ICANN Domain Metrica & INFERMAL

Siôn Lloyd

ICANN OCTO-SSR

GAC: Discussion on DNS Abuse ICANN 82

March 2025

Agenda

ICANN Domain Metrica

INFERMAL project

What is ICANN Domain Metrica?

A system to **collect**, **combine** and **compare** any metadata related to domain names.

The platform has a **dynamic dashboard** with relevant **statistics** and visualisations; alongside an API to access raw data.

ICANN Domain Metrica

- Data and statistics for **gTLDs** and **registrars**
- **Searchable** for gTLDs, registrars and domains [get **Metadata** and statistics]
- Shareable **domain-level** data
- **Interactive visualisations** and comparisons [allows to filter on dates and add gTLDs to compare]
- **Abuse map** - abuse hosts geolocation [Maxmind data]
- **Domain Popularity Ranking** [Tranco list]

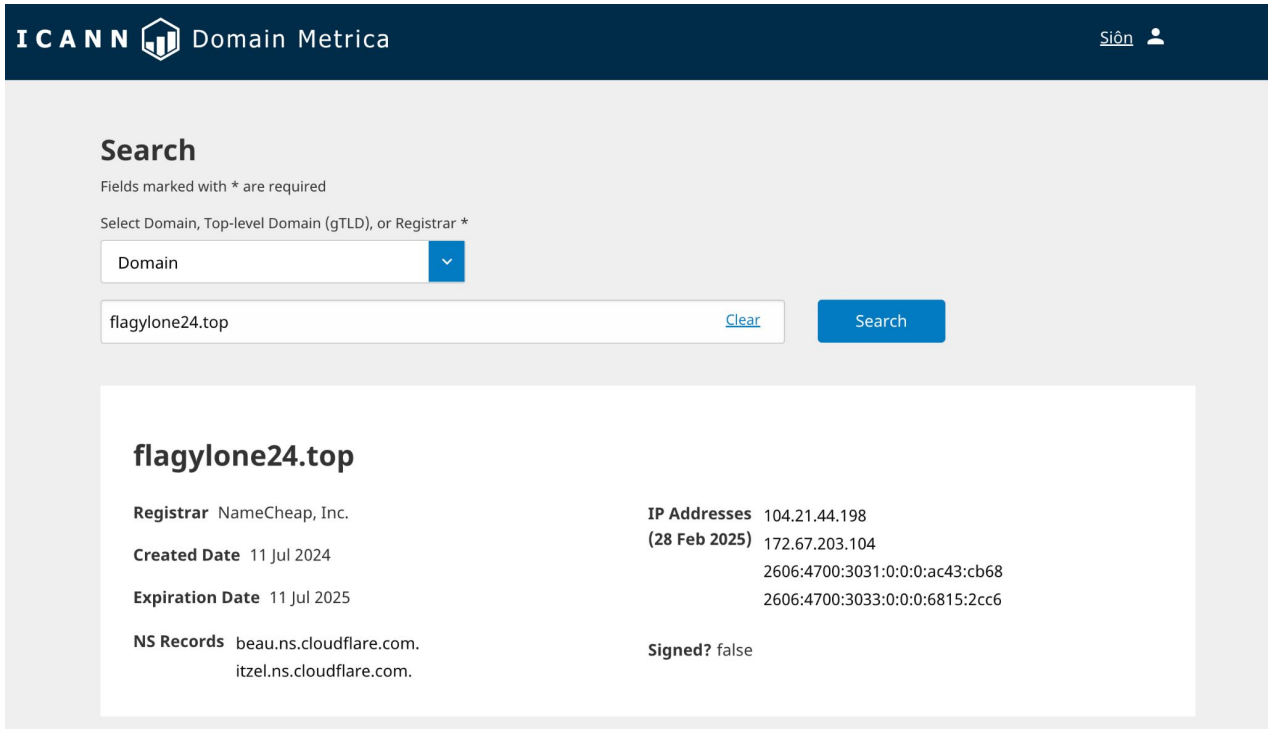
- MoSAPI
  - Access to lists of reported domains (contracted parties)
- A separate API for the rest of the ICANN community

ICANN Domain Metrica - Use Case I

We suspect the domain “flagylone24.top” to be involved with abuse

Search in the UI

Background



ICANN Domain Metrica - Use Case I

Current active reports

Current Reported Abuse

Last updated 06 Mar 2025

Summary of the latest reported abuse updated daily

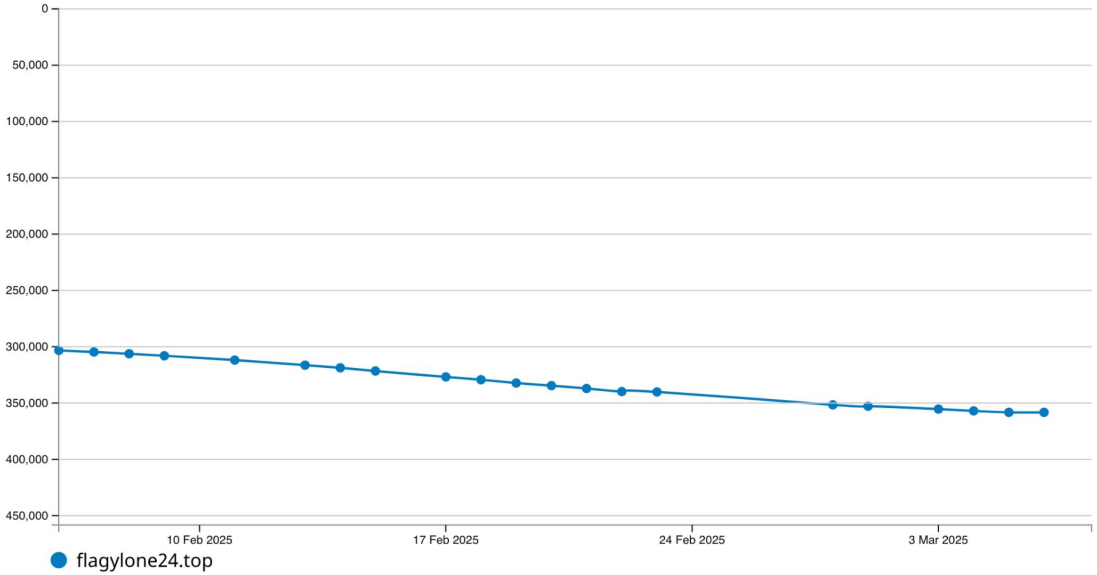
RBL Name	Reported Abuse Type	URL Count
surbl	Phishing	1

Popularity of domain

Tranco Popularity Ranking

A Research-Oriented Top Sites Ranking Hardened Against Manipulation

Click the chart title to download, compare, or change date range



ICANN Domain Metrica - Use Case II

What do we know about the TLD “com”?

Search in the UI

Select Domain, Top-level Domain (gTLD), or Registrar *

TLD

com Clear Search

Background

com

Last Updated 06 Mar 2025

Registry http://www.verisigninc.com

Type generic

Delegation Date no data available

Zone Size 154,482,406

Size Change (since 05 Mar 2025) +23,510

Number of Signed Delegations 6,359,930

Current Reported Abuse

Current Reported Abuse

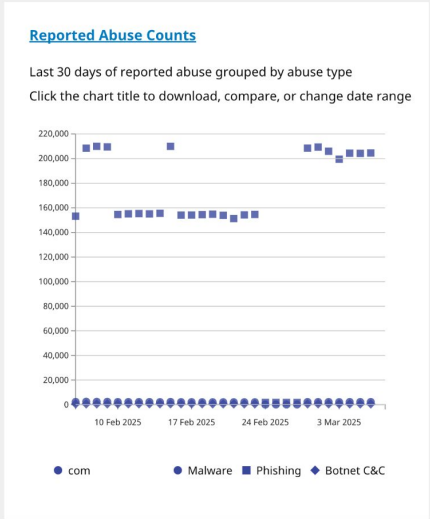
Last updated 06 Mar 2025

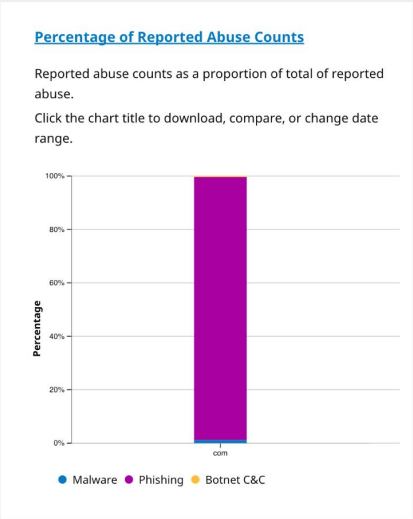
Summary of the latest reported abuse updated daily

Reported Abuse Type	Unique Domain Counts	Percentage of Total Zone Size
Phishing	204,574	0.132%
Malware	2,158	0.001%
Botnet C&c	555	0.000%

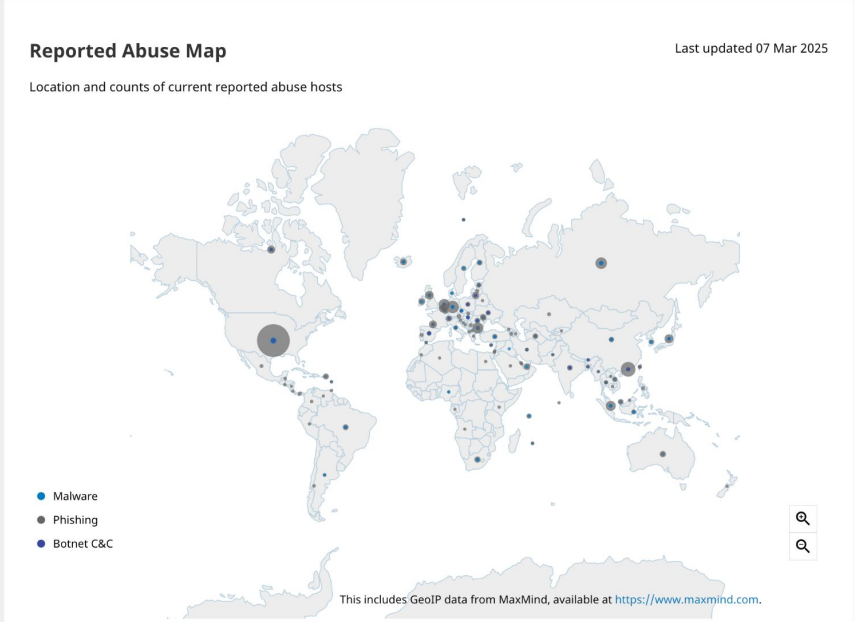
ICANN Domain Metrica - Use Case II

Reported Abuse Trends





Hosting locations



ICANN Domain Metrica

RBL Name: Select

Reported Abuse Type: Select

Reset

CSV | JSON

Note: the list shown here will not contain all reported domains. The number of results we can return is limited by our license agreements, we also only display fresh reports, that is, reports first seen in the previous 7 days. See the FAQ for more details.

1 - 20 of 446 results

Last updated 06 March 2025

Domain	RBL Name	Reported Abuse Type	URL Count
[illegible]	spamhaus	Botnet C&C	1
[illegible]	spamhaus	Botnet C&C	1
[illegible]	surbl	Malware	1
[illegible]	spamhaus	Malware	1
[illegible]	spamhaus	Malware	1
[illegible]	spamhaus	Malware	1
[illegible]	surbl	Phishing	1
[illegible]	surbl	Phishing	1
[illegible]	surbl	Phishing	1
[illegible]	surbl	Phishing	1
[illegible]	surbl	Phishing	1
[illegible]	surbl	Phishing	1
[illegible]	surbl	Phishing	1
[illegible]	surbl	Phishing	1
[illegible]	surbl	Phishing	1
[illegible]	surbl	Phishing	1
[illegible]	surbl	Phishing	1
[illegible]	surbl	Phishing	1
[illegible]	surbl	Phishing	1

‹ Previous 1 2 3 4 5 6 7 8 9 10 Next ›

Shareable **domain-level** data

(For registry and registrar users only)

ICANN Domain Metrica

- Domain Metrica is not “finished”
  - It is planned to evolve through its existence
  - Reflect feedback, new use cases, *etc.*
  - Build on what we have

- Yearly evaluation of the inputs lists we use [using our RBL evaluation methodology **OCTO037**]

Want to know more?

Metrica homepage:
https://www.icann.org/octo-ssr/metrica-en

DASC webinar on ICANN Domain Metrica (4 December 2024):
https://community.icann.org/display/ccnsowkspc/ccNSO+Webinars

INFERMAL

Inferential Analysis of Maliciously Registered Domains

INFERMAL

A project funded by ICANN

Led by Professor Maciej Korczyński (KOR Labs / Université Grenoble Alpes)

Looked at registration policies to reveal patterns in attacker preferences at TLD-registrar level

Final report was published in November 2024

More details and further links can be found at:
https://www.icann.org/resources/pages/inferential-analysis-maliciously-registered-domains-infermal-2024-12-03-en

INFERMAL

Features examined included Registration Attributes, *e.g.*:

- Pricing
  - Cost of registration
- Discounts
  - Fixed or percentage reduction in advertised cost, *e.g.* on “bulk” registrations
- Bulk registration facilities
  - Ability to search multiple domains in one interaction
- Free API availability
  - How much automation is possible (without subscription)
- Payment methods
  - Cryptocurrency, pay-pal, *etc.*
- Free services
  - Web hosting, email, TLS certificates, *etc.*

…

INFERMAL

And also Verification and security practices, *e.g.*:

- Validation of contact details
  - *e.g.* email/physical address, phone number checked **before** domain purchase
- Registration restrictions
  - *e.g.* any documentation required, local presence
- Domain string check
  - *e.g.* attempt to register “office365-my-account”

- Measure domain “uptimes”
  - how long to reported domains remain active (reactive measure)

INFERMAL

Datasets

- Phishing
  - APWG, PhishTank, OpenPhish
- Benign domain names
  - ICANN CZDS, Google CT logs, etc.
- Features
  - TLD-List (*e.g.*, domain registration costs, discounts, free features) *
  - Manually collected data (*e.g.*, free API, API create user account, API register domain, restrictions)
  - Active measurements (uptimes)
- Active WHOIS and DNS measurements

* https://tld-list.com/

INFERMAL

Strongest correlations with **increasing** abuse were

- Free API availability
- Free DNS / hosting
- Registration discounts

Strongest correlations with **decreasing** abuse were

- Validation on email address / phone number
- Presence of registration restrictions

Likely that attractiveness to attackers results from a combination of factors.

Essential to consider economic implications, impact on legitimate users and the likely response of attackers to adjustments.

We would like to extend our thanks to Professor Maciej Korczyński and his team.

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg