Updates on ICANN's DNS Security Threat Mitigation Program

Patrick Jones

30 Sept 2022 – TLDCON

ICANN

Patrick Jones

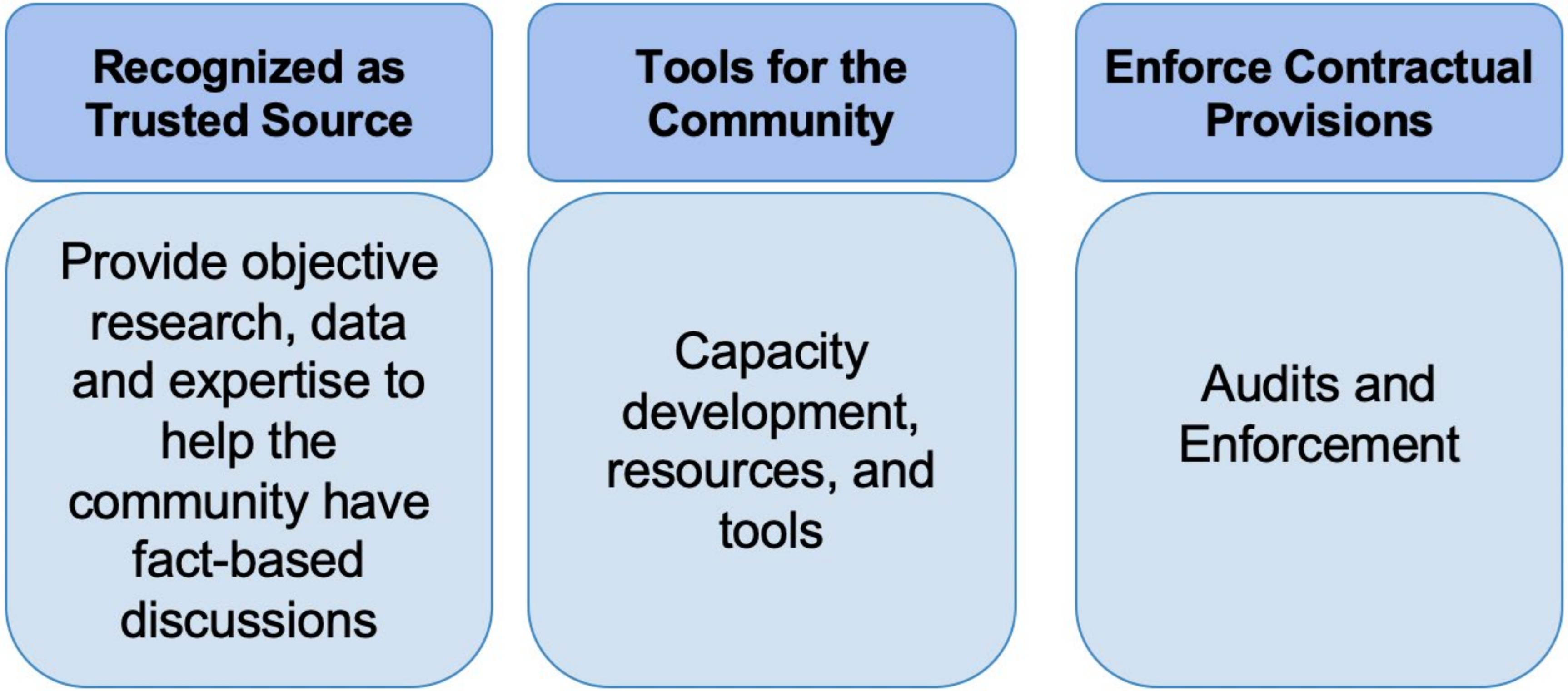
Senior Director, Global Stakeholder Engagement

ICANN

ICANN DNS Security Threat Mitigation Program

ICANN’s DNS Ecosystem Security Mitigation Program

Ensuring the Security, Stability and Resiliency of the DNS are foundational aspects of ICANN’s purpose and mission



Recognized as Trusted Source

Provide objective research, data and expertise to help the community have fact-based discussions

Tools for the Community

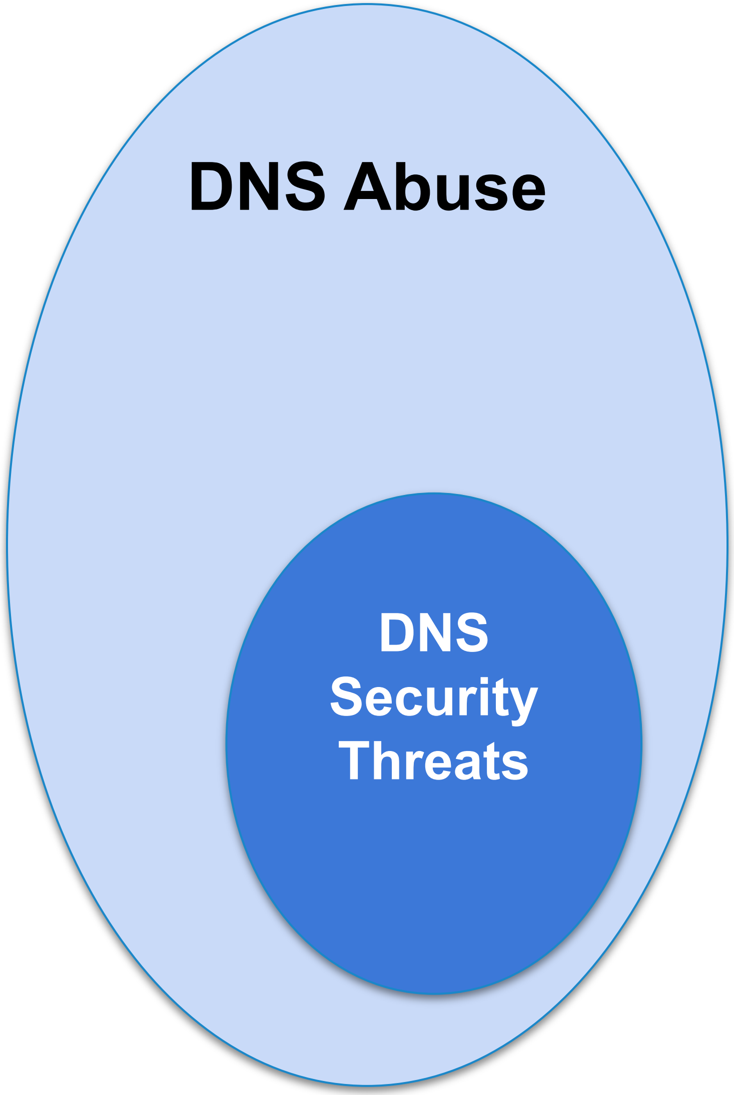
Capacity development, resources, and tools

Enforce Contractual Provisions

Audits and Enforcement

DNS Security Threats & DNS Abuse

- No consensus definition of DNS abuse
- Bylaws focus our remit on Security & Stability of the DNS and prohibit content regulation
- DNS security threats:
  - Phishing
  - Malware
  - Botnets
  - Pharming
  - Spam (as a vector)



ICANN DNS Ecosystem Security activities

Examples of current ICANN org projects related to DNS ecosystem security:

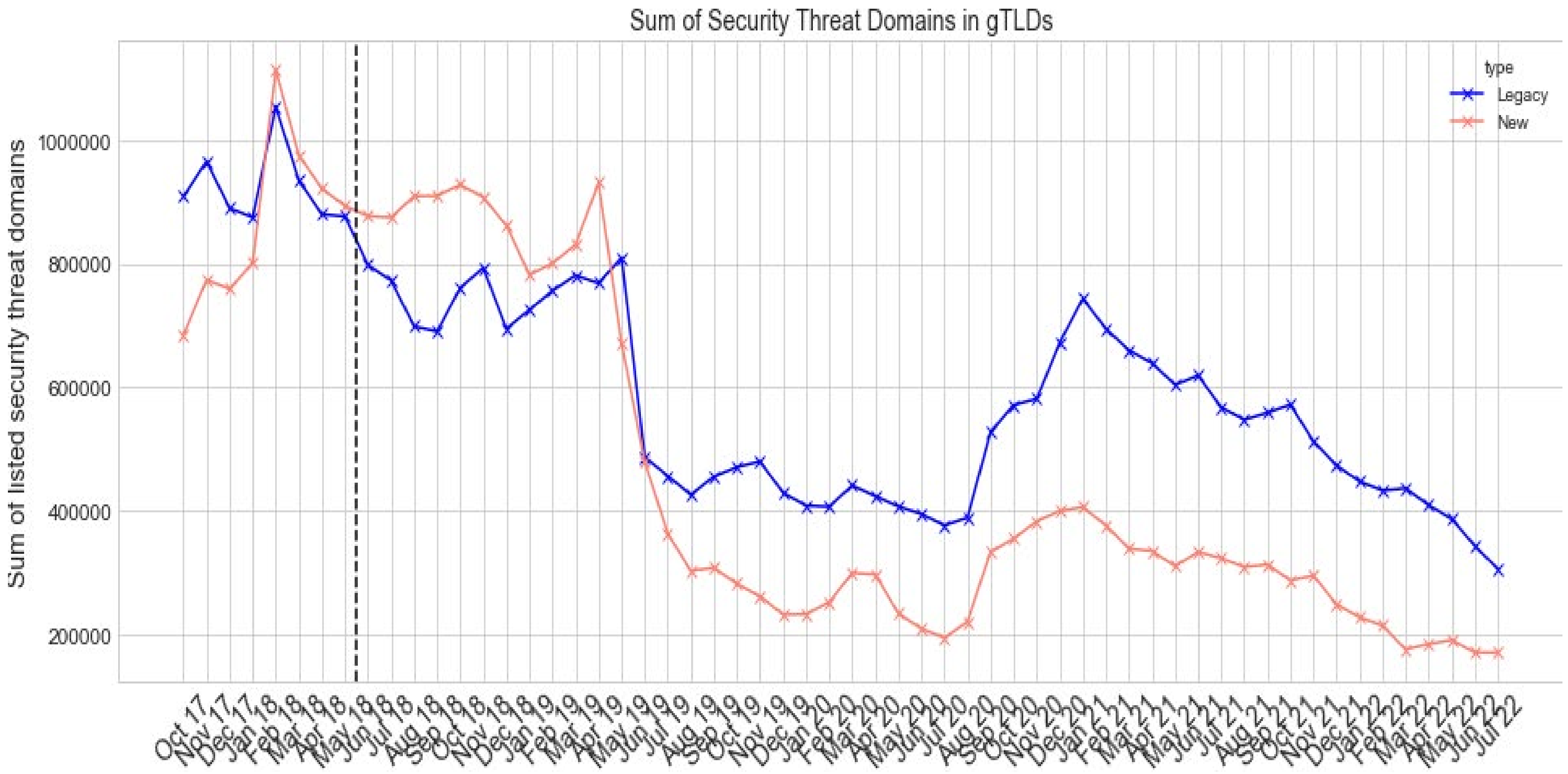
- **DNS Security Facilitation Initiative Technical Study Group**
- **Domain Abuse Activity Reporting (DAAR)** – system for studying & reporting on DNS registration and security threats across top-level domains
- **Domain Name Security Threat Information Collection & Reporting (DNSTICR) –** initially studying COVID-19-related domain registrations to ID names used for phishing/malware
- **Knowledge-sharing & Instantiating Norms for DNS & Naming Security (KINDNS)**
- **Identifier Technologies Health Indicators (ITHI)** – monitoring the health of the registered identifiers ecosystem, https://ithi.research.icann.org/
- **Regional capacity development trainings**

Domain Abuse Activity Reporting

ICANN @ICANN · May 17

#ICANN Reports DNS Abuse is Trending Downward Globally - Domain Name System (DNS) Coordinator Publishes a Report Relying on Four Years of Data. Read our most recent press release, available in all UN languages, here >> go.icann.org/3FUyP3p

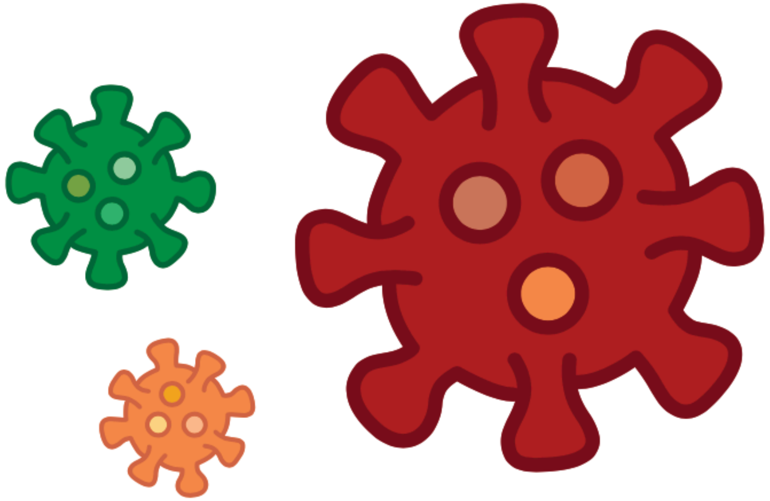
Domain Abuse Activity Reporting (raw counts)



Origins of the DNSTICR project.

During the **COVID-19 pandemic**, criminals phished the vulnerable, the inattentive, the elderly, children, and the less fortunate. These criminals target victims all over the world and in many languages, to steal money and personal information.

Criminals and scammers call, email, or text victims to trick them into revealing their personal information, or into buying fake vaccine IDs, bogus COVID-19 tests, or fake cures.



ccNSO DNS Abuse Standing Committee Survey

20 Sept 2022 – launched survey for ccTLDs on DNS abuse

- **Survey Deadline is 15 October 2022, limited to one response per ccTLD**
- **34 questions, should take no more than 10-15 minutes to complete**
- **Results to be published on the ccNSO website, with ability to opt-out to publication of ccTLD identifier**
- **Go to** https://www.surveymonkey.com/r/DASC0922

Public Comment on Contractual Changes

6 Sept 2022 – proposed amendments to Base gTLD Registry Agreement & Registrar Accreditation Agreement to add RDAP contractual obligations and enable ICANN org to use Bulk Registration Data Access for research purposes (extending DAAR to registrars)

- **In April 2022, ICANN and RySG reached agreement on use of BRDA for research purposes. Now we are going through the process of amending the base Registry Agreement.**
- **Extending DAAR will make it more robust, reliable and useful for analyzing security threat activitiy.**
- **Comments close 24 October 2022**

Opportunities to participate

5th ICANN DNS Symposium

- 14-16 November in Brussels
- IANA Community Day 17 November
- Registration is free and open now; must register in advance to attend in-person

(Source: https://www.icann.org/ids)

Engage with ICANN – Thank You and Questions

ICANN

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann