feb 2024 - Musk denies selling Starlink to Russia

The Guardian, Feb 11, 2024

https://www.theguardian.com/world/2024/feb/12/ukraine-accuses-russia-forces-using-elon-musk-starlink?utm_source=chatgpt.com

Newsweek, Feb 12, 2024 (response):

"There have been recorded cases of the use of these devices by the Russian occupiers," Andriy Yusov, a spokesperson for Kyiv's GUR, told Ukrainian outlet RBC in an article published on Saturday. "This is starting to take on a systemic nature," Yusov told the outlet.
Troops with Moscow's 83rd Assault Brigade are using Starlink to access the internet in hotspots in the eastern Donetsk region, including near the village of Klishchiivka and the town of Andriivka, the GUR said in a separate statement. Russia controls part of the Donetsk region.
SpaceX has repeatedly said it does "not do business of any kind with the Russian government or its military."
"Starlink is not active in Russia, meaning service will not work in that country," the company said in a statement. "SpaceX has never sold or marketed Starlink in Russia, nor has it shipped equipment to locations in Russia. If Russian stores are claiming to sell Starlink for service in that country, they are scamming their customers."

https://www.newsweek.com/elon-musk-false-reports-starlink-russia-ukraine-spacex-1869007

2025

July 2025

September 2025

Footnotes

2.
https://en.wikipedia.org/wiki/Starlink