ICANN 81 ANNUAL GENERAL MEETING

Domain Name System (DNS) Abuse Updates

ICANN 81 Annual General Meeting
Istanbul, Türkiye

13 November 2024

Agenda

Topic	Time (Estimated Duration)	Speaker
Opening Remarks	13:15	ICANN GDS
Updates on Domain Metrica	13:15 (35 minutes)	ICANN OCTO
Updates on INFERMAL	13:35 (35 minutes)	ICANN OCTO - KOR Labs
Closing remarks	14:05	ICANN GDS

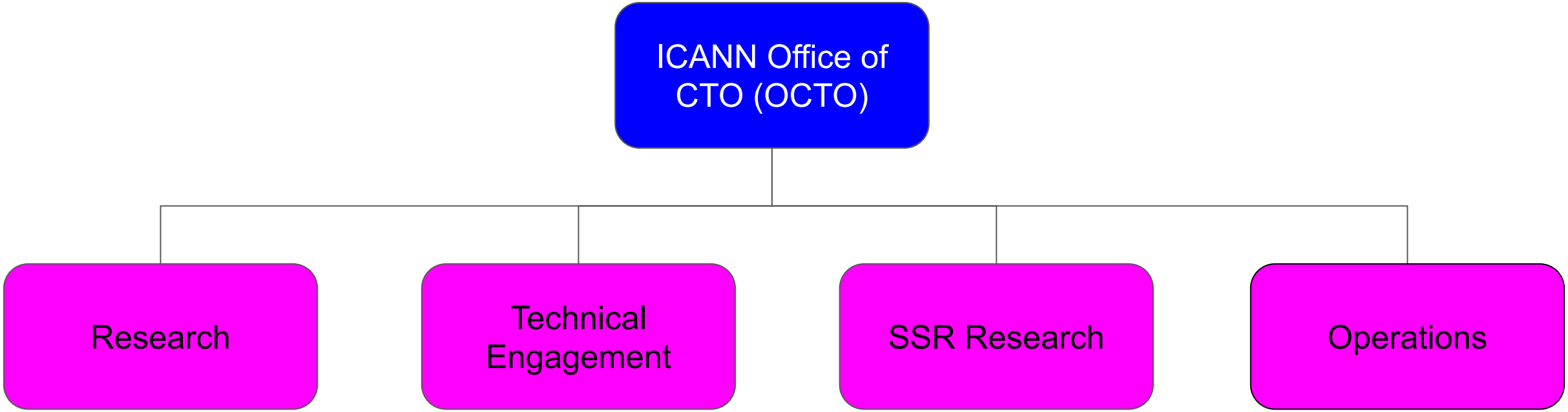
ICANN Domain Metrica

Dr. Siôn Lloyd
Dr. Samaneh Tajalizadehkhoob
SSR Research
ICANN Office of CTO (OCTO)

Nov 12th, 2024

ICANN
Domain Metrica

Who We Are, Where We Fit



Who We Are, Where We Fit

SSR Research

Who We Are, Where We Fit

SSR Research

Samaneh Tajalizadehkoob

Who We Are, Where We Fit

SSR Research

Samaneh Tajalizadehkoob

Carlos Gañán

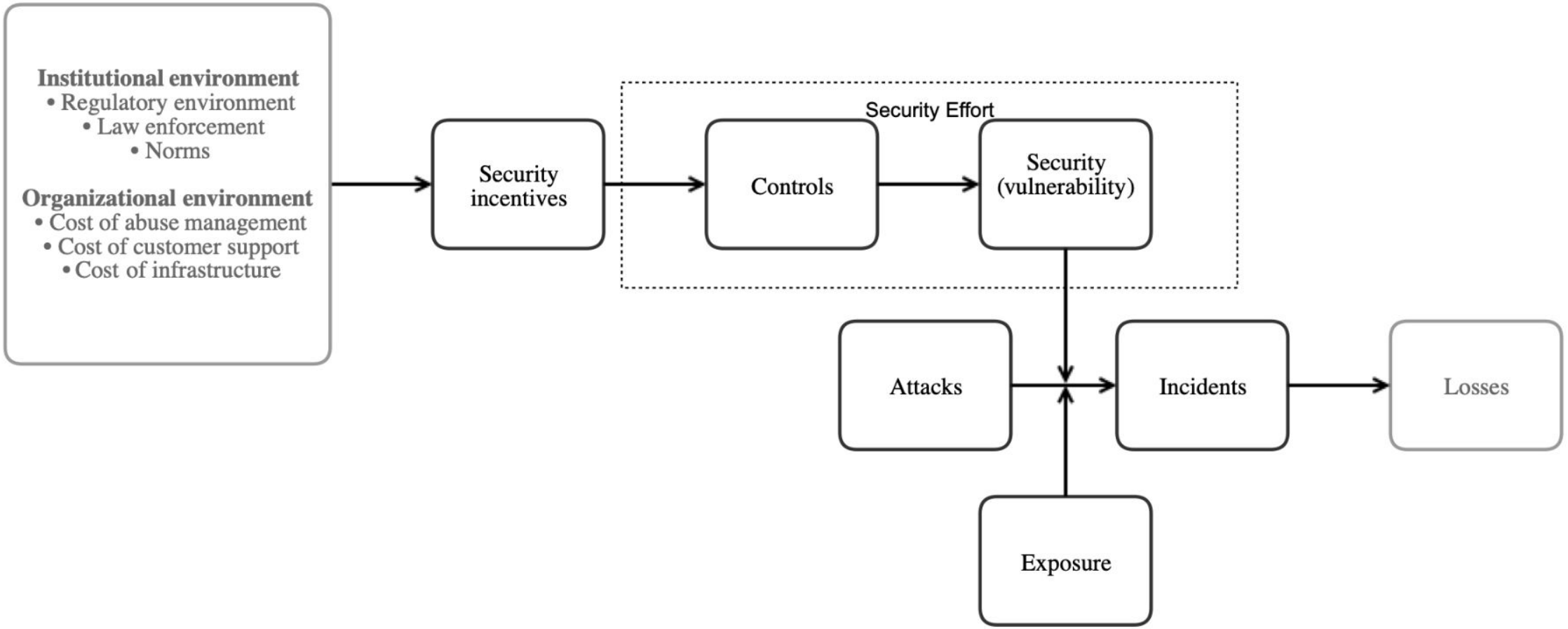
Sam Cheadle

Siôn Lloyd

Security Stability & Resilience (SSR) Research

- Think Tank that mostly do **research** and **development** on **Internet identifiers**
- We look to use **data** and **scientific** methods to answer questions of interest to the community
- Our goal is to
  - Increase **reliability** of the [existing] metrics that are used to measure (e.g., security, insecurity, abuse, etc.)
  - Develop [new] metrics/method **from scratch**

SSR Research Conceptual Framework



Security Efforts - Example of DNS Abuse

- **Where is DNS Abuse Concentrated?**
  - Counts of **reported** domains appear in RBLs
    - What domains? [Report vs. incident]
      - "**Reports**" or reported domains, lack corroborating evidence whether they "became" an attack.
      - "**Attacks**" attempts of using reported domains to create damage
      - "**Incidents**" are materialised attacks which cause some form of loss (either tangible or intangible)
- **What are the mitigation measures?**
  - Reactive measures [take downs, any action after RBL appearance]
  - Proactive measures [controls, policies, configurations, things to do to not be attractive/avoid abuse concentrations]

ICANN Domain Metrica

The next generation of ICANN measurements

ICANN

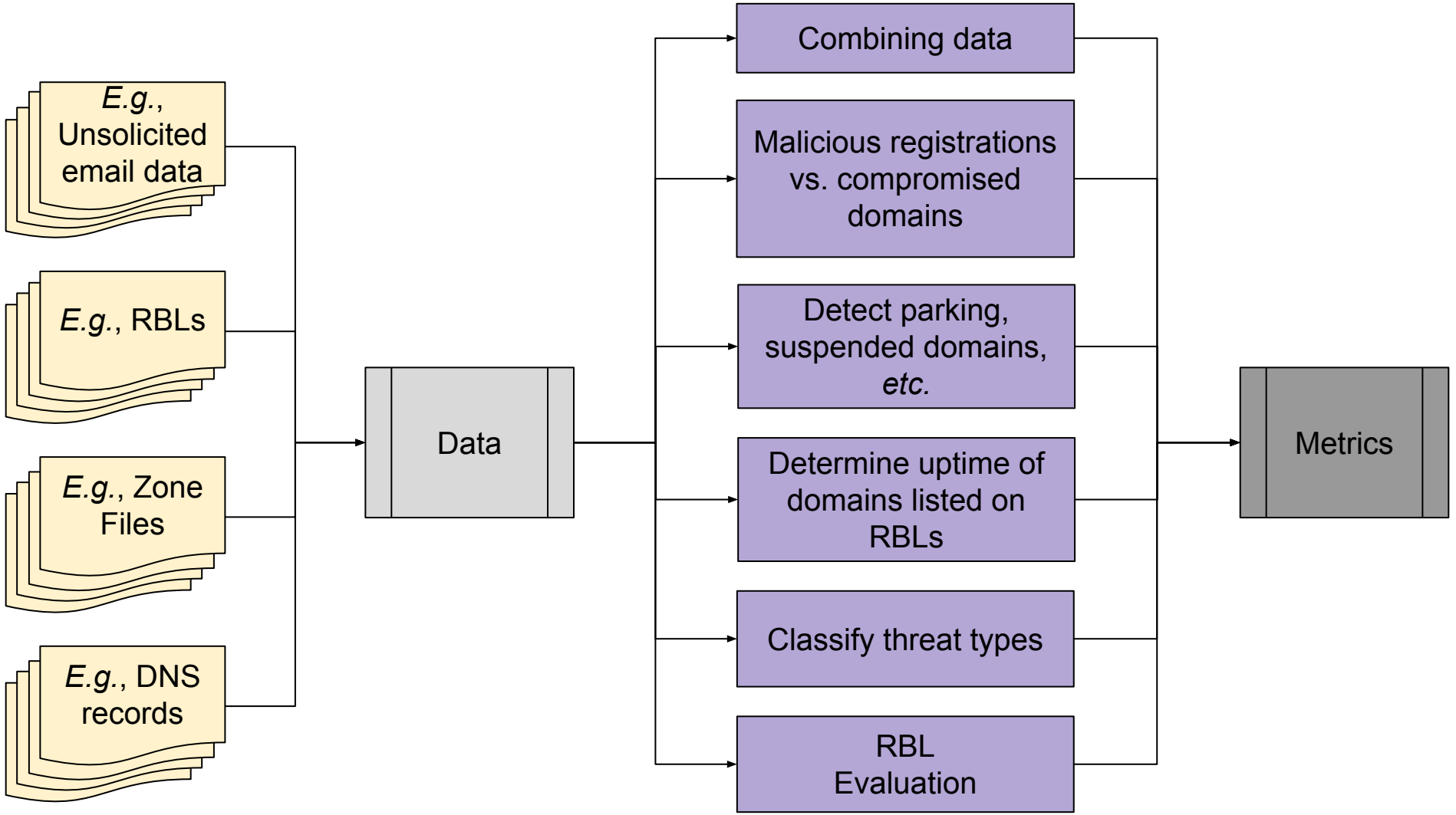
Domain Metrica

ICANN Domain Metrica - General Idea

- 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.

Data into Metrics



ICANN Domain Metrica - Design Principles

Modular

- Contain metadata about domain names added over time as modules
- The output of OCTO research projects can feed in

Flexible

- It can be used in multiple ways depending on the user
- Built to be updated as new requirements arise
- The system remains relevant over time

Transparent

- Methodologies and sources used will be public
- Data will be shared (where allowed by licencing)

ICANN Domain Metrica - the Team

Who?

ICANN SSR Research providing the vision and science.

ICANN E&IT providing development resource.

Why is ICANN doing this?

Requests from the community and reviews for more detailed data

What Metrica Module 1 Measures so far

- **Where is DNS Abuse Concentrated?**
  - Counts of **reported** domains appear in RBLs
    - What domains? [Report vs. incident].
      - "**Reports**" or reported domains, lack corroborating evidence whether they "became" an attack.
      - "**Attacks**" attempts of using reported domains to create damage
      - "**Incidents**" are materialised attacks which cause some form of loss (either tangible or intangible)
- What are other attributes of the reported domains?
    - Geo location of hosts
    - Which types of domains [popularity]
- **What are the mitigation measures?**
  - Reactive measures [take downs, any action after RBL appearance]
  - Proactive measures [controls, policies, configurations, things to do to not be attractive/avoid abuse concentrations]

ICANN Domain Metrica - Module 1

Module 1 : DNS Abuse Reputation and Domain Popularity Ranking

1. Data and statistics for **gTLDs** and **registrars**
2. **Searchable** for gTLDs, registrars and domains / **Metadata** on searched terms
3. Shareable **domain-level** data
4. **Interactive visualisation**s and comparisons [allows to filter on dates and add gTLDs to compare]
5. **Abuse map** - abuse hosts geolocation [Maxmind data]
6. **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

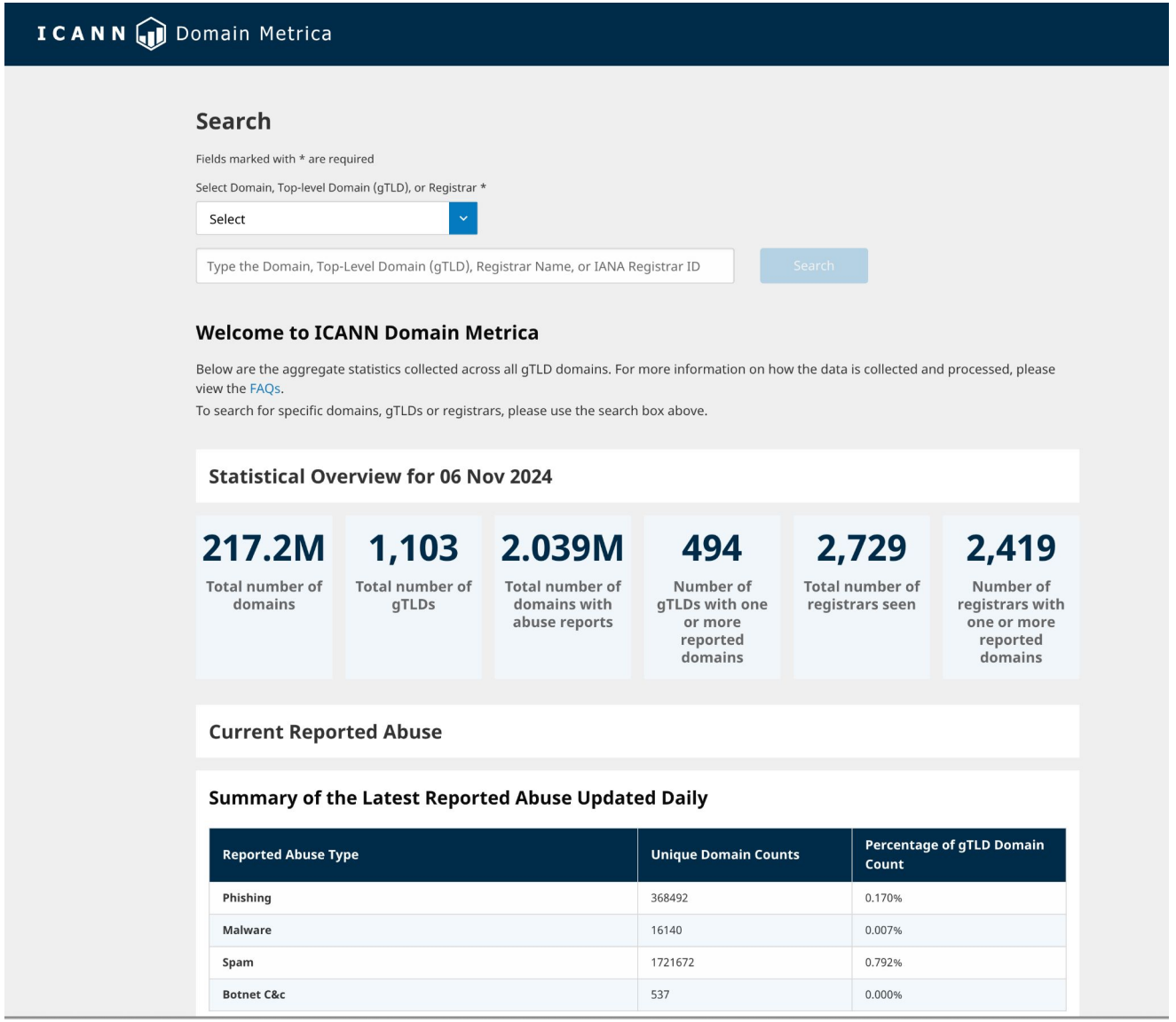
24th September: Pilot release to small user group [aim was to ask for feedback]
29th October: Rr/Ry User launch (MoSAPI on 30th October)
4th December: General launch [subject to change]

Feedback from pilot and early use

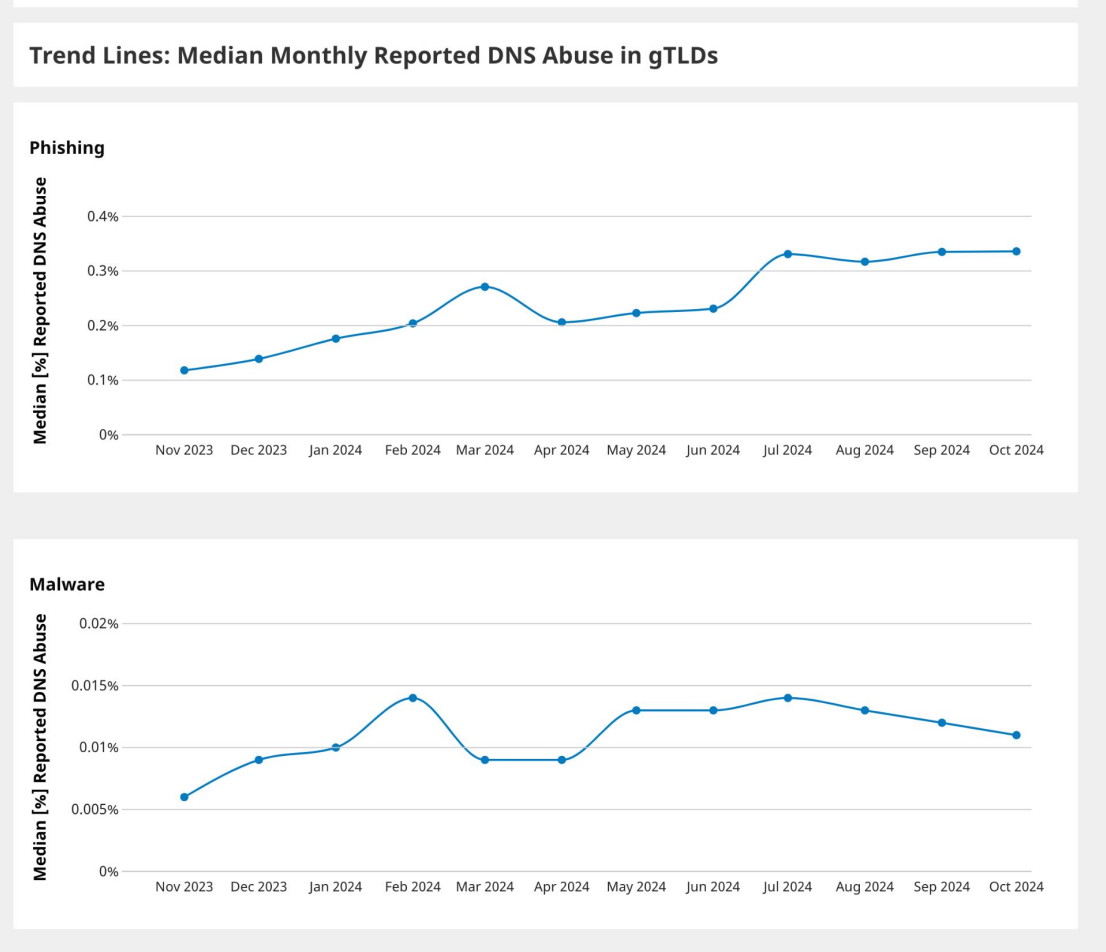
- Spam - definition too broad
  - Doesn’t match contracts - we are addressing this
- Performance issues
  - Looking at bottlenecks, *etc.*
- Documentation
  - Expand FAQs - More “in-line” help

ICANN Domain Metrica - Module 1

General Data and statistics for **gTLDs** and **registrars**

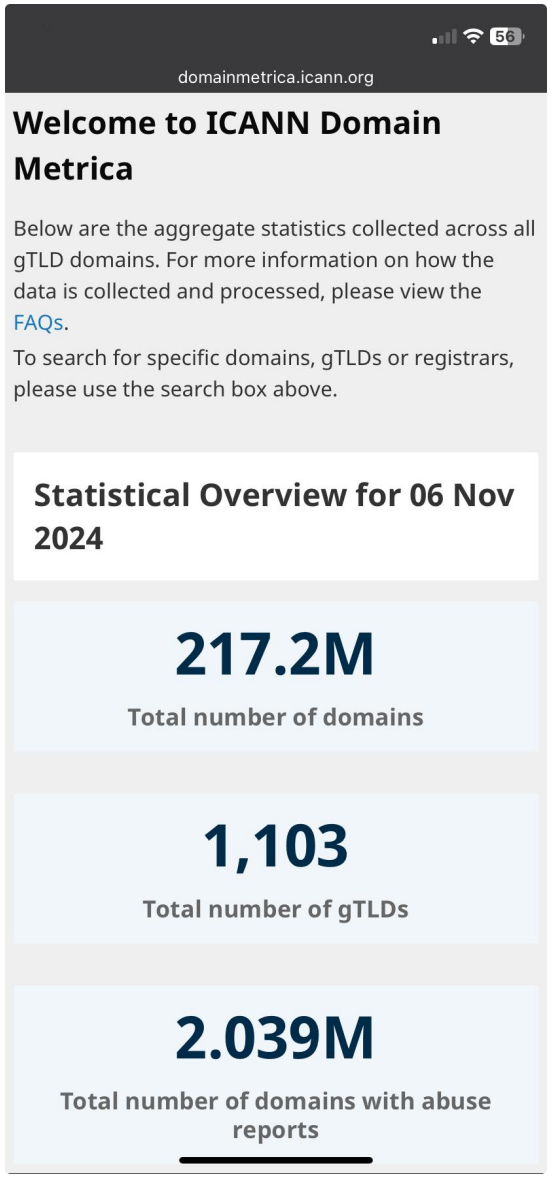


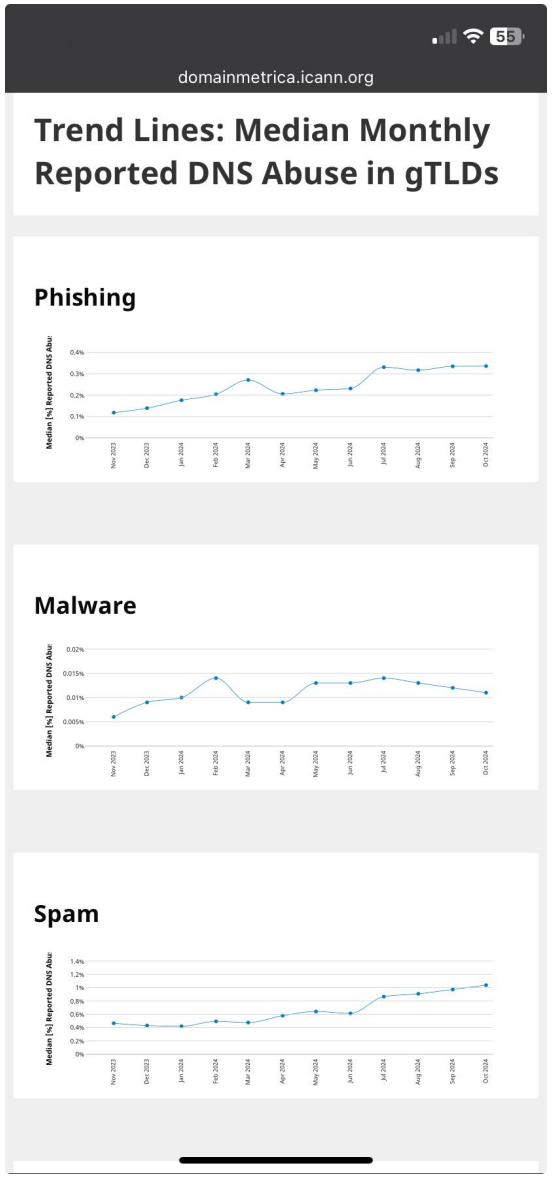
ICANN Domain Metrica - Module 1



Data and statistics for **gTLDs** and **registrars**

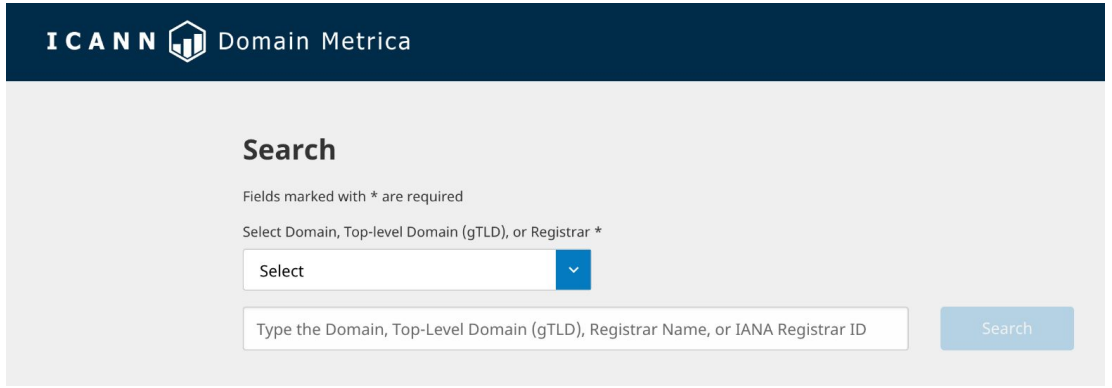
ICANN Domain Metrica - Module 1

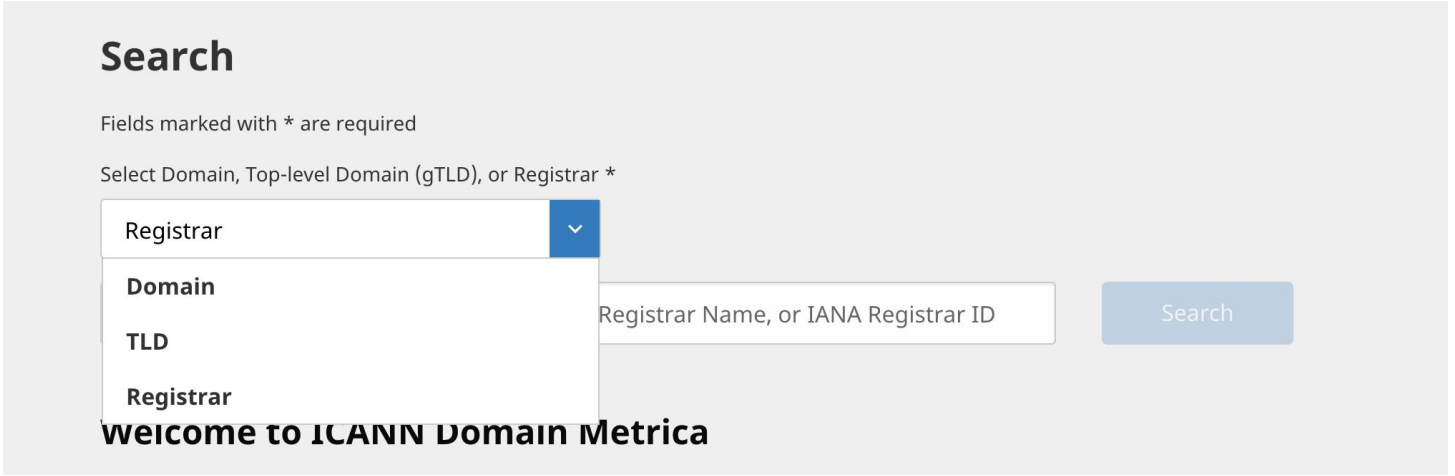




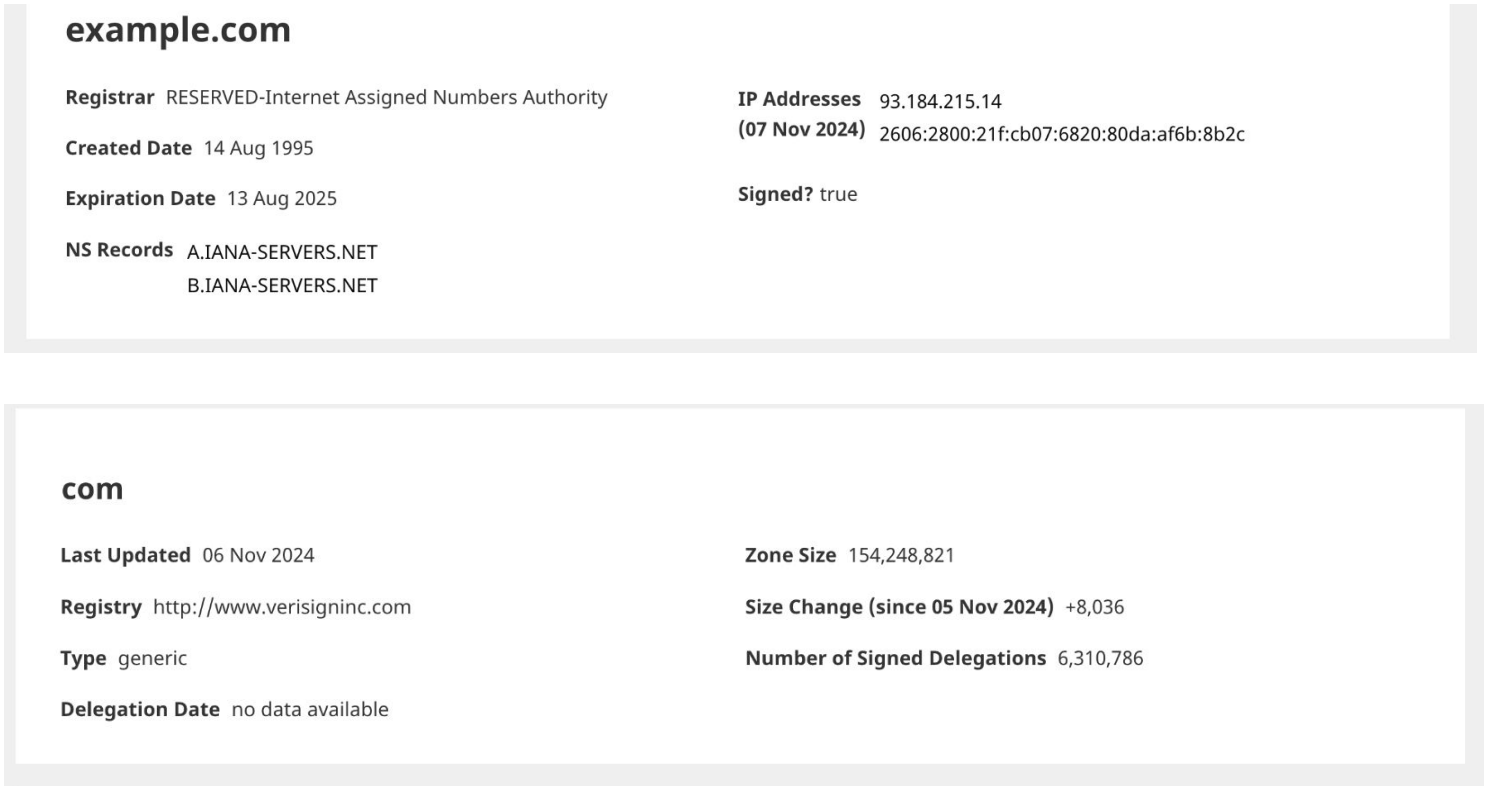
ICANN Domain Metrica - Module 1

Searchable for gTLDs, registrars and domains



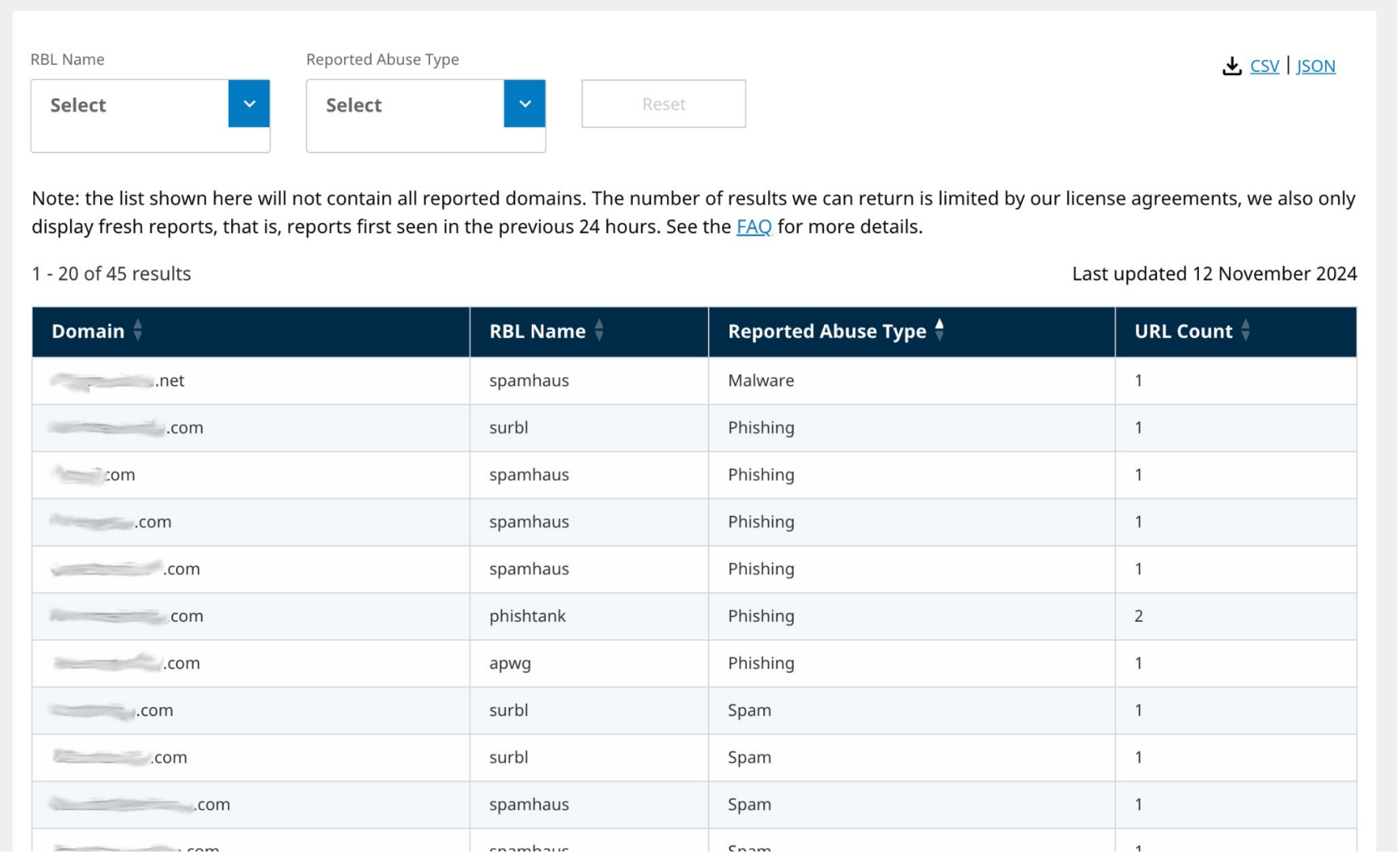


ICANN Domain Metrica - Module 1



Metadata on searched terms

ICANN Domain Metrica - Module 1



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 24 hours. See the FAQ for more details.

1 - 20 of 45 results

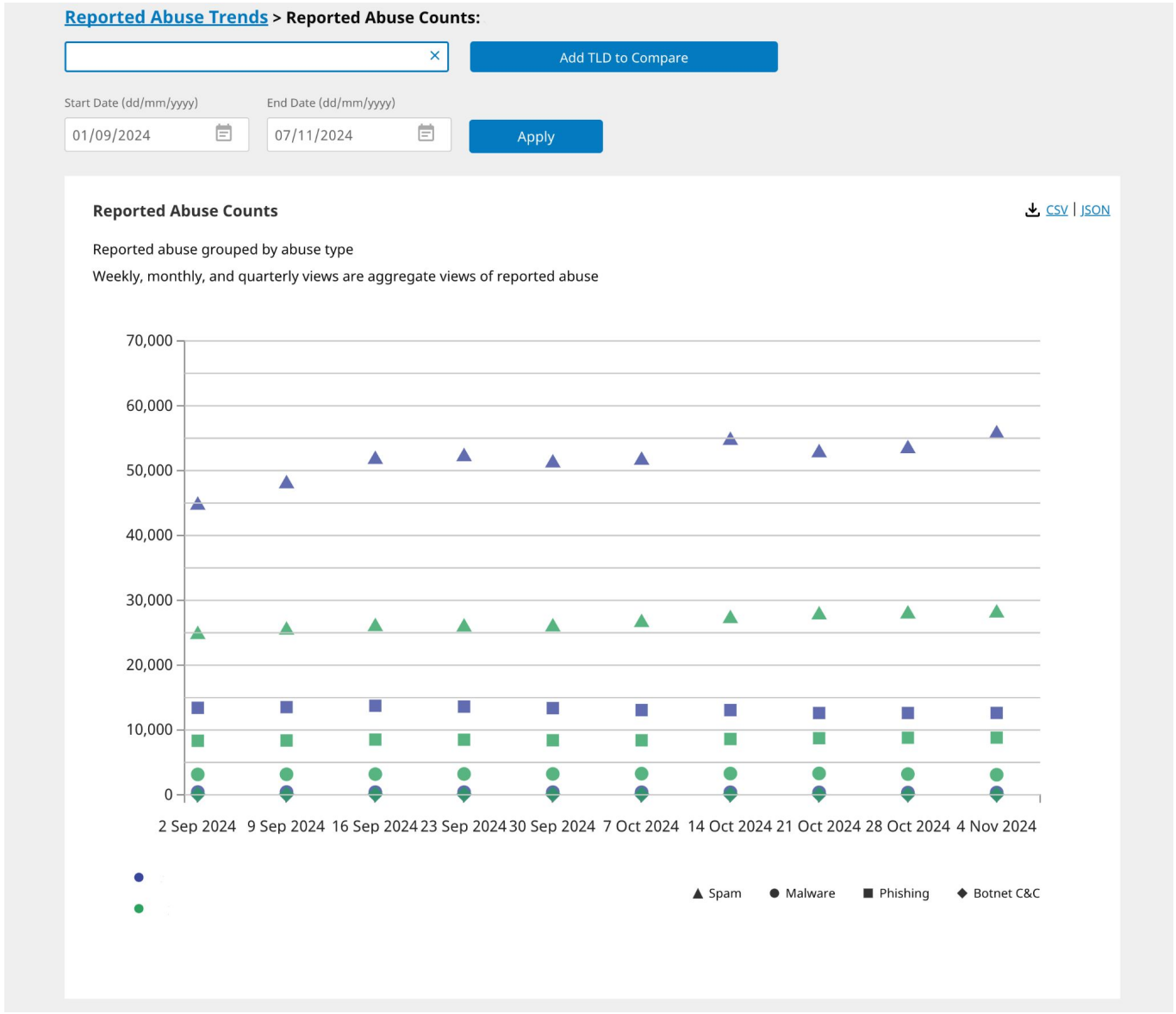
Last updated 12 November 2024

Domain	RBL Name	Reported Abuse Type	URL Count
[redacted].net	spamhaus	Malware	1
[redacted].com	surbl	Phishing	1
[redacted]com	spamhaus	Phishing	1
[redacted].com	spamhaus	Phishing	1
[redacted].com	spamhaus	Phishing	1
[redacted]com	phishtank	Phishing	2
[redacted].com	apwg	Phishing	1
[redacted].com	surbl	Spam	1
[redacted].com	surbl	Spam	1
[redacted].com	spamhaus	Spam	1
[redacted]	[redacted]	[redacted]	1

Shareable **domain-level** data

(For registry and registrar users only)

ICANN Domain Metrica - Module 1

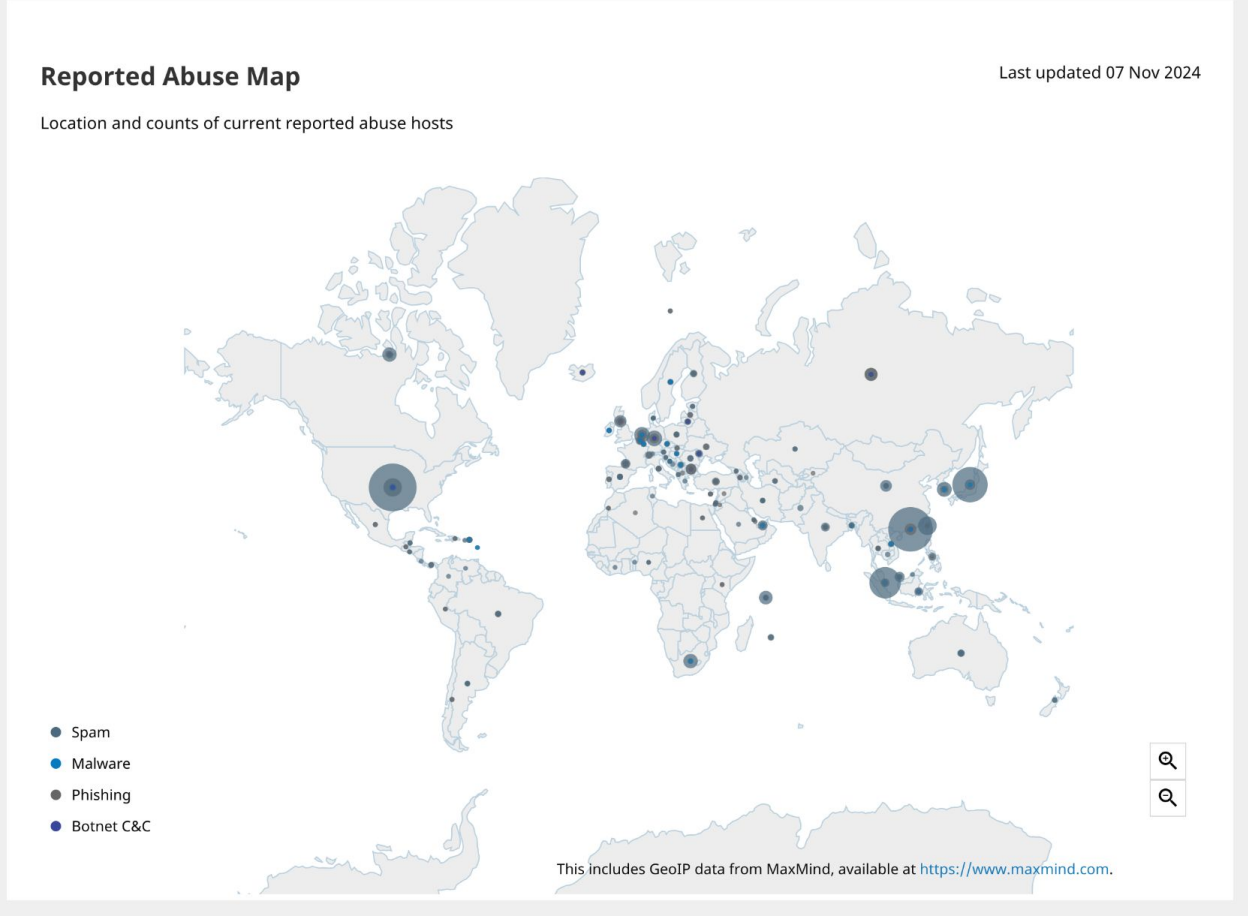


Interactive visualisations filter on **dates** and add **gTLDs** to compare

ICANN Domain Metrica

Interactive visualisations filter on **dates** and add **gTLDs** to compare

ICANN Domain Metrica



Abuse map - abuse hosts geolocation

ICANN Domain Metrica

5- Domain Popularity Ranking (Tranco list)

example.com

Registrar RESERVED-Internet Assigned Numbers Authority

Created Date 14 Aug 1995

Expiration Date 13 Aug 2025

NS Records A.IANA-SERVERS.NET
B.IANA-SERVERS.NET

IP Addresses (07 Nov 2024) 93.184.215.14
2606:2800:21f:cb07:6820:80da:af6b:8b2c

Signed? true

Current Reported Abuse

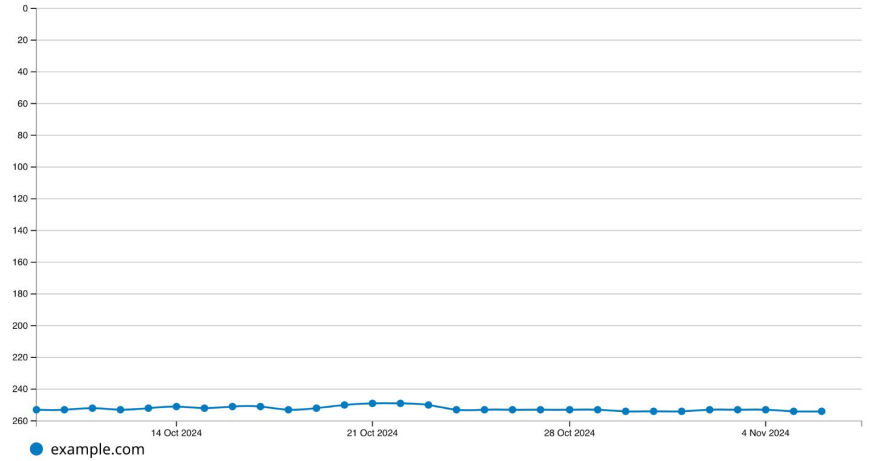
Summary of the latest reported abuse updated daily

No current active abuse reports found

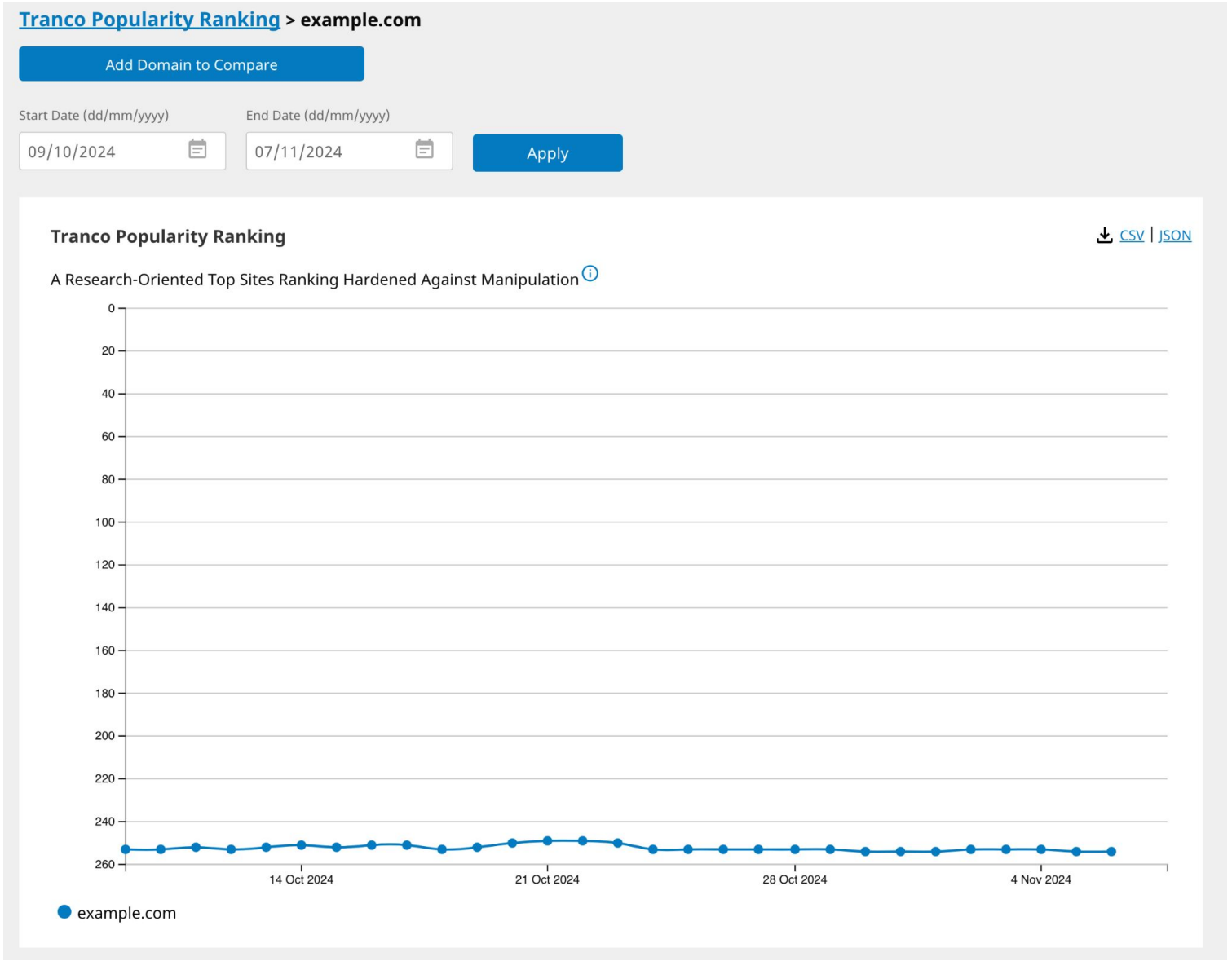
Tranco Popularity Ranking

A Research-Oriented Top Sites Ranking Hardened Against Manipulation

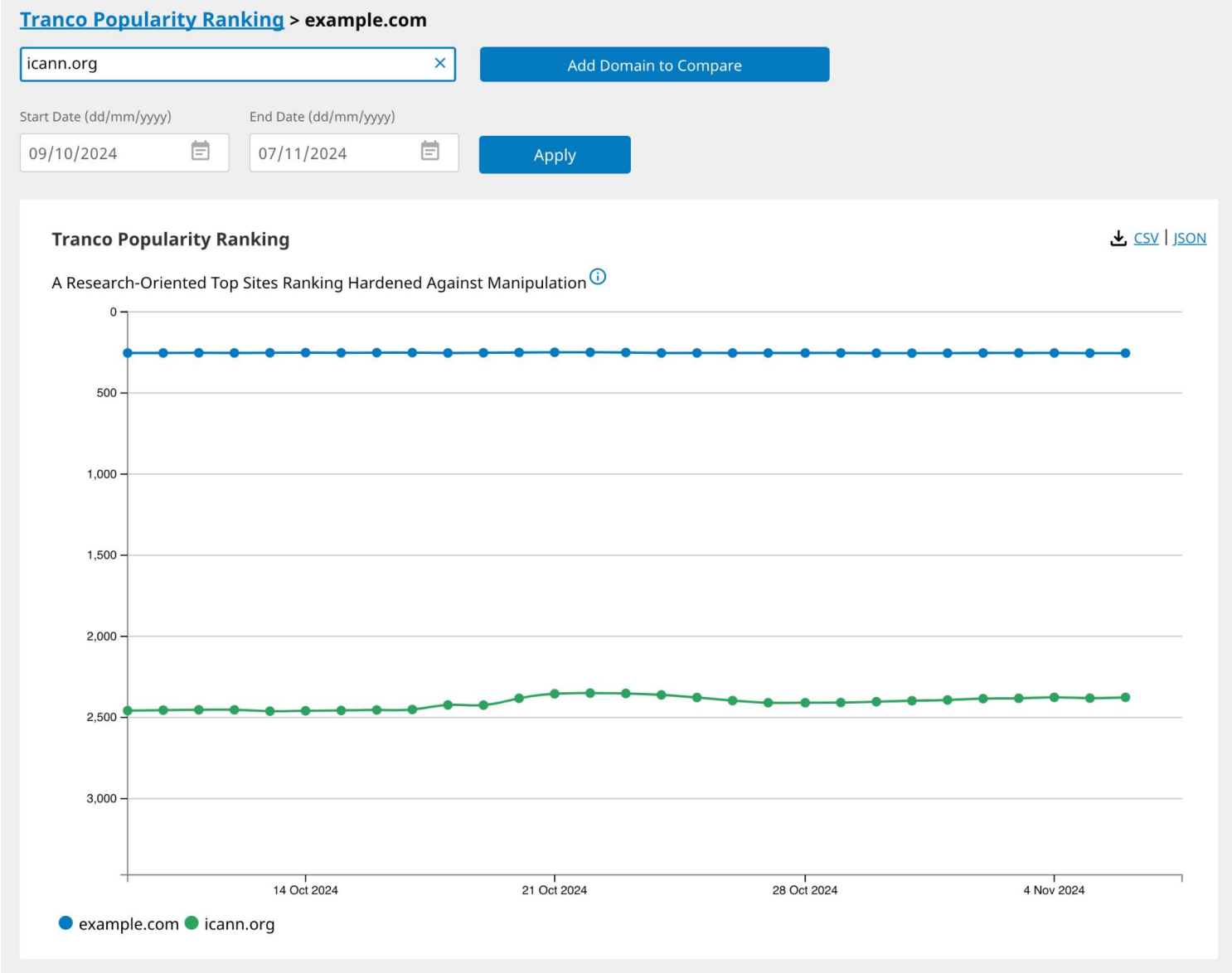
Click the chart title to download, compare, or change date range



ICANN Domain Metrica



ICANN Domain Metrica



ICANN Domain Metrica

What does/will Domain Metrica **add to existing systems**?

- Dynamic interactive dashboard - allows for filters [time/abuse type]
- Time series data, allows **narrowing down up to "date"**
- Download **underlying data** via an API - or **exported from UI**
- Includes NS and delegation **metadata** and **flags** on searched terms
- **Check against the zone on daily basis** (if domain is not delegated, not included in the counts, mitigations are acknowledged)
- Provide **underlying domain names**
- Provides **Tranco domain popularity ranking** (research indicates a relation between the domain abuse and popularity)

ICANN Domain Metrica - Future Outlook

Domain Metrica is not "**finished**"

I. It is planned to evolve through its existence
   A. Reflect feedback, new use cases, *etc.* [improvements to module 1]
   B. Build on the foundations we have
   C. Yearly evaluation of the inputs lists we use [RBLs using our RBL evaluation methodology **OCTO037**]

Future modules and metrics?

I. Research the science/metrics within the SSR Research team
II. Build prototype
III. Productionise and add to Domain Metrica as future modules

Q&A on Domain Metrica

Analysis

ICANN Org Funded Projects: INFERMAL

A new research project called Inferential Analysis of Maliciously Registered Domains (INFERMAL).

The study aims to systematically analyze the preferences of attackers and possible measures to mitigate malicious activities across domains, top-level domains (TLDs) and registrars in a proactive way.

Study Funded by **ICANN Org**
Study Conducted by **KOR Labs**

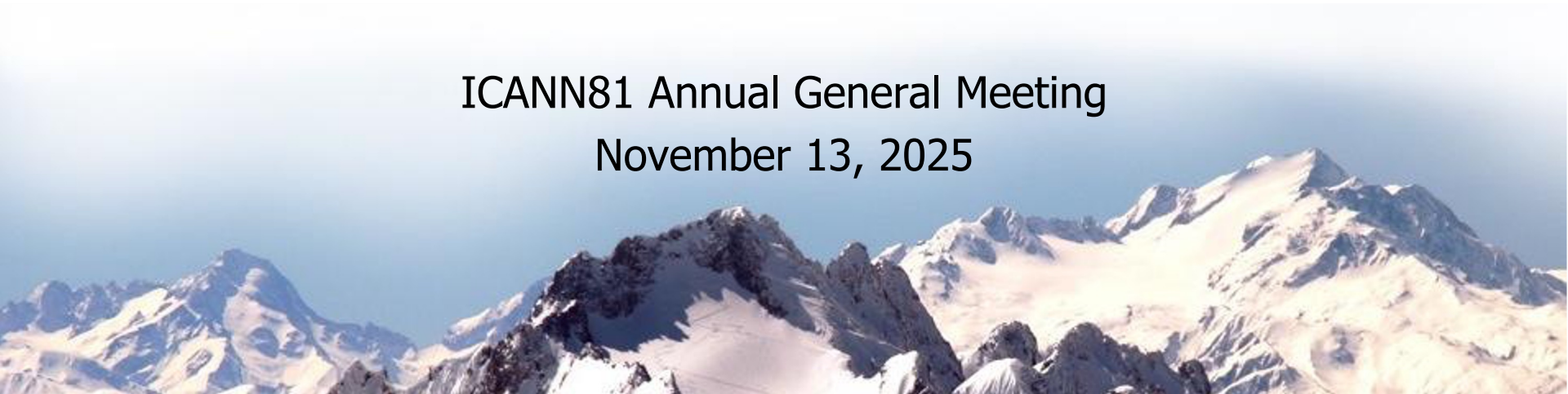
INFERMAL: Inferential analysis of maliciously registered domains

Yevheniya Nosyk, **Maciej Korczyński**, Sourena Maroofi, Jan Bayer, Zul Odgerel, Andrzej Duda
KOR Labs / Grenoble Alpes University

ICANN Org Project Coordination:

Samaneh Tajalizadehkhoob, Carlos Gañán

ICANN81 Annual General Meeting
November 13, 2025



Motivation

- Cybercriminals exploit domains for: phishing, malware, spam, botnets
- Constantly register new domains to fuel attacks
- Prior studies show high abuse in specific registrars and TLDs
- No comprehensive research on factors influencing malicious registrations

Goal

- Investigate domain abuse from the **attacker's perspective**
- Identify factors driving malicious domain registrations

Approach – overview

- Scope: Maliciously registered phishing domains

- Features: 73 features encompassing three latent factors:
  1. Registration attributes
  2. Proactive verification
  3. Reactive security practices

- GLM regression analysis:
  1. Relationship between features and the concentration of phishing domains at the registrar-TLD level
  2. Features are favored by attackers alone or also by legitimate users

Datasets

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

- Active WHOIS and DNS measurements

* https://tld-list.com/

Maliciously registered phishing and benign domains

- 534 K bloclisted URLs (Aug 2023 – Jan 2024)
- **108 K** domain names

- Excluding domains of benign services
- Active measurements (DNS, WHOIS) over one month to verify if the takedown occurred
- **28 K** registered maliciously

- Mapping between domains and daily-collected registration features
- **14 K** maliciously registered (165 TLDs, 31 registrars)

- Benign dataset of 15.4 K domains under 259 TLDs originating from 38 registrars

Rank	Registrar	TLD	#Domains
1.	NameSilo	top	1,807
2.	NameSilo	com	852
3.	GoDaddy	com	832
4.	Hostinger	online	764
5.	NameSilo	info	513
6.	Hostinger	com	479
7.	Namecheap	com	479
8.	Alibaba Cloud	com	327
9.	NameSilo	xyz	233
10.	Hostinger	cloud	225
11.	NameSilo	buzz	222
12.	Sav	com	211
13.	Alibaba Cloud	shop	197
14.	NameSilo	us	191
15.	Hostinger	site	179
16.	NameSilo	life	178
17.	NameSilo	sbs	171
18.	Hostinger	shop	156
19.	NameSilo	cc	149
20.	Alibaba Cloud	top	148

20 most frequently observed registrar/TLD pairs in our dataset of maliciously registered domain names

Selected features

1. Registration attributes

   - **Free API**: the registrar APIs enable users to search, purchase, and manage domains
   - **Free bulk search**: the capability to search domains in bulk
   - **Available payment methods**: 24 boolean features for each payment method, including PayPal, Bitcoin, etc.
   - **Pricing:** domain name registration prices
   - **Discounts:** deducting a fixed amount or % from the regular price
   - **Pricing terms:** might apply only to a limited number of domains or new customers
   - **Free web hosting, free DNS, free email account:** included for free in each domain registration

Selected features

2. Proactive verification

- **Operational validation of the registrant contact details**: Test whether contact details (email/phone) are verified during account creation or before domain purchase.

- **Domain registration warnings and restrictions**: three labels defined:
    i. `9e86e6d5d4c676441da` (the first 20 characters of the MD5hash of "DNS abuse"),
    ii. `office365-my-account`
    iii. `facebook-login-page`

  For each registrar-TLD pair, we proceed to the payment prompt.

- **Registration restrictions**: 14 boolean features, e.g., local presence required, ID required, professionals only

Selected features

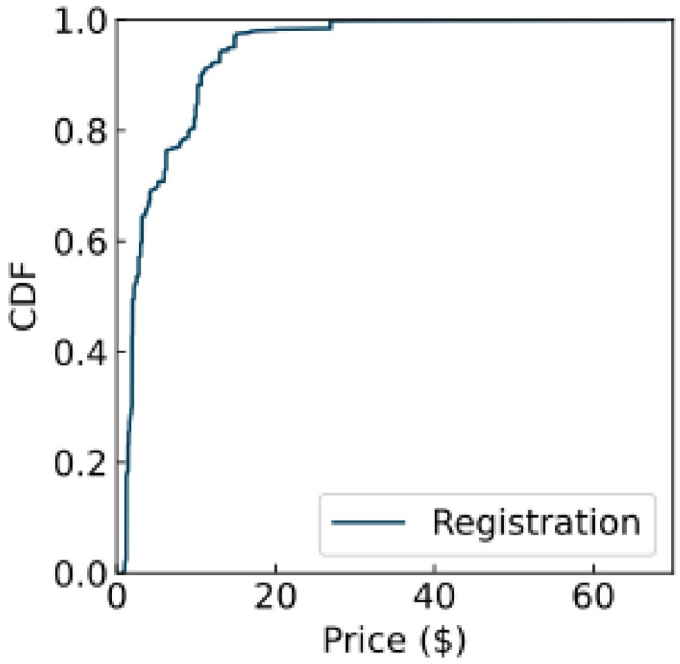
3. Reactive security practices: malicious domain name uptimes (with and without notifications)

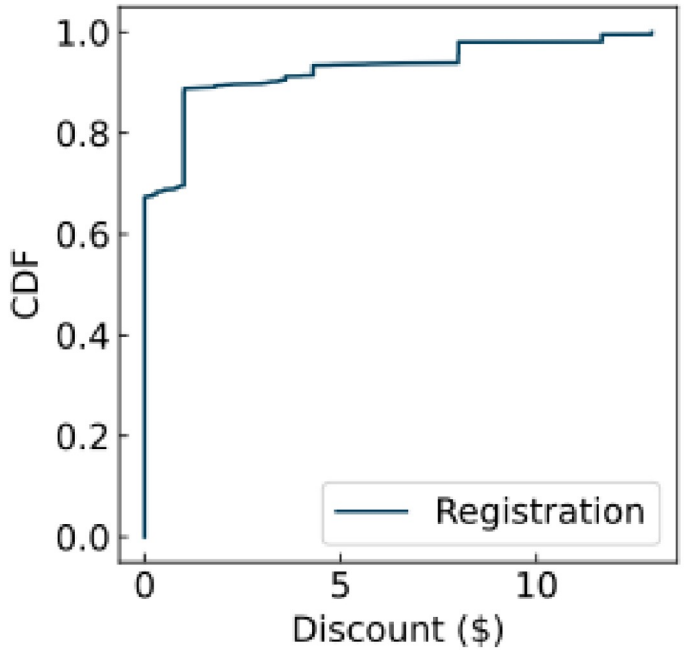
   - WHOIS/DNS measurements
   - 5 minutes, 15 m, 30 m, 1 hour, 2 h, 3 h, 4 h, 5 h, 6 h, 12 h, 24 h, 36 h, and 48 h after blocklisting, and then every 12 hours
   - for a subset of maliciously registered domain names, notifications are sent to registrars

Descriptive Analysis of Features

Prices and discounts: Registration

- Prices range from $0.78 to $69, with nearly 50% costing $2 or less

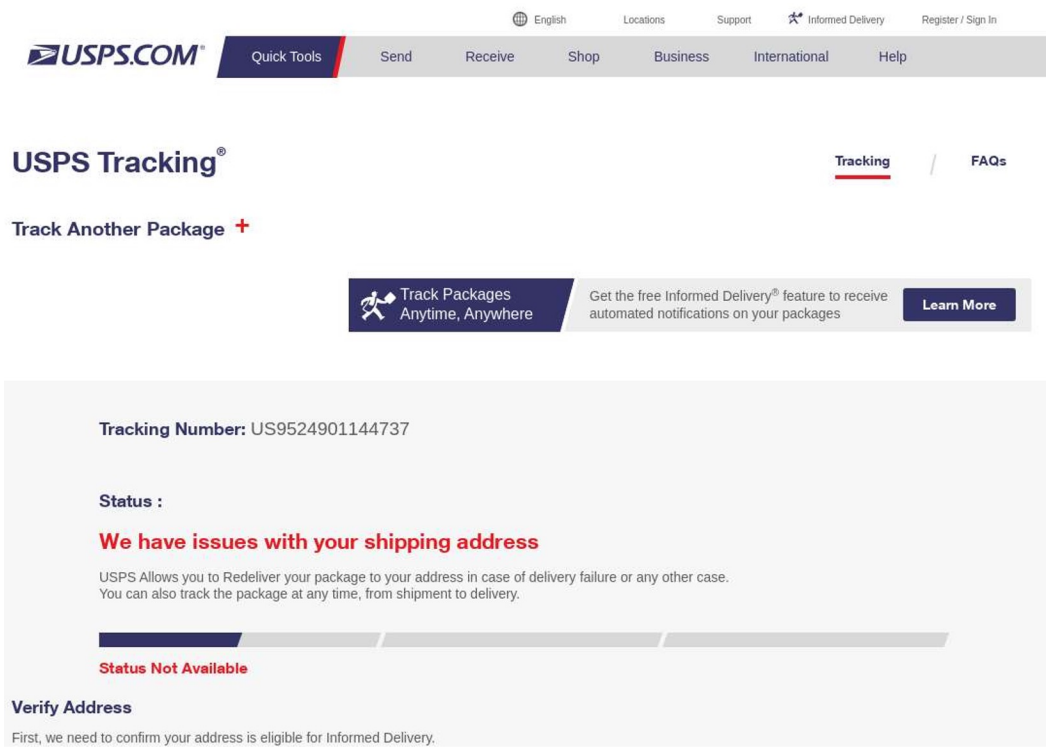




Descriptive Analysis of Features

Prices and discounts: Registration

- Examples of expensive domains include usps.bar ($69), support-fb.sh ($59.99), and dhlcenter.net ($56)



Descriptive Analysis of Features

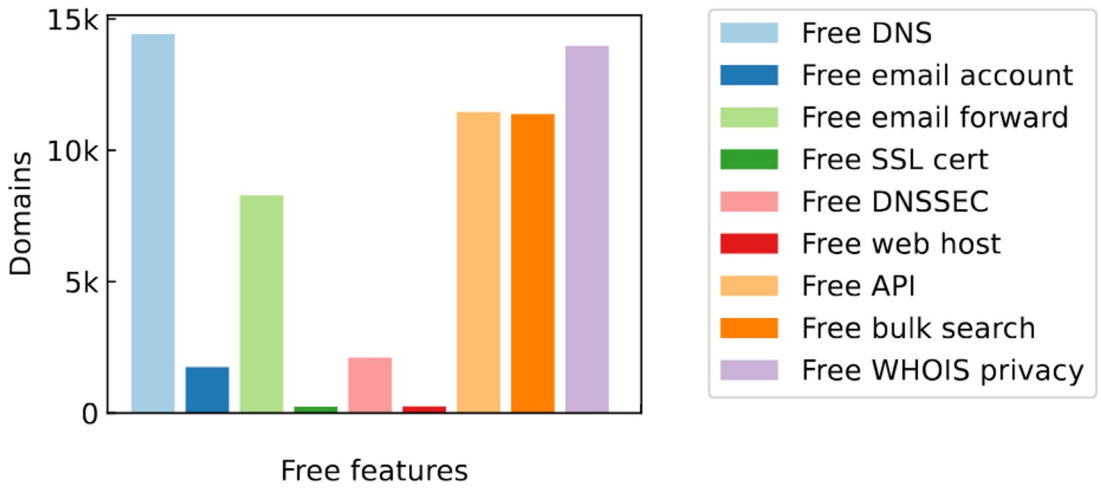
Registration prices and discounts:

- Registration prices may be subject to various terms (e.g., 4,423, reduced registration prices were valid for one domain), discounts to new customers only

Descriptive Analysis of Features

Free features

- A free API is offered by 16 of the 31 registrars we examined
- Four registrars permit the automated account creation (e.g., as a subaccount under an existing API user)
- 18 registrars offer a "bulk search" to check availability and prices for 20 to 10 K+



Descriptive Analysis of Features

Payment methods

- 13 are supported by the 31 analyzed registrars. Bitcoin supported in more than two-thirds of cases.

Domain Name Registrant Data

- Phone verification is rare: 23 registrars check syntax, and only 6 validate operationally

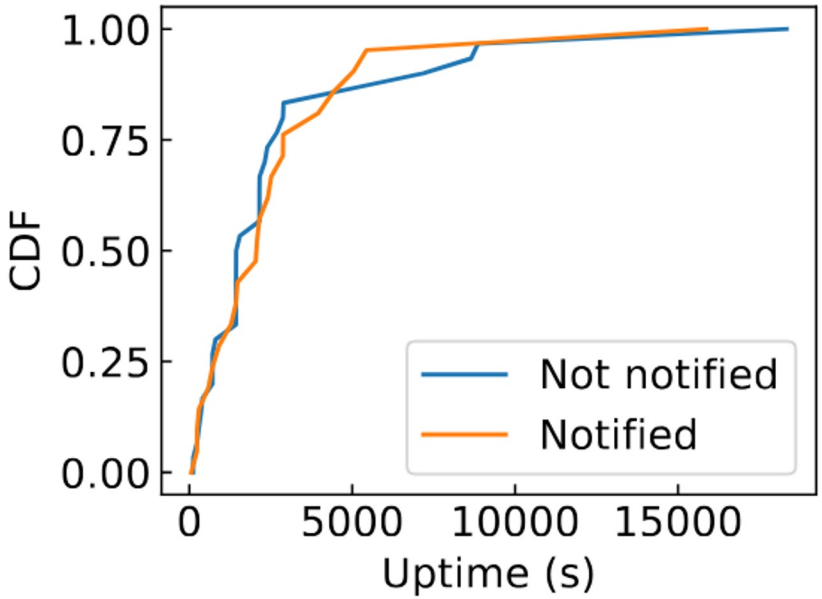
Prevention of Trademark Infringement

- Two registrars blocked trademarked domains from being added to the cart

Descriptive Analysis of Features

Malicious Domain Uptimes

- Similar results at the domain and registrar levels



CDF of uptimes for notified and not notified registrars

Driving Factors of Domain Abuse

Model 1: Relationship between features and the concentration of phishing domains at the **registrar-TLD** level

Driver	Type	Correlation with abuse counts	Increase
Retail registration price	Numerical	Weak positive	1$↓ (6.6%↑)
Retail registration discounts	Numerical	Positive	1$↓ (49%↑)
Cryptocurrency payment(s) available	Boolean	Positive	30%
APIs to register domains or to create accounts available	Boolean	Strong positive	401%

Driving Factors of Domain Abuse

Our analysis suggests that while initial pricing plays a role, attractiveness to attackers likely results from a combination of factors

Driver	Correlation with abuse counts	Correlation with abuse counts	Increase
Free DNS service	Boolean	Positive	205%
Free hosting service	Boolean	Positive	88%
Presence of restrictions (e.g., commitment required, local presence, professionals only)	Boolean	Negative	63%
Validation of email/phone present	Boolean	Negative	70%
Shorter uptimes	Numerical	Statistically significant but negligible correlation	~0%

Discussion and conclusions

- Key factors driving malicious domain registrations from the **attacker's perspective**.
- This study did not include instances of benign domains that have been compromised, for example, at the website or hosting level.
- Results should be interpreted with caution and may or may not be generalized into actions by registrars or TLDs.
- Some factors are combined and involve a variety of features.
- Attractiveness to attackers likely results from a combination of factors.
- It is essential to consider the economic implications, the impact on legitimate users, and the likely response of attackers to adjustments, the result of partial/full implementation.

Acknowledgements

We would like to thank the ICANN OCTO-SSR research team (Carlos and Samaneh) for scientific discussions, ICANN for funding this research, the Anti-Phishing Working Group, Phishtank, and OpenPhish for access to their feeds, and Spamhaus and SURBL, whose datasets helped us filter out malicious domains from the benign list we sampled. We thank Rowena Schoo, Graeme Bunton (Netbeacon Institute), Siôn Lloyd (ICANN) for their insightful comments on the presentation.

Questions

Contact information

Yevheniya Nosyk, Maciej Korczyński, Sourena Maroofi, Jan Bayer, Zul Odgerel, Andrzej Duda (KOR Labs / Grenoble Alpes Univ.)

Maciej Korczyński
KOR Labs
maciej.korczynski@korlabs.io

Samaneh Tajalizadehkhoob
ICANN OCTO
samaneh.tajali@icann.org

Q&A on INFERMAL

DNS Abuse: A Broad and Complex Issue

DNS Abuse encompasses a wide range of problems, making it a multifaceted issue that requires diverse approaches.

Need for Community Involvement

- Addressing DNS Abuse effectively requires the active participation of the entire community, not just individual organizations.

Role of ICANN

- ICANN is taking significant steps to tackle DNS Abuse, but it's just one part of a larger effort.

ICANN Community Engagement

- Various stakeholders within the ICANN community are working on different aspects of DNS Abuse, reflecting a collaborative approach.

Call to Action: ICANN Community Efforts

The ICANN community is best positioned to determine what policy recommendations, if any, may be needed to mitigate DNS Abuse.

One World, One Internet

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