ICANN DNS Security Threat Mitigation Program Update

Recent and future ICANN efforts to mitigate DNS Security Threats and highlights of ICANN data, trend analysis

22 July 2021

Agenda

- Intro to ICANN's DNS Security Threat Mitigation Program
- ICANN's DNS Security Threat Mitigation Efforts
  - DAAR, DNSTICR,
  - Compliance Audits, Abuse Complaints
  - Work with the Contracted Parties
  - Educational Outreach
- What's next
- Q&A

The DNS Security Threat Mitigation Program

- Ensuring Security, Stability, and Resilience (SSR) of the DNS are foundational aspects of ICANN's purpose and mission.

- ICANN aspires to engender trust in domain names through applying our values and pursuing our mission of ensuring the SSR of the DNS

- Missing Link: Org-Wide Coordination & Collaboration

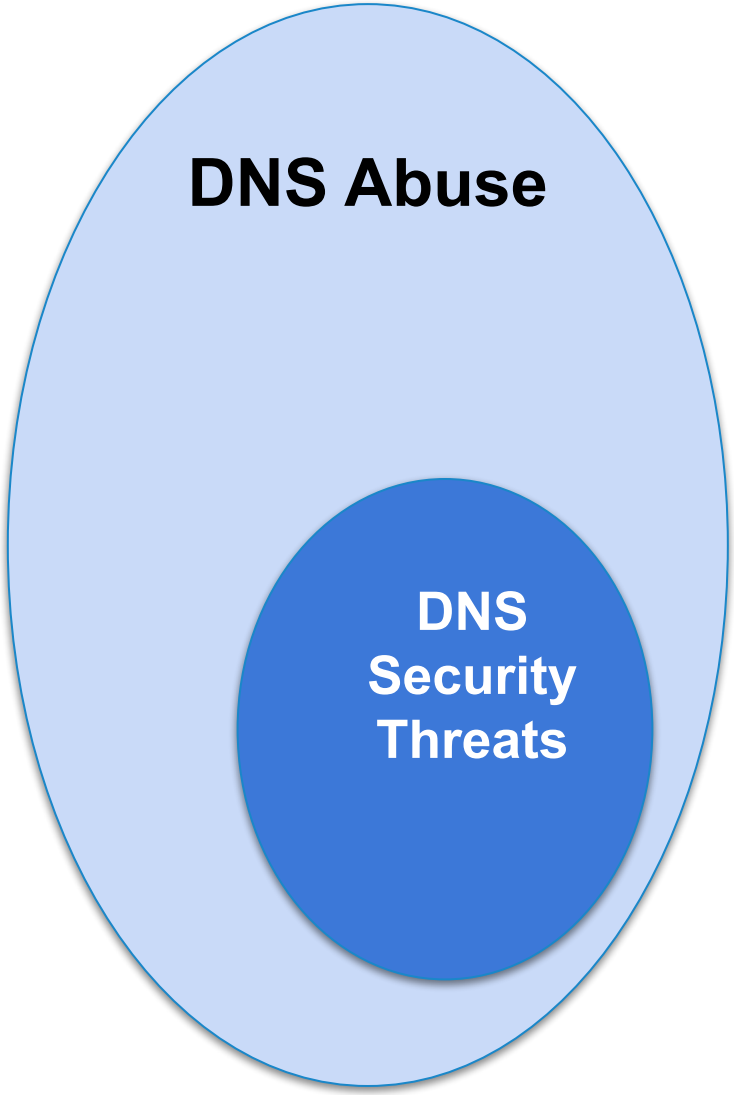
Our Approach

We have three main areas of focus:

Recognized as Trusted Source	Tools for the Community	Enforce Contractual Provisions
Provide objective research, data and expertise to help the community have fact-based discussions	Capacity development, resources, and tools	Audits and Enforcement

DNS Security Threats and DNS Abuse

- **No Consensus Definition of DNS Abuse**
- **Bylaws focus our remit on Security and Stability of the DNS and prohibit content regulation**
- **DNS Security Threats:**
  - Phishing
  - Malware
  - Botnets
  - Pharming
  - Spam (as a vector)



The Program and What We Do

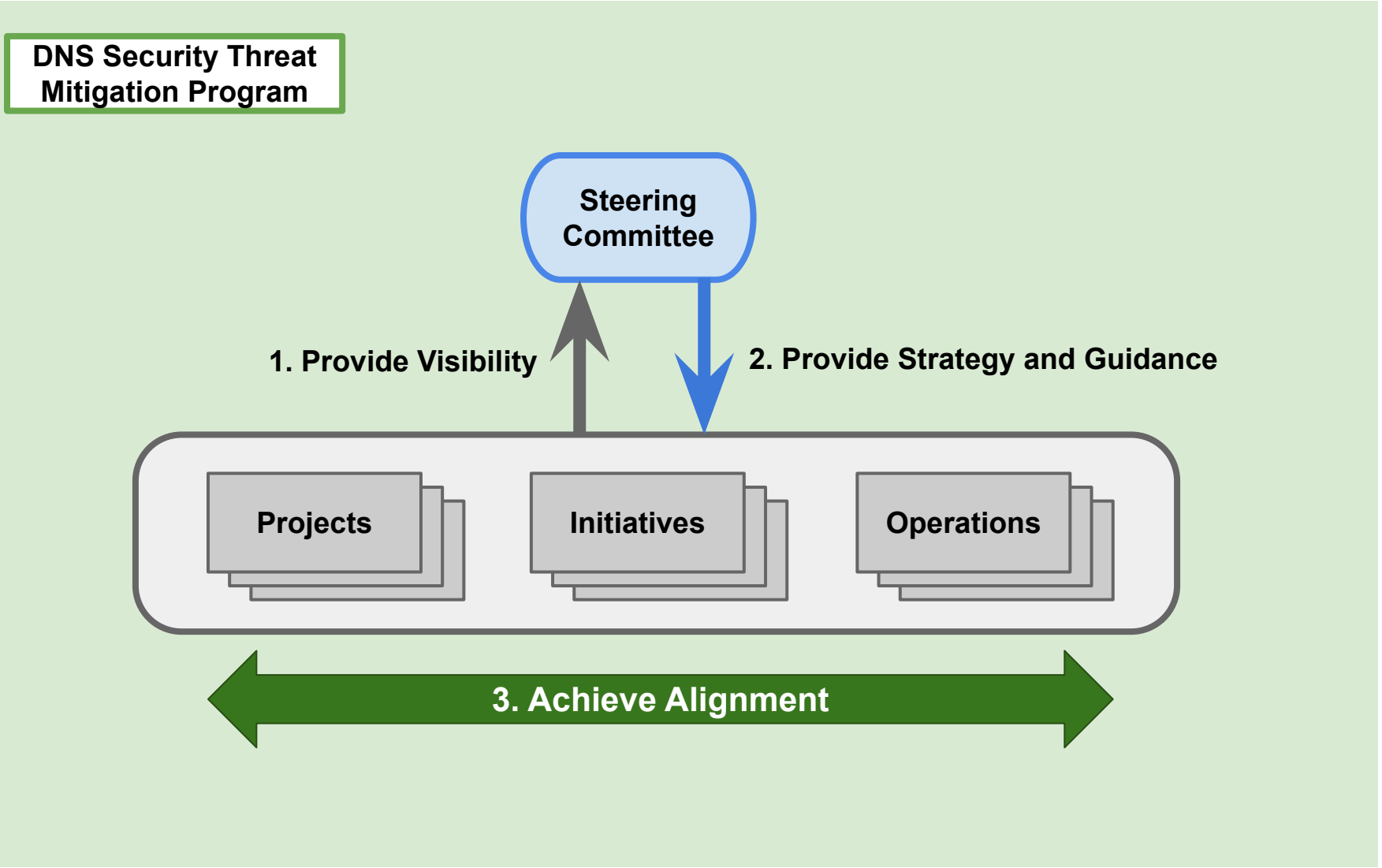
Goal

Make the Internet safer for end users by reducing the rate of DNS security threats across the Internet.

Objectives

- Create a collaborative platform which provides visibility across org's various DNS security threats and abuse related initiatives/projects
- Raise awareness about DNS security threats
- Recognition that ICANN is a trustworthy, fact-based source of data for measurement of DNS security threats in TLDs for which ICANN has data
- Reduce the rate of DNS security threats

Program Governance



Domain Abuse Activity Reporting (DAAR)

- A system for studying and reporting on domain name registration and security threats (domain abuse) across top-level domain (TLD) registries. The overarching purpose of DAAR is to develop a robust, reliable, and reproducible methodology for analyzing security threat activity, which the ICANN community may use to make informed policy decisions.

- Uses a combination of DNS data (Zone Files) and reputation data (Reputation Block Lists)

- Creates *Daily* statistics and *Monthly* reports

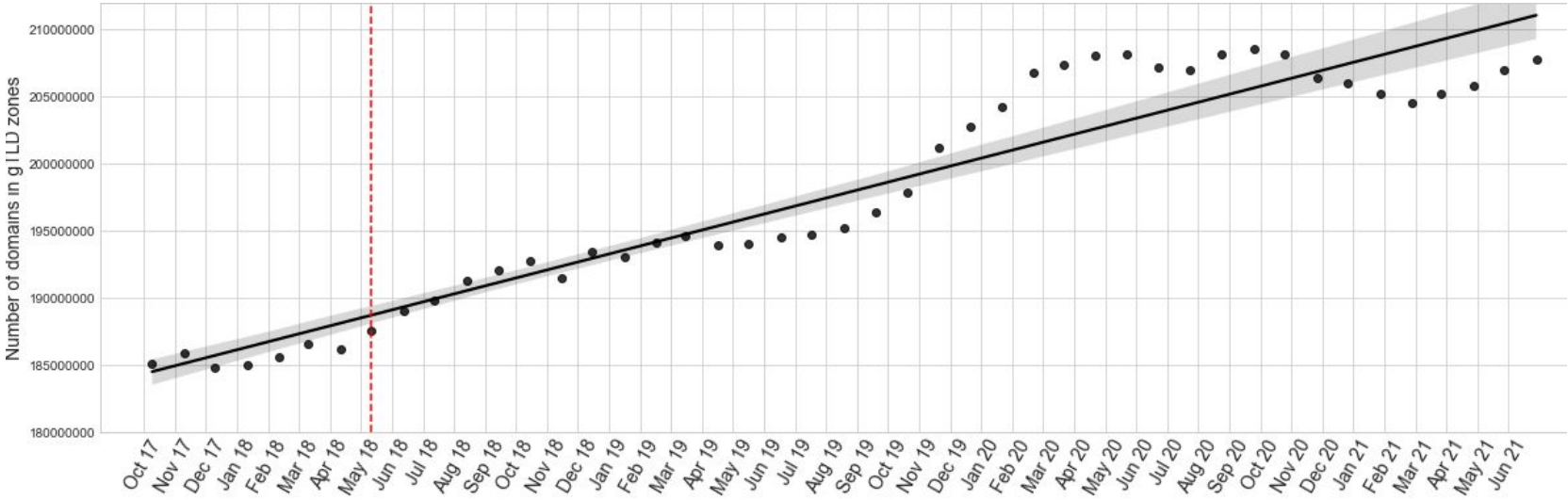
- 17 ccTLDs joined since June 2020

- Currently investigating access to registration data to enable the addition of registrar metrics

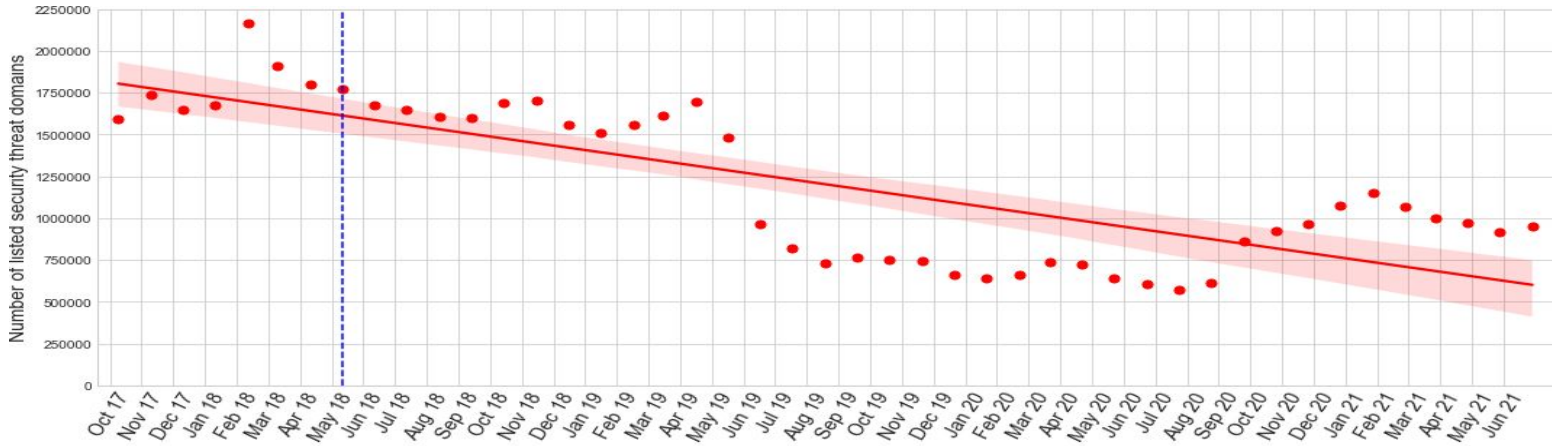
  https://www.icann.org/octo-ssr/daar

Security Threat Distributions over Time

Domains in gTLD zones

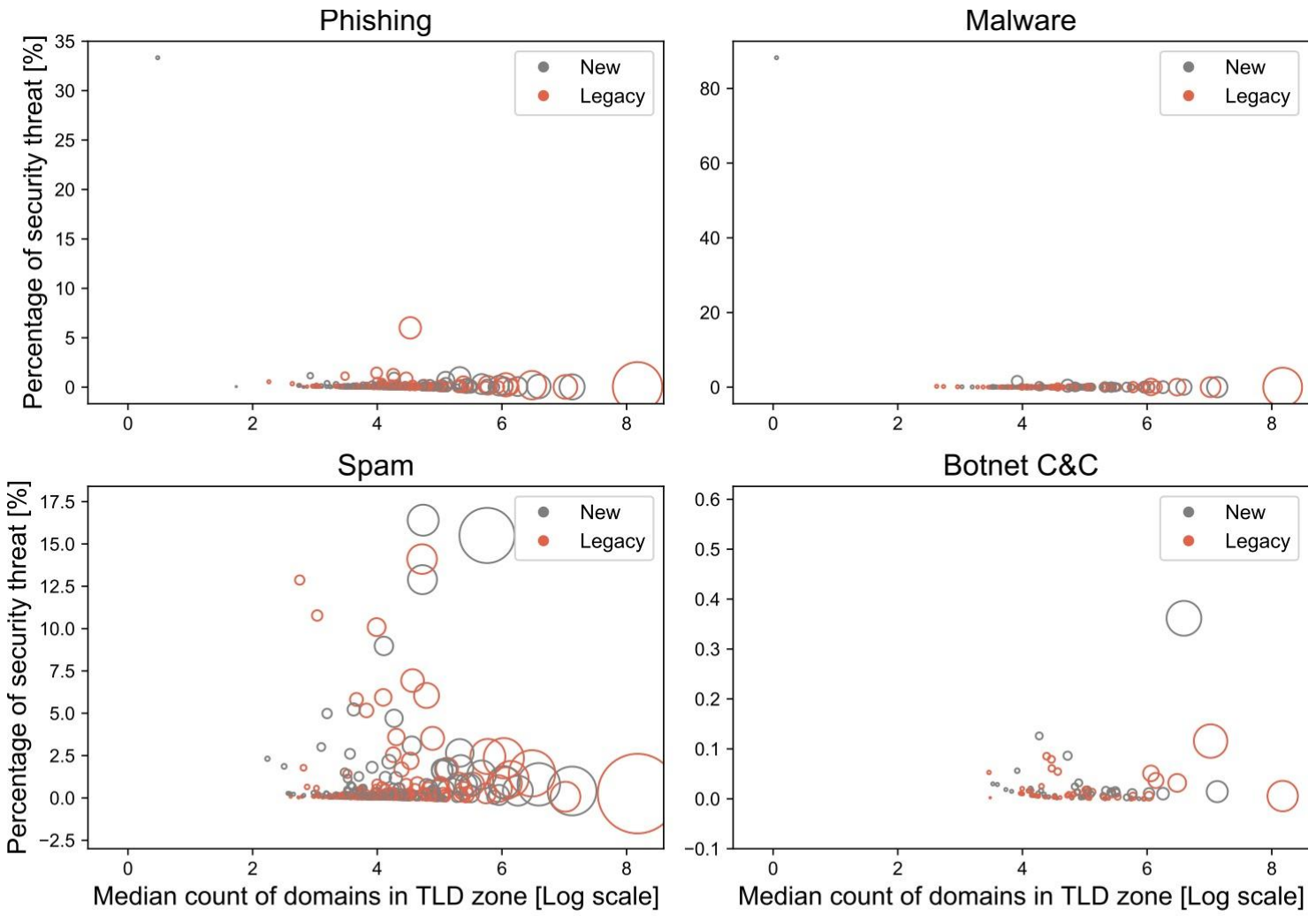


Security threat domains in gTLDs



Security Threat Trends

June 2021



Circle size indicates median threat counts [square root]

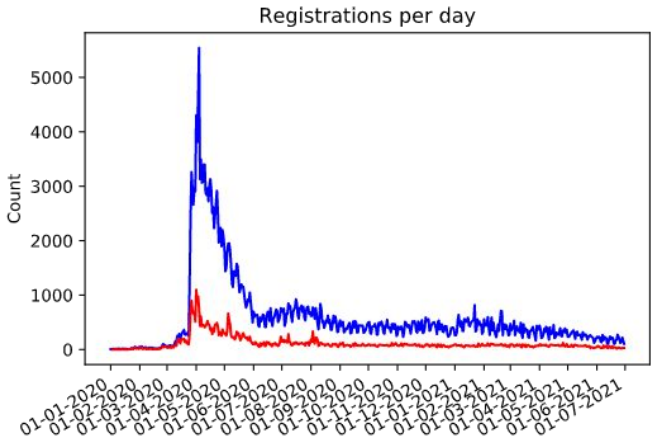
Domain Name Security Threat Identification, Collection and Reporting (DNSTICR)

- Look for malicious registrations related to the pandemic
  - First, filter new registrations (from gTLDs) on a list of terms ("COVID", "pandemic", *etc.;* plus translations)
  - Find evidence from third-party sources (evidence of phishing and/or malware distribution)

- Where sufficient evidence can be found, send a report to the registrar Reports include:
  - The evidence found
  - Screenshots if appropriate
  - Details of DNS (nameservers and IP addresses)

Domain Name Security Threat Identification, Collection and Reporting (DNSTICR)

- January 2020 to July 2021
  - Detected 317,811 pandemic-related domains (both legitimate and malicious)
  - Only phishing and malware distribution
- May 2020 to July 2021
  - Consistent collection and analysis period
    - Detected 204,799 pandemic-related domains (both legitimate and malicious)
    - Of these, 12,439 (6.1%) domains had one or more reports in phishing/malware reputation lists **and** had nameservers or resolved to an IP address
    - High confidence reports: 3,694 (1.8%) domains
- Reporting of high confidence domains to registrars started in June 2020
  - ~300 reports sent to date



Registrations per day matching one or more of our filter terms (blue line) plus those which had one or more third-party reports (red line). Dates in DD-MM-YYYY format.

DNS Security Threat Audits

- Auditing registry and registrar compliance with their contractual obligations is an important means for ensuring that the community's policies (as captured in and incorporated by ICANN's agreements) are implemented and enforced.
- Risk-based approach to audits:

1. November 2018 – June 2019 Audit

Registry Operators compliance with Registry Agreement (RA) obligations related to DNS security threats. Report is published here "Report on the Registry Operator (RO) for Addressing DNS Security Threats",

1. January 2021- July 2021 Audit

Registrar compliance with Registrar Accreditation Agreement (RAA) obligations related to DNS security threats. The report is finalized; results will be discussed in the report, when it is published.

Find more information about ICANN Compliance audits:
https://www.icann.org/resources/pages/audits-2012-02-25-en

Abuse Complaints

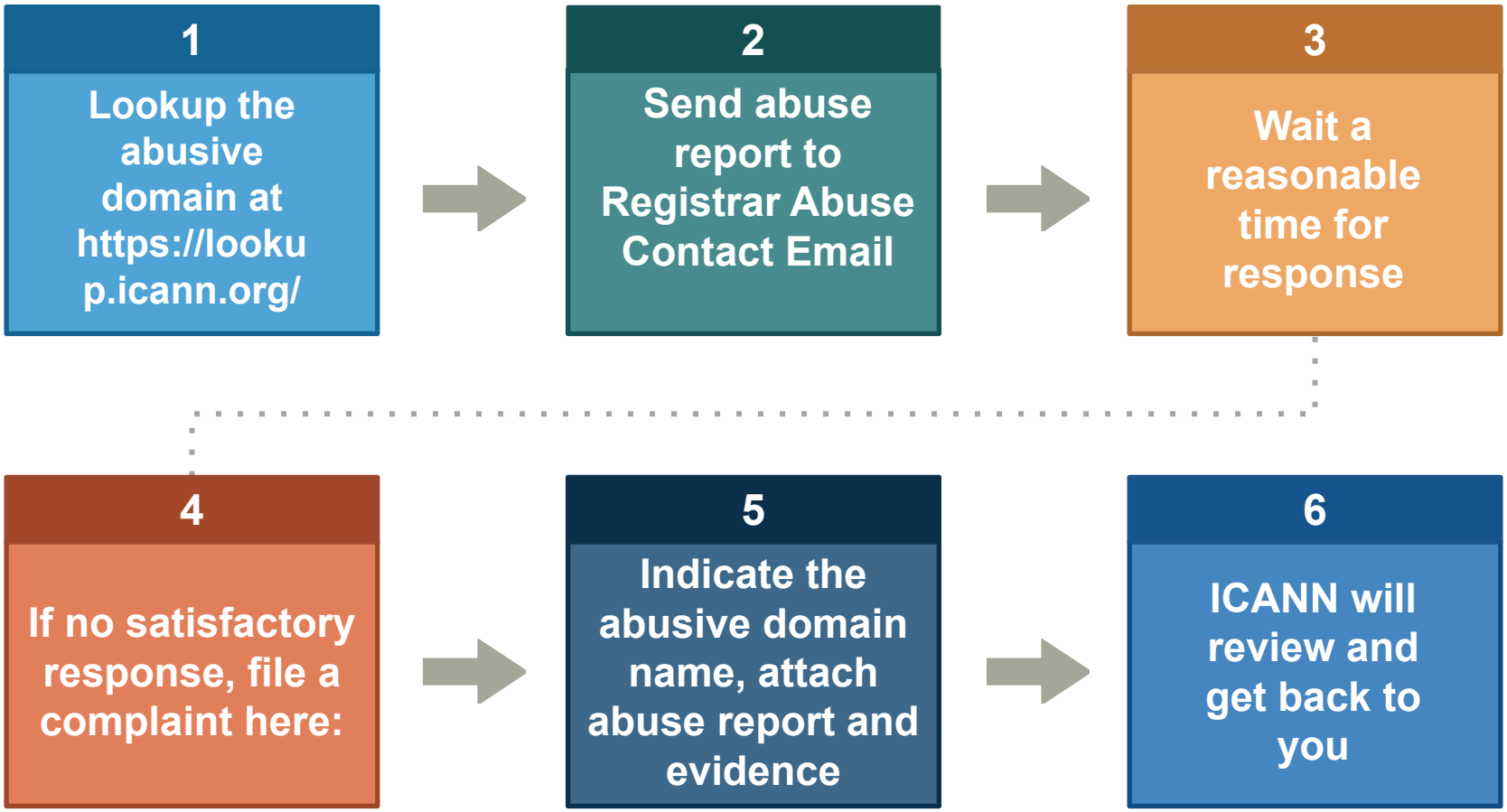
RAA Related Abuse Complaints:

From July 2020 to June 2021, ICANN Compliance:

- Received 3,152 complaints; closed 2,477 complaints without initiating an investigation with the registrar
- Of the 531 complaints that were or could have been addressed by Compliance, 403 (**76%**) involved domain names that were suspended.
- Most registrars demonstrated having taken steps to investigate and respond to the abuse reports in accordance with the registrar's own domain name use and abuse policies.
    - Examples of these steps include: suspending the domain name; providing information to the complainant to report abuse to the entity hosting the content; and terminating the registrar's agreement with the registrant and allowing the transfer to a different registrar.
- No formal notice of breach was issued.

Abuse	JUL-20	AUG-20	SEP-20	OCT-20	NOV-20	DEC-20	JAN-21	FEB-21	MAR-21	APR-21	MAY-21	JUN-21	Total
Received	148	209	256	320	306	249	245	251	273	305	281	309	3,152
Closed Before 1st Notice	250	133	139	171	267	255	237	57	235	117	241	375	2,477
1st Inquiry/Notice	13	48	16	18	20	15	14	6	31	19	11	29	240
2nd Inquiry/Notice	0	0	8	3	3	0	0	6	8	2	3	1	34
3rd Inquiry/Notice	0	0	0	0	0	1	0	0	1	0	0	0	2

Filing an Abuse Complaint with ICANN



https://icannportal.force.com/compliance/s/abuse-domain

Work with the Contracted Parties

- Capacity Development / Information Sharing
- Opportunities for best practices, clarifications or standardization
- Tools and Resources
  - Expedited Registry Security Requests
  - New: Security Response Waiver (registrar)
  - DAAR data via API
- New: Enhanced Registrar Accreditation Application
- New: Registrar DAAR - request to registries for access to data set

Educational Outreach

- Workshops and Conventions
  - Technical Workshops
  - DNS Ecosystem Security, DNSSEC and DNS Abuse Mitigation workshops for ccTLDs, regional partners and public safety entities (64 sessions in 2021 through 1 July 2021)
  - ICANN DNS Symposium (May 2021)

- Collaboration on Measurements and Research Projects
  - Outreach to ccTLDs to join DAAR project
  - Encouraging regional partners to participate in ITHI
  - Presentation on research and measurement conducted by ICANN that impact the DNS security.

- Educational Resources
  - Updated course material on ICANN Learn and training curriculum by ICANN's OCTO Technical Engagement team
  - Formally add DNS Threat mitigation to ICANN training course catalogue.

Next Steps

- Continue the org's work related to mitigation of DNS Security Threats
  - Registrar Audit Final Report
  - Expansion of DNSTICR
  - Enhancements to DAAR
  - Tools for Contracted Parties
  - Capacity Development Events
- Support the Board's understanding of DNS Abuse
  - Technical and remit expertise
  - Assessments of community recommendations

Visit us at
https://www.icann.org/resources/pages/dns-security-threat-mitigation-2021-07-19-en
for more information.

Community Feedback/Q&A

More questions? Send us an email at DNSsecuritythreats@icann.org

Engage with ICANN - Thank You and Questions

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg