

Iris Investigate Portal

User Guide / Workflows

domaintools.com

Product Overview

Iris Investigate

Investigative platform and API draws on 25+ years of current and historical data to enable seamless, efficient cyber investigations in an intuitive UI.

Comprehensive passive DNS data of real-time and historical global Internet infrastructure data.

- THREAT INTELLIGENCE & HUNTING
- FRAUD PREVENTION
- FORENSICS & INCIDENT RESPONSE
- BRAND PROTECTION
- ACTOR PROFILING
- SOC AUTOMATION



Getting Started

01 Account Activation

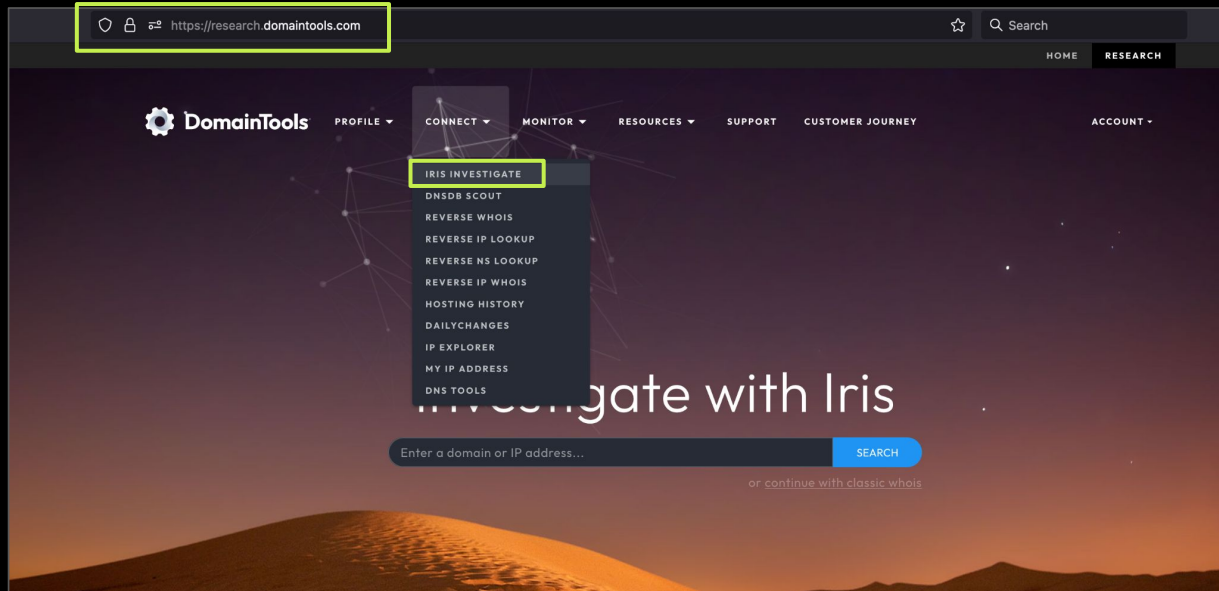
Users receive login email upon account creation.

02 Start Investigations

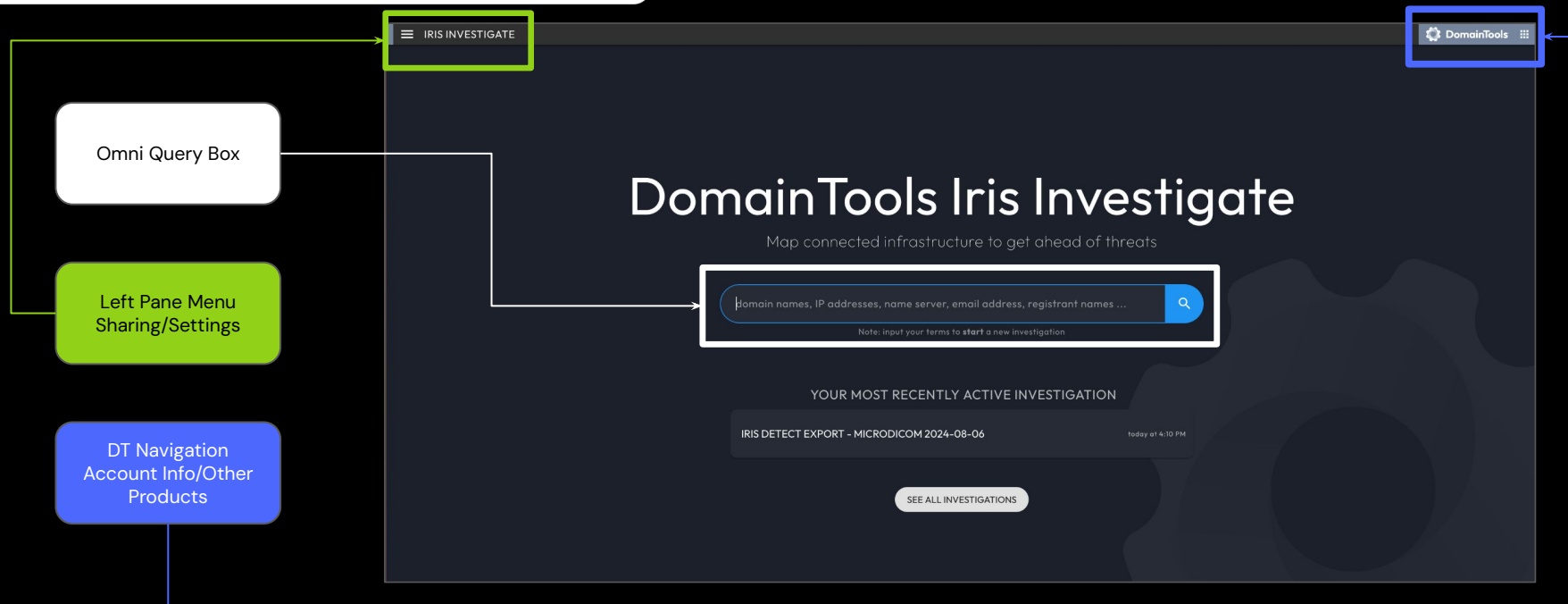
Iris Investigations can be started from the research home page with a single domain or IP address.

03 Direct Access

To access the platform directly, select 'Iris Investigate' under the 'Connect' menu.



Iris Investigate Home Page



Iris Investigate

Map connected infrastructure to get ahead of threats

domain names, IP addresses, name server, email address, registrant names ...



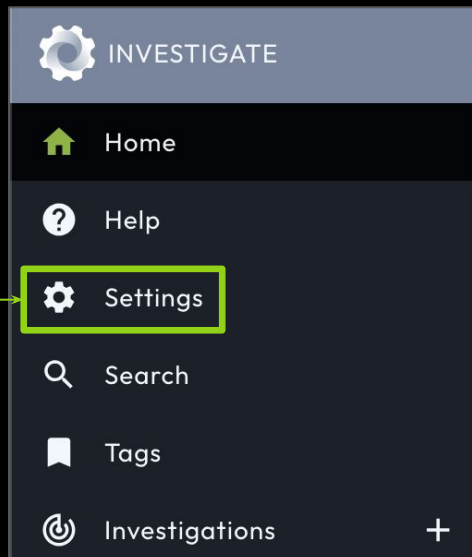
Note: input your terms to **start** a new investigation

Getting Started Tips

- 1000 character limit
- Supports multiple inputs (domains, IPs, x509, names, phone numbers, etc)
- Supports defanged URLs



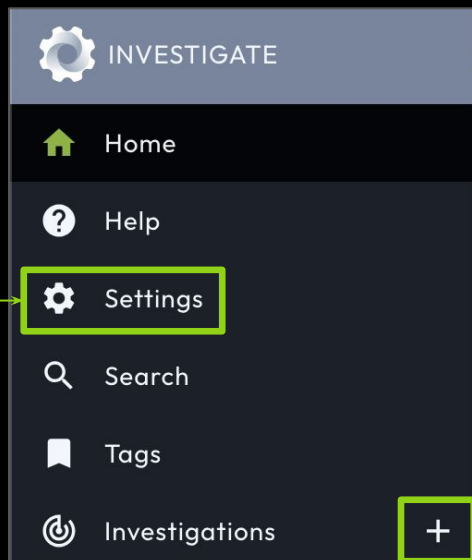
Iris Nav Pane Guide



Settings of Interest

- Dark Mode/Light Mode
- Pivot Engine Ordering (Prioritize views of DNS, x509, Whois, etc)
- Historical Search Toggle (match against current state or include Whois history)
- Guided Pivot Thresholds (UX indication of 'smaller' groupings for potential reverse pivots)

Iris Nav Pane Guide



Quick Facts

- Investigations & their queries are persistent, result sets may change as new data is collected
- Investigations can be shared across the account with read/write/edit options
- Investigations are not shareable beyond the account level
- Queries are exportable/shareable via 'Search Hashes'

The Pivot Engine

Pivot Engine										
99 Avg Risk 164 Avg Age				DOWNLOAD		Page 1 of 2 (568 records)				
☐	DOMAIN	RISK SCORE	TAGS	IP	CREATE DATE	WEBSITE TITLE	FIRST SEEN	REGISTRAR	NAME SERV	
☐	emergencyhelpnetwork.com	100		IP	ISP IP INFORMATION	ASN	CC	2025-03-01	Emergency Help Network	2025-03-01
	Q ₁ INSPECT			104.21.30.244	Q ₁ CloudFlare Inc.	13335	US	59 days old		9:19 AM
	3 GUIDED PIVOTS			172.67.131.189	Q ₁ CloudFlare Inc.	13335	US	2 months ago	IANA ID: 1068	jasmine.ns.c
										kellen.ns.clo
☐	communityreliefzone.com	100		IP	ISP IP INFORMATION	ASN	CC	2025-03-01	Community Relief Zone	2025-03-01
	Q ₁ INSPECT			104.21.80.1	Q ₁ CloudFlare Inc.	13335	US	59 days old		9:19 AM
	3 GUIDED PIVOTS			104.21.112.1	Q ₁ CloudFlare Inc.	13335	US	2 months ago	IANA ID: 1068	jasmine.ns.c
				104.21.96.1	Q ₁ CloudFlare Inc.	13335	US			
				104.21.32.1	Q ₁ CloudFlare Inc.	13335	US			kellen.ns.clo
				104.21.64.1	Q ₁ CloudFlare Inc.	13335	US			
				104.21.16.1	Q ₁ CloudFlare Inc.	13335	US			
				104.21.48.1	Q ₁ CloudFlare Inc.	13335	US			
☐	getemergencyaid.com	100		IP	ISP IP INFORMATION	ASN	CC	2025-03-01	Get Emergency Aid	2025-02-28
										NAMECHEAP INC
										HOSTNAM

The pivot engine shows the most recent data collected for any given domain in a scrollable, tabular format

The Right Click

Right-clicking on a data point in the pivot engine gives the reverse pivot count of that value across the Iris dataset (all tracked "Domains" like those seen on the left side here)

The screenshot displays the DomainTools interface with a pivot table. The table has columns for DOMAIN, RISK SCORE, TAGS, IP, and CREATE DATE. Two domains are listed: emergencyhelpnetwork.com and communityreliefzone.com. A right-click context menu is open over the 'communityreliefzone.com' row, showing a 'Filters' section with a 'NEW SEARCH' button and a 'Narrow Query' section with options: MATCHING, GREATER THAN, LESS THAN, and EXCLUDE. A highlighted message in the menu states: '~ 220,956 domains share this value.' Below this, there are two input fields for 'Date Created (RDAP)' and 'Date Created (Whois)', both containing the value '20250301'.

DOMAIN	RISK SCORE	TAGS	IP	CREATE DATE
emergencyhelpnetwork.com	100		104.21.10.244 172.67.131.189	2025-03-01 59 days old
communityreliefzone.com				2025-03-01 59 days old

Filters and Pivots

Filters

NEW SEARCH

Narrow Query

MATCHING

GREATER THAN

LESS THAN

EXCLUDE

Virtually any data point or any combination of data points can be the subject of a reverse lookup



Filters and Pivots

They can be complex and include many conditions

A screenshot of a complex search filter interface. It features a vertical stack of filter sections, each starting with an 'AND' button. The first section has a dropdown set to 'Auto', a dropdown set to 'IANA Id', and a text input field containing '1068'. The second section has a dropdown set to 'Auto', a dropdown set to 'Emails', and a text input field containing 'dns@cloudflare.com'. The third section has a dropdown set to 'TLD' and a dropdown set to 'Matches'. The fourth section has a dropdown set to 'Risk Score' and a dropdown set to 'Greater Than or Equal To', with a text input field containing '50'. The fifth section has a dropdown set to 'First Seen' and a dropdown set to 'Within', with a text input field containing 'the last day'. At the bottom, there is a summary bar that says 'ALL of these conditions are true' and a button labeled 'NARROW YOUR SEARCH'.

A screenshot of a search filter interface. It has a dropdown set to 'Auto', a dropdown set to 'Contact Street', and a dropdown set to 'Exactly Matches'. Below these is a text input field containing '17505 Telge Rd Ste 102 #245'. At the bottom right, there is a button labeled 'EXPAND YOUR SEARCH'.

Or highly targeted

A screenshot of a search filter interface. It has a dropdown set to 'Domain Name' and a dropdown set to 'Matches'. Below these is a text input field containing 'af.mil'.

Guided Pivots

yourfaceai.com

INSPECT

4 GUIDED PIVOTS

Found in 3 columns

- IP
- Website Title
- Trackers

IP	ISP IP INFORMATION	ASN	CC
13.51.8.70	Amazon Data Services Sweden	16509	SE

2025-03-21
39 days old

AI Photo & Video Generator | YourFace AI

Our interface will highlight most data fields that are connected to fewer than 500 domains by default.

These reverse pivots can be used to find tight correlations between domains in our dataset.

Guided Pivots

Admin

TEL:+1.9402081117

Filters

NARROW SEARCH

EXPAND SEARCH

NEW SEARCH

EXCLUDE

PHONE/FAX

P:tel:+1.3253059955

P:tel:+1.3253059955

P:tel:+1.9402081117

P:tel:+1.9402081117

P:tel:+1.9402081117

~ 117 domains share this value.

Contact Phone (RDAP)

tel:+1.9402081117

Contact Phone (Whois)

19402081117

117 domains

105 domains

Right-clicking on a guided pivot will give you the option to look at the result set in our pivot preview pane.

You can then add the data point to your query as a filter.

Contact Phone

tel:+1.9402081117

52 Avg Risk 116 Avg Age

☐	DOMAIN NAME	FIRST SEEN	RISK SCORE
☐	quickassistnet.com	2025-04-27	97
☐	nourishmealsupport.com	2025-04-26	34
☐	supporthouseworks.com	2025-04-26	100
☐	helpsportshub.com	2025-04-26	59
☐	housinghelpandsupportnetwork2025-04-18	2025-04-18	34
☐	aidwithgroceries.com	2025-04-16	34
☐	totalhouseaid.com	2025-04-16	34
☐	healthemergencyaid.com	2025-04-15	67
☐	foodhelpproject.com	2025-04-12	34
☐	communitygrocerhelp.com	2025-04-12	82
☐	familyfirstresources.com	2025-04-08	34
☐	myagreedailytrivia.com	2025-04-01	35
☐	securehousingrelief.com	2025-03-13	62
☐	playassistnetwork.com	2025-03-13	43
☐	householdaidnetwork.com	2025-03-13	34
☐	gethelpfastassist.com	2025-03-13	34
☐	fitnesshelpassist.com	2025-03-13	34

ALL (117)

COMMON (17)

MISSING (100)

NEW

EXPAND

NARROW

EXCLUDE

Historical Data

Iris gives you access to our historical data:

- Screenshots (2002-present)
- Whois (2001-present)
- DNS (2006-2021)
- pDNS (2010-present)
- DNS, x509, website data, Whois/RDAP (2021-present)

Passive DNS

pDNS

Scope: Apex+Subdomains Query: *.af.mil

SEARCH BY QUERY SEARCH

Record Type: A Source: All Result Limit: 500 After Date: mm / dd / yyyy Before Date: mm / dd / yyyy CLEAR

		TYPE	SOURCE	COUNT	RESPONSE	FIRST SEEN	LAST SEEN	DURATION
C								
w		A	D	1	214.48.248.245	2025-04-28, 12:09	2025-04-28, 12:09	1s
w		A	D	1	214.48.244.245	2025-04-23, 08:52	2025-04-23, 08:52	1s
w		A	C	1	23.50.154.37	2025-04-14, 01:02	2025-04-14, 01:02	1s
w		A	C	1	184.51.232.143	2025-04-14, 01:02	2025-04-14, 01:02	1s
w		A	C	1	104.66.126.140	2024-04-11, 14:08	2024-04-11, 14:08	1s
b		A	B	376	127.0.0.1	2024-03-15, 11:05	2025-04-28, 08:54	1y 43d 21h
b		A	D	3215226	127.0.0.1	2024-03-15, 10:02	2025-04-28, 08:48	1y 43d 22h
	www.af.mil	A	C	1	184.85.149.5	2024-03-03, 22:14	2024-03-03, 22:14	1s

The pDNS pane allows users to view the observed DNS queries for a given name or network over the last 15 years.

Passive DNS

pDNS

Scope: Apex Only Query: af.mil SEARCH BY QUERY SEARCH

Record Type: NS Source: D Result Limit: 500 After Date: mm / dd / yyyy Before Date: mm / dd / yyyy CLEAR

QUERY	TYPE	SOURCE	COUNT	RESPONSE	FIRST SEEN	LAST SEEN	DURATION
af.mil	NS	D	14334623	gunter-ns2.afnoc.af.mil.	2021-10-13, 11:13	2025-04-29, 05:54	3y 198d 18h
af.mil	NS	D	14334623	hickam-ns2.afnoc.af.mil.	2021-10-13, 11:13	2025-04-29, 05:54	3y 198d 18h
af.mil	NS	D	14334623	yokota-ns10.afnoc.af.mil.	2021-10-13, 11:13	2025-04-29, 05:54	3y 198d 18h
af.mil	NS	D	14334623	lackland-ns2.afnoc.af.mil.	2021-10-13, 11:13	2025-04-29, 05:54	3y 198d 18h
af.mil	NS	D	14334623	ramstein-ns2.afnoc.af.mil.	2021-10-13, 11:13	2025-04-29, 05:54	3y 198d 18h
af.mil	NS	D	35665	wpafb-ns10.afnoc.af.mil.	2021-07-12, 11:06	2021-07-21, 11:37	9d 31m 24s
af.mil	NS	D	1132290	hickam-ns10.afnoc.af.mil.	2020-09-30, 10:35	2021-07-12, 11:04	285d 1h 5m
af.mil	NS	D	7711081	scott-ns10.afnoc.af.mil.	2019-09-25, 12:00	2020-09-30, 11:11	1y 5d 23h
af.mil	NS	D	2	ramstein-014s10.afnoc.af.mil.	2020-02-22, 15:23	2020-02-22, 15:23	1s
af.mil	NS	D	37140	osan-ns10.afnoc.af.mil.	2014-04-23, 07:14	2014-04-25, 11:58	2d 4h 44m
af.mil	NS	D	37140	scott-ns1.afnoc.af.mil.	2014-04-23, 07:14	2014-04-25, 11:58	2d 4h 44m
af.mil	NS	D	37140	beale-ns10.afnoc.af.mil.	2014-04-23, 07:14	2014-04-25, 11:58	2d 4h 44m
af.mil	NS	D	37140	langley-ns10.afnoc.af.mil.	2014-04-23, 07:14	2014-04-25, 11:58	2d 4h 44m

Here are current/historical NS queries and answers for af.mil:

- **Scope:** Apex domain af.mil
- **Record Type:** Nameserver
- **Source:** D (DNSDB)
- **Count:** Number of observed cache misses between first/last seen dates

Example Usage

Example Usage


Blog

Threat Intelligence

Windows Remote Desktop Protocol: Remote to Rogue

April 7, 2025

Google Threat Intelligence Group

When executed, this configuration file initiates an RDP connection to the malicious command-and-control (C2 or C&C) server `eu-southeast-1-aws[.]govtr[.]cloud` and redirects all drives, printers, COM ports, smart cards, WebAuthn requests (e.g., security key), clipboard, and point-of-sale (POS) devices to the C2 server.

<https://cloud.google.com/blog/topics/threat-intelligence/windows-rogue-remote-desktop-protocol>

Example Usage

Starting with apex domain
for the command and
control server.



The screenshot shows the DomainTools Iris Investigate interface. At the top, it says "DomainTools" and "Iris Investigate". Below that, it says "Map connected infrastructure to get ahead of threats". There is a search bar with "govtr.cloud" entered. A green box highlights the search bar, and a line points from the text "Starting with apex domain for the command and control server." to it. Below the search bar, there is a note: "Note: input your terms to **start** a new investigation".

Example Usage

Pivot Engine 									
100 Avg Risk		258 Avg Age		 DOWNLOAD		< Page 1 of 1 (1 record)			
☐	DOMAIN	FIRST SEEN ▾	REGISTRAR	NAME SERVER		SSL INFORMATION			
☐	govtr.cloud  INSPECT	2024-08-15 10:14 PM 8 months ago	NameSilo, LLC IANA ID: 1479	HOSTNAME	IP INFORMATION	HASH	SUBJECT	ALT NAMES	ISSUER COMMON NAME
				ns3.dnsowl.com	162.159.26.234 	da3fe726a3... 	CN=govtr.cloud	govtr.cloud	Encryption Everywhere DV TLS CA - G2
					162.159.27.98 				
				ns1.dnsowl.com	162.159.27.173 	c7c4a463fe... 	CN=govtr.cloud	*.govtr.cloud	E5
					162.159.26.136 			govtr.cloud	
				ns2.dnsowl.com	162.159.26.49 				
					162.159.27.130 				

DomainTools discovered
this domain on 8/15/2024.

Additional Hosting IPv4s

Domain History govtr.cloud				
DATE	FIELD	PREVIOUS VALUE		NEW VALUE
2024-10-19 7:45 AM	IP Address	3.94.204.138 (US) (AS14618) Amazon Data Services NoVa		185.76.79.118 (US) (AS9009) EDIS GmbH
2024-09-24 3:28 AM	IP Address	91.195.240.123 (DE) (AS47846) Sedo GmbH		3.94.204.138 (US) (AS14618) Amazon Data Services NoVa

Observed hosting
infrastructure via DT lookups +
Domain History

Observed FQDNs in DNS on
DNSDB passive DNS network

Query * 185.76.79.118								SEARCH
Record Type	Source	Result Limit	After Date	Before Date				
All	D	500	mm / dd / yyyy	mm / dd / yyyy				
QUERY	TYPE	SOURCE	COUNT	RESPONSE	FIRST SEEN	LAST SEEN	DURATION	
data.govtr.cloud	A	D	3	185.76.79.118	2025-01-13, 21:19	2025-01-25, 14:08	11d 16h 49m	
monitoring.govtr.cloud	A	D	1	185.76.79.118	2025-01-13, 21:19	2025-01-13, 21:19	1s	
www.eu-southeast-1-aws.govtr.cloud	A	D	6	185.76.79.118	2024-11-25, 01:19	2024-12-23, 03:04	28d 2h 21m	
*.govtr.cloud	A	D	5	185.76.79.118	2024-11-03, 12:25	2025-04-01, 20:05	149d 6h 39m	
www.govtr.cloud	A	D	16	185.76.79.118	2024-10-26, 10:38	2025-03-03, 08:56	127d 23h 17m	
eu-southeast-1-aws.govtr.cloud	A	D	421	185.76.79.118	2024-10-23, 02:18	2025-04-28, 03:33	187d 1h 15m	

Wildcard Searching in Passive DNS

pDNS

Scope: Apex Only Query: * eu-southeast-1-aws.* SEARCH BY QUERY SEARCH

Record Type: All Source: D Result Limit: 500 After Date: 01 / 01 / 2024 Before Date: mm / dd / yyyy CLEAR

QUERY	TYPE	SOURCE	COUNT	RESPONSE	FIRST SEEN	LAST SEEN
eu-southeast-1-aws.barx.cloud	A	D	16	54.254.211.1	2024-11-01, 02:56	2025-04-11, 07:2
eu-southeast-1-aws.gov-sk.cloud	A	D	95749	185.216.72.196	2024-10-30, 19:16	2025-04-29, 10:3
eu-southeast-1-aws.mzv-cz.cloud	A	D	94303	2.58.203.61	2024-10-30, 19:16	2025-04-29, 11:15
eu-southeast-1-aws.mzv-sk.cloud	A	D	46705	185.76.79.62	2024-10-30, 19:16	2025-04-28, 13:0
eu-southeast-1-aws.mindef-nl.cloud	A	D	93503	80.87.206.241	2024-10-30, 19:16	2025-04-28, 18:1
eu-southeast-1-aws.quirinale.cloud	A	D	47466	151.236.16.226	2024-10-30, 19:16	2025-04-29, 06:1
eu-southeast-1-aws.difesa-it.cloud	A	D	23854	151.236.16.220	2024-10-30, 16:53	2025-02-01, 18:4
eu-southeast-1-aws.msz-pl.cloud	A	D	94698	62.72.7.213	2024-10-30, 10:37	2025-04-29, 10:1
eu-southeast-1-aws.mil-pl.cloud	A	D	46823	93.188.163.16	2024-10-30, 10:23	2025-04-29, 05:1
eu-southeast-1-aws.amazonsolutions.cloud	A	D	135857	81.17.31.106	2024-10-30, 09:31	2025-04-29, 09:1
eu-southeast-1-aws.dep-no.cloud	A	D	12342	212.1.213.198	2024-10-30, 09:22	2024-12-06, 00:1
eu-southeast-1-aws.ukrainesec.cloud	A	D	12561	5.133.9.252	2024-10-30, 08:05	2024-12-06, 00:1
eu-southeast-1-aws.gov-ua.cloud	A	D	735	173.255.204.62	2024-10-29, 18:52	2025-04-29, 03:1
eu-southeast-1-aws.govtr.cloud	A	D	421	185.76.79.118	2024-10-23, 02:18	2025-04-28, 03:1

Additional Domains using similar FQDN patterns:

- barx[.]cloud,
- dep-no[.]cloud,
- zero-trust[.]solutions,
- mindef-nl[.]cloud,
- mzv-sk[.]cloud,
- gov-sk[.]cloud,
- mil-pl[.]cloud,
- mzv-cz[.]cloud,
- msz-pl[.]cloud,
- quirinale[.]cloud,
- difesa-it[.]cloud,
- ukrainesec[.]cloud,
- amazonsolutions[.]cloud,
- govtr[.]cloud,
- gov-ua[.]cloud

DomainTools