DomainTools

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

DomainTools

Getting Started

01 Account Activation

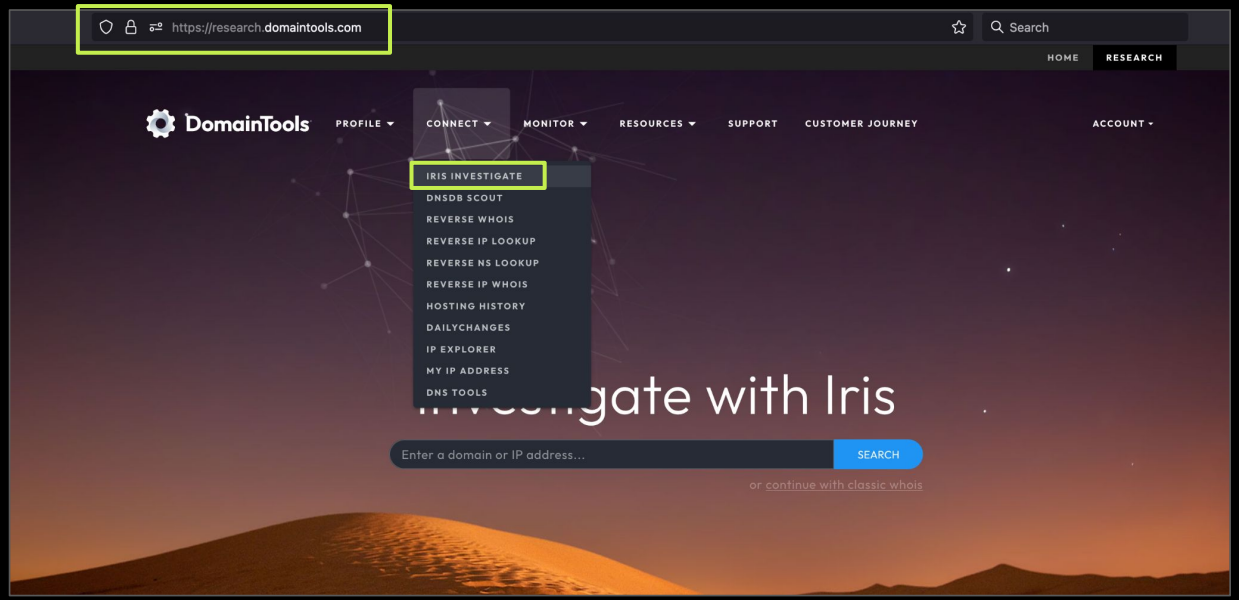
Users receive login email upon account creation.

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.



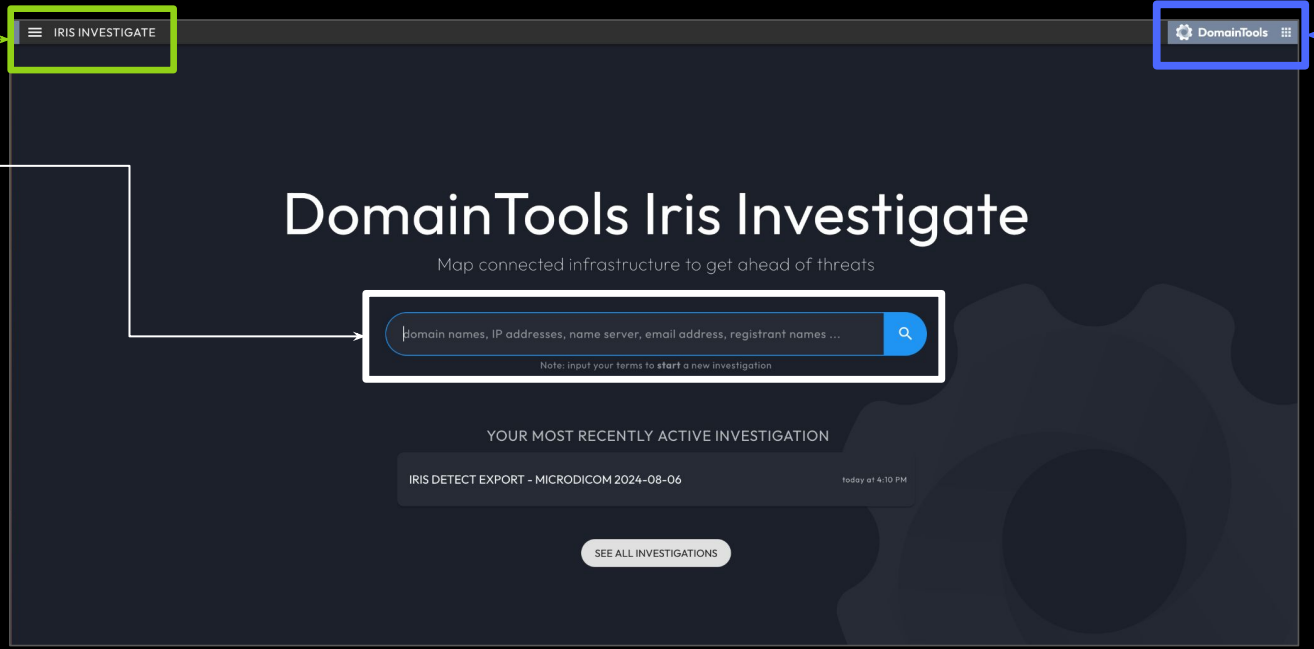
DomainTools

Iris Investigate Home Page

Omni Query Box

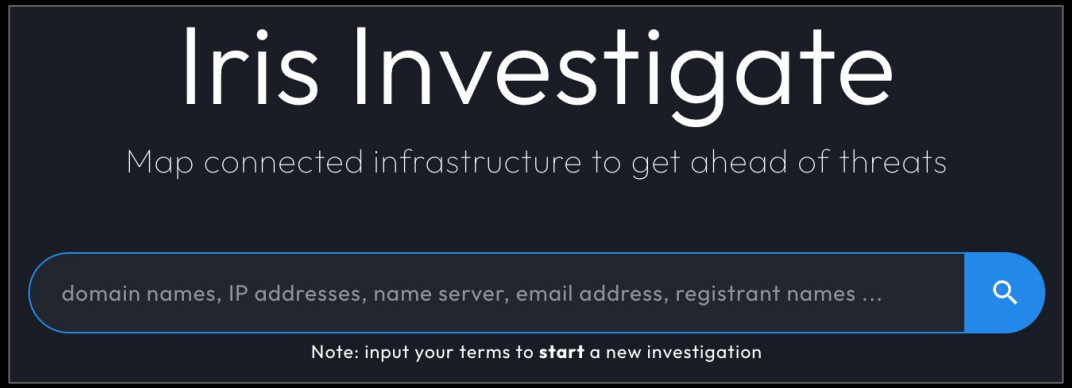
Left Pane Menu
Sharing/Settings

DT Navigation
Account Info/Other
Products



DomainTools

Omni Query Box

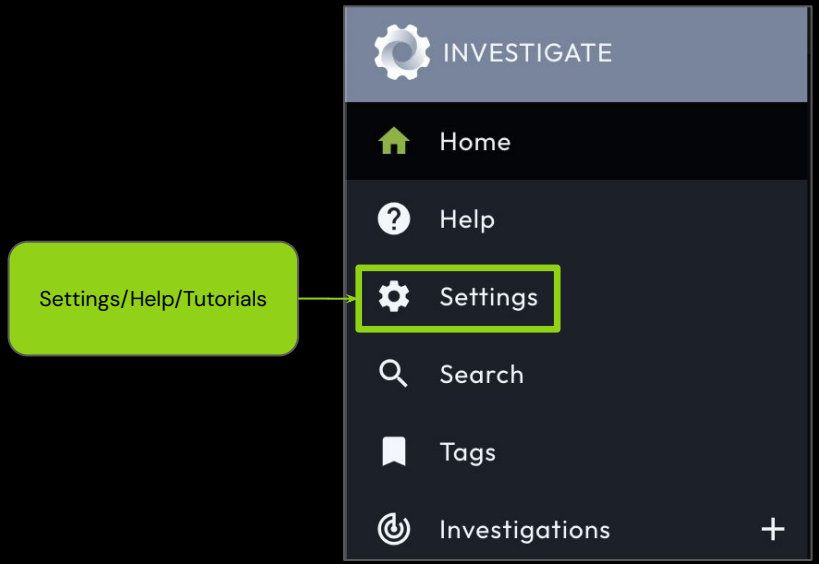


Getting Started Tips

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

DomainTools

Iris Nav Pane Guide

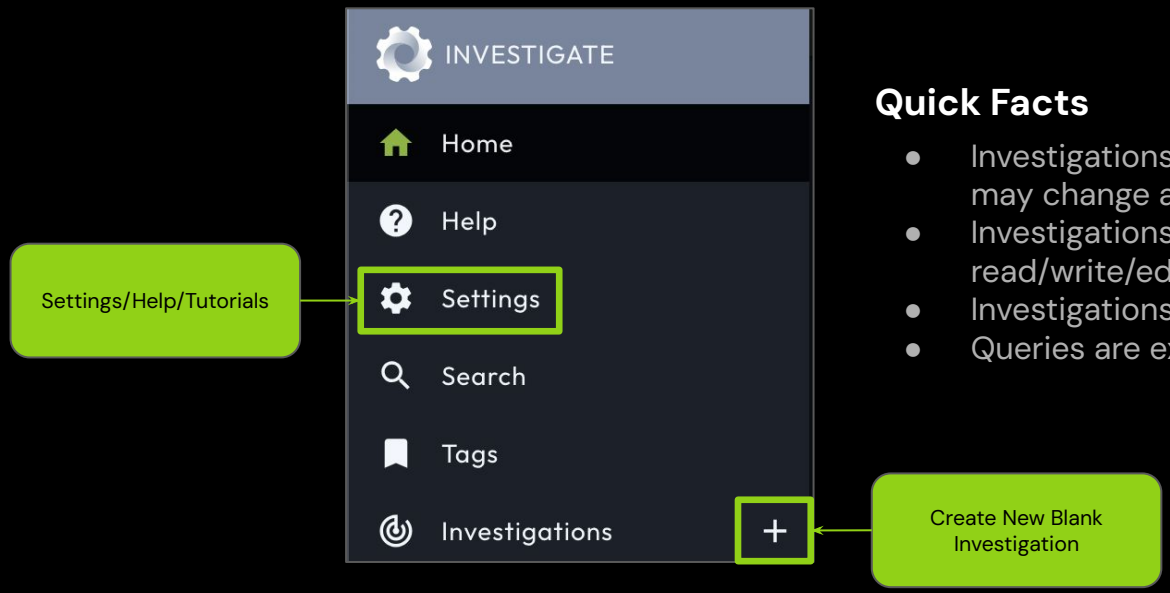


Settings of Interest

- 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)

DomainTools

Iris Nav Pane Guide

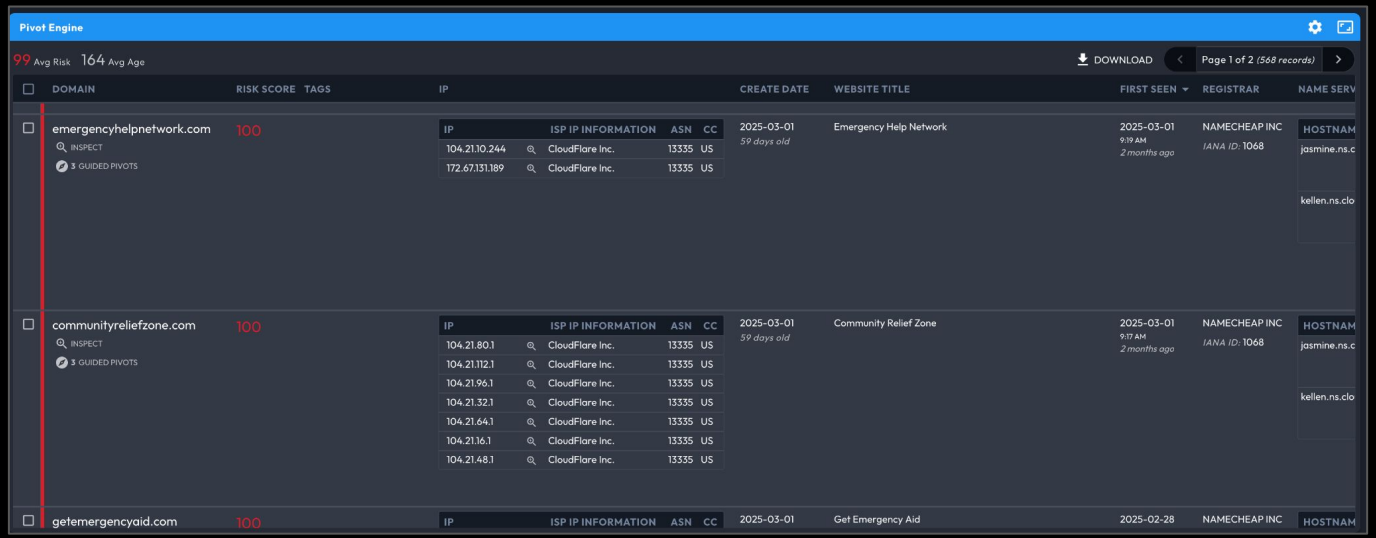


Quick Facts

- 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’

DomainTools

The Pivot Engine

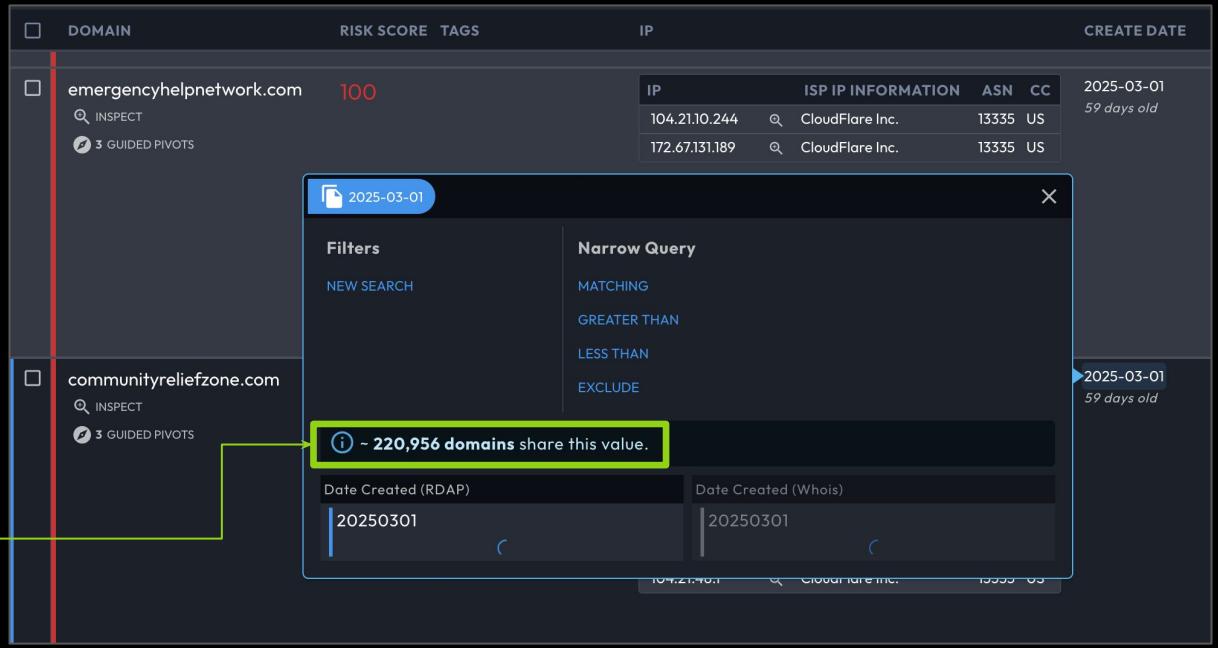


The pivot engine shows the most recent data collected for any given domain in a scrollable, tabular format

DomainTools

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)



DomainTools

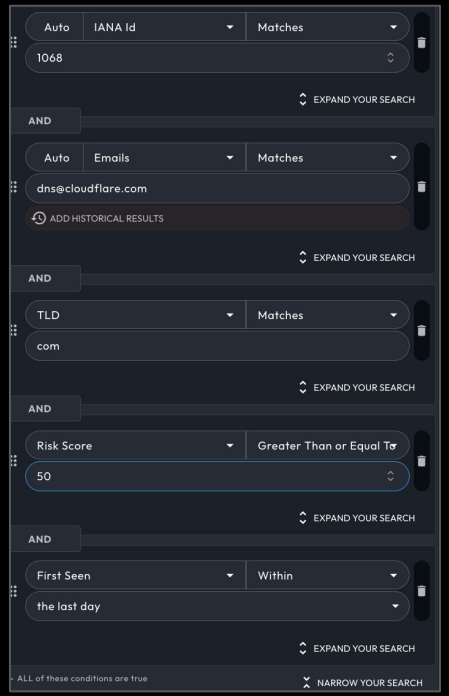
Filters and Pivots

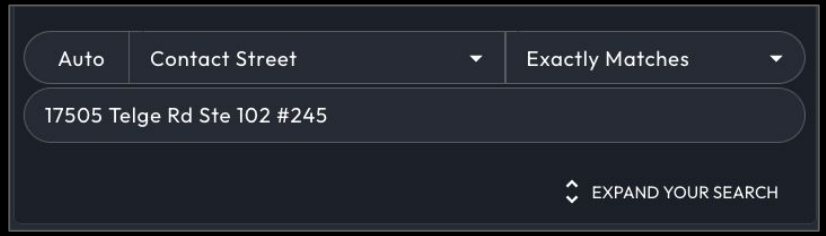
Virtually any data point or any combination of data points can be the subject of a reverse lookup

DomainTools

Filters and Pivots

They can be complex and include many conditions





Or highly targeted

DomainTools

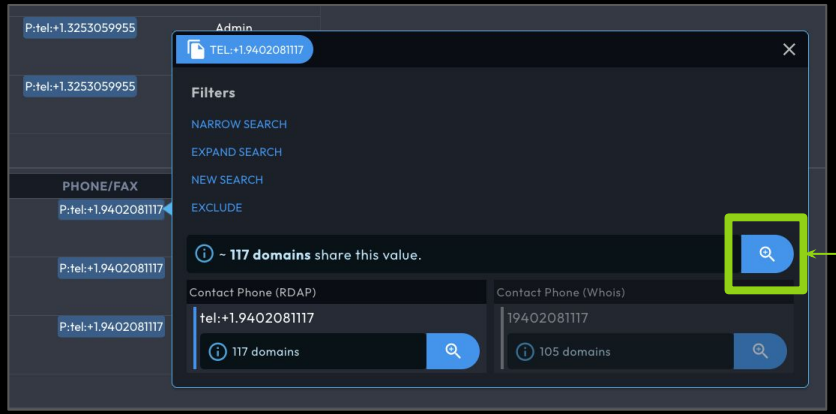
Guided Pivots

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.

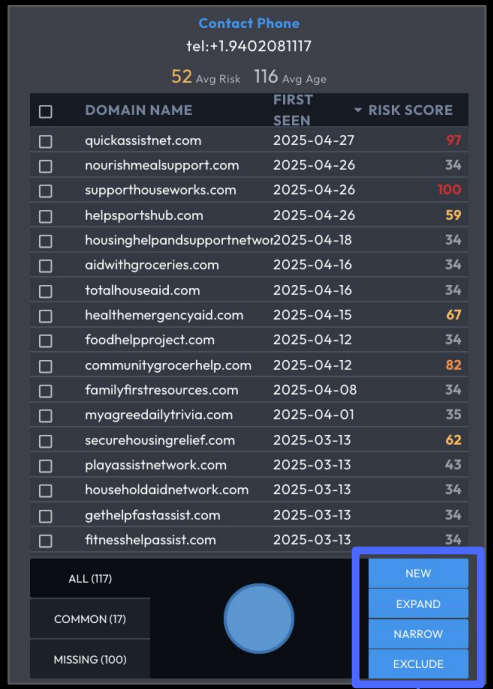
DomainTools

Guided Pivots



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.



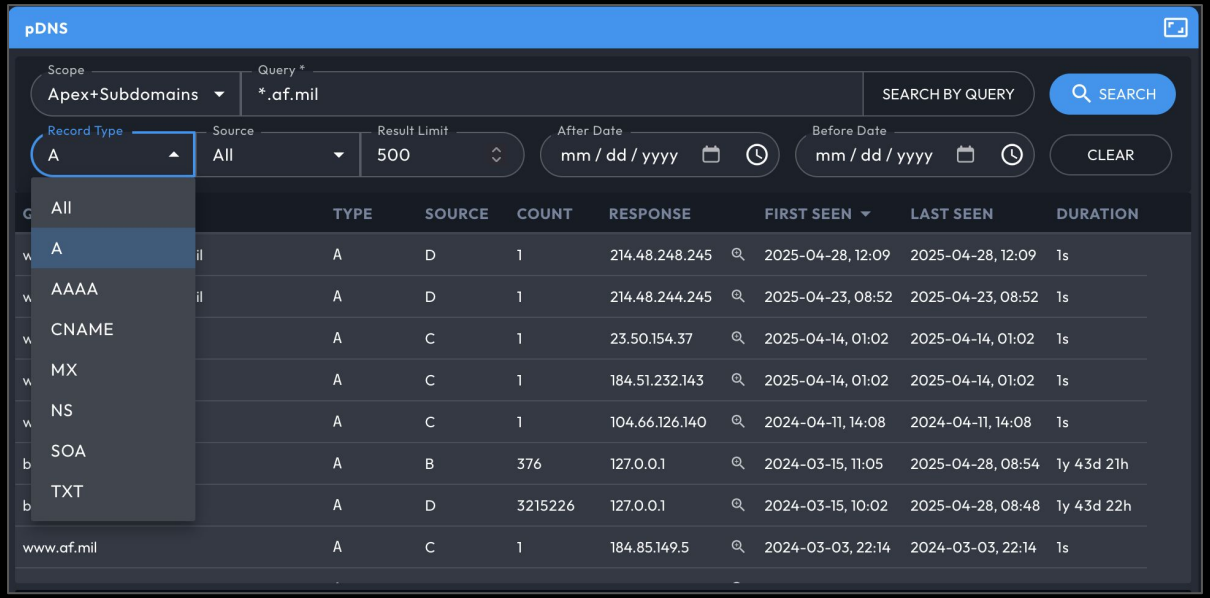
DomainTools

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)

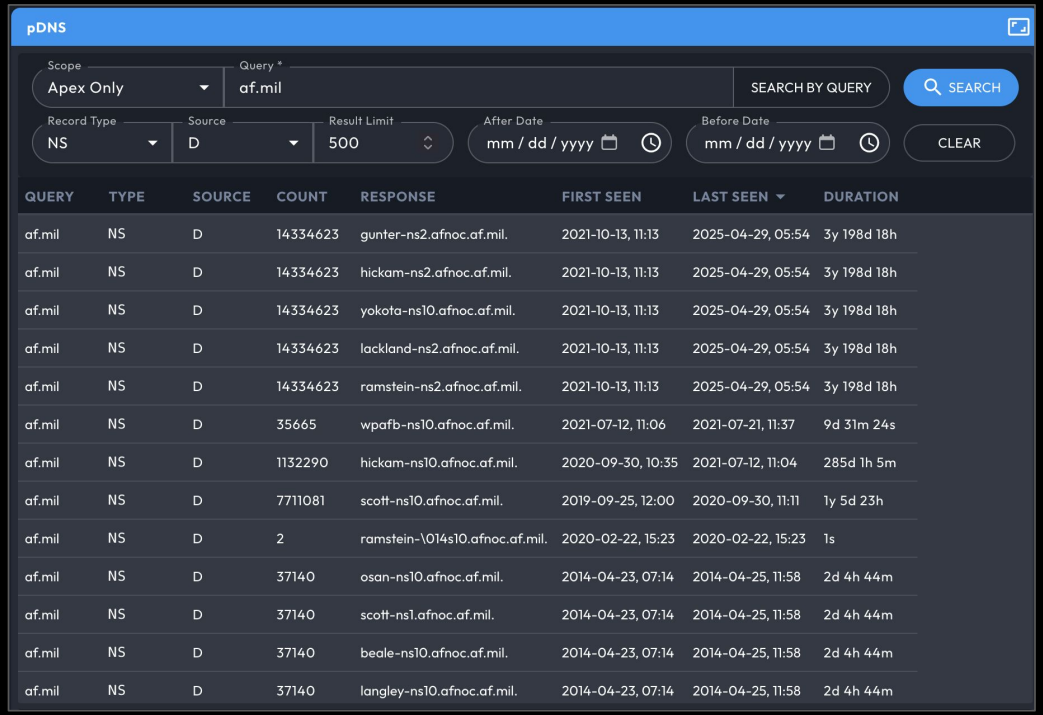
Passive DNS



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

DomainTools

Passive DNS



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

DomainTools

Example Usage

DomainTools

Example Usage

Google Cloud

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

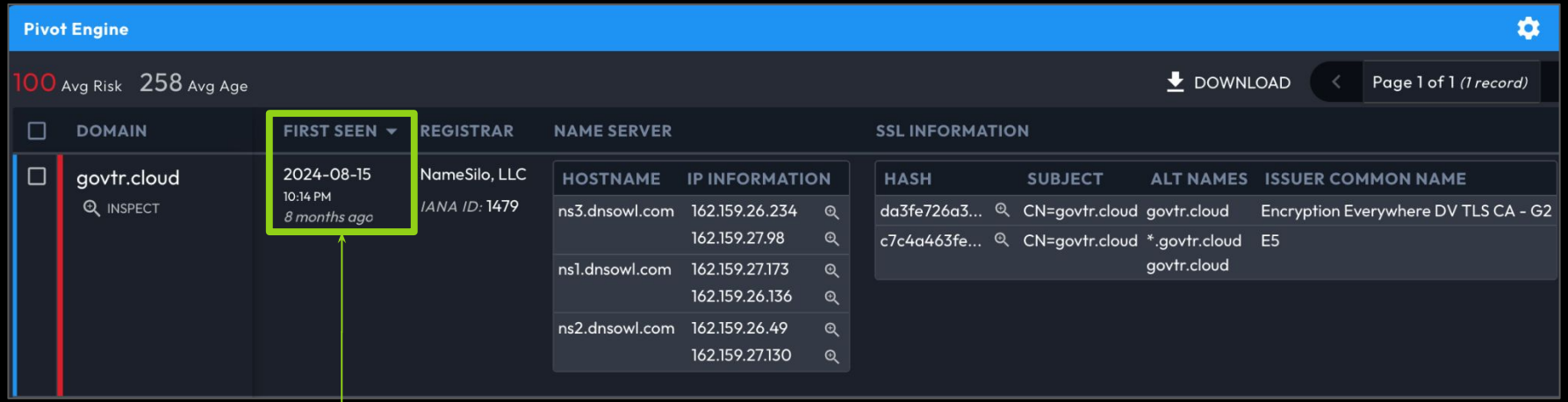
DomainTools

Example Usage

Starting with apex domain for the command and control server.

DomainTools

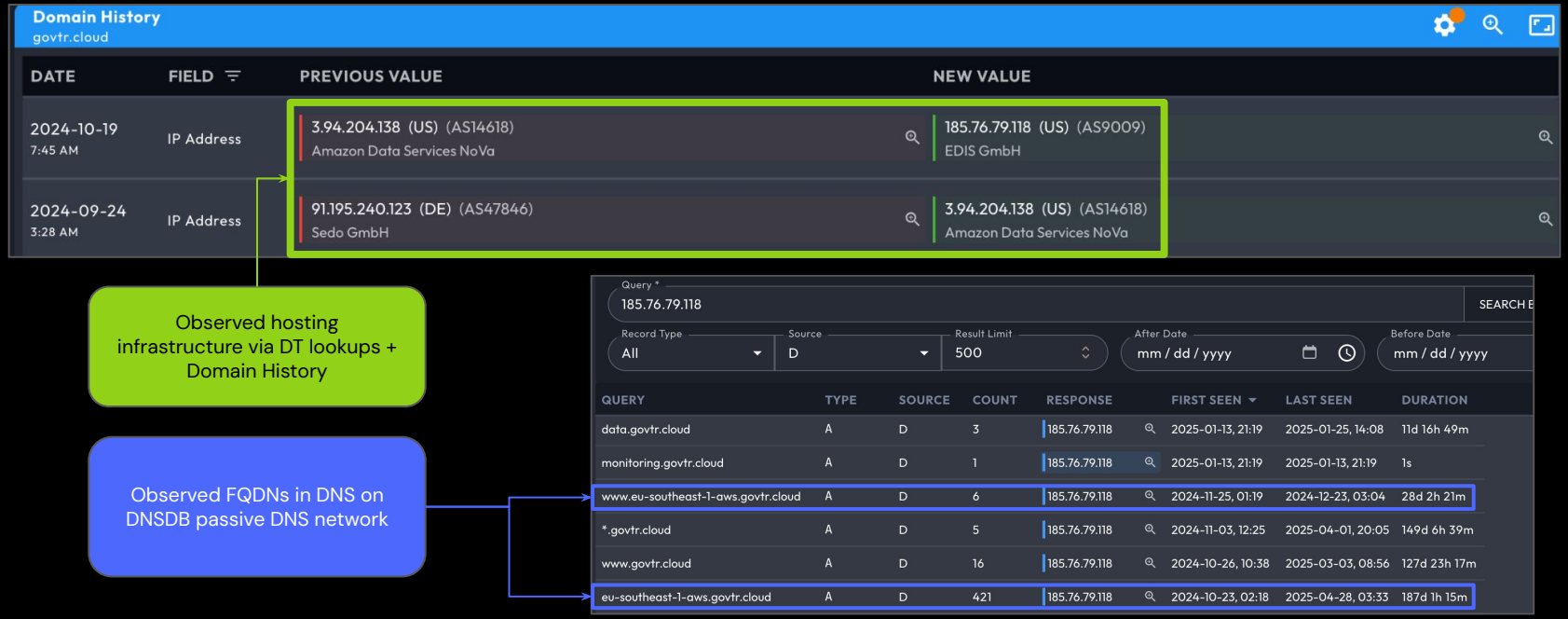
Example Usage



DomainTools discovered this domain on 8/15/2024.

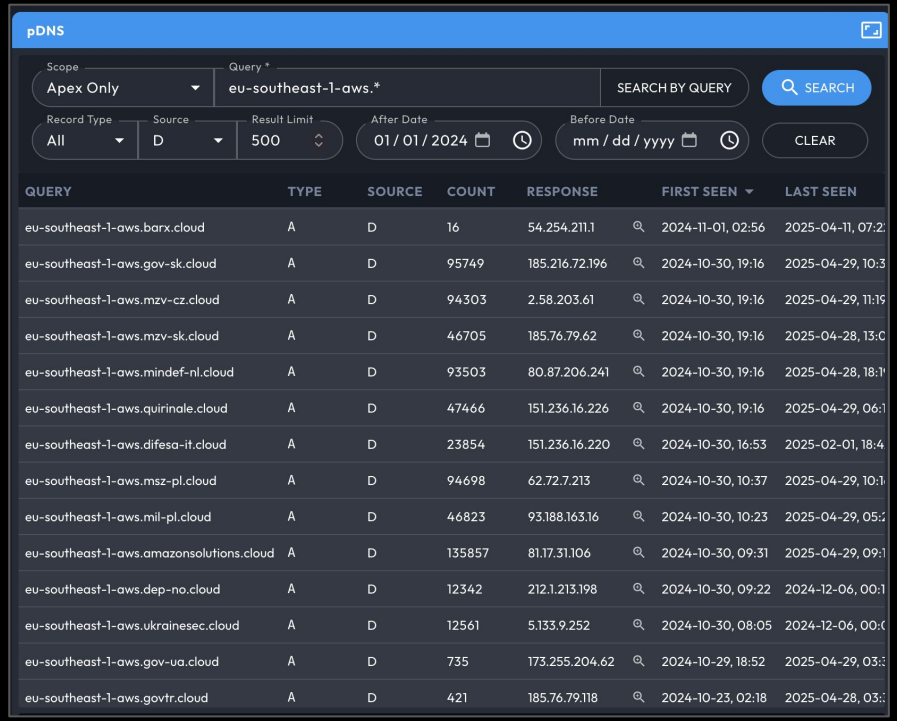
DomainTools

Additional Hosting IPv4s



DomainTools

Wildcard Searching in Passive DNS



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, 11:19
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, 05:2
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, 00:0
eu-southeast-1-aws.gov-ua.cloud	A	D	735	173.255.204.62	2024-10-29, 18:52	2025-04-29, 03:3
eu-southeast-1-aws.govtr.cloud	A	D	421	185.76.79.118	2024-10-23, 02:18	2025-04-28, 03:3

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


DomainTools