DNS Abuse Mitigation

GAC PSWG Speakers:
Laureen Kapin (US Federal Trade Commission, Co-Chair GAC PSWG)
Chris Lewis-Evans (UK National Crime Agency, Co-Chair GAC PSWG)
Gabriel Andrews (US Federal Bureau of Investigation)

GAC Speaker:
Sumitaka SHIRAKABE (Japan, Ministry of Internal Affairs and Communications)

Invited Speaker:
Ivett Paulovics (Co-author of EC DNS Abuse Study)

ICANN73

8 March 2022

ICANN | GAC
Governmental Advisory Committee

Agenda

1. **Why Domain Name System (DNS) Abuse Mitigation is Important**
2. **European Commission Study on DNS Abuse**
3. **Other Recent Developments**
   - DNS Security Facilitation Initiative Technical Study Group
   - SSAC 115 and Domain Name Abuse Institute Centralized Abuse Reporting Tool (CART)
   - Generic Names Supporting Organization (GNSO) Small Team on DNS Abuse
4. **Upcoming: Plenary Session on DNS Abuse**
   - Maliciously registered domains and Compromised domains (Wed. March 9th)
5. **Future Work**
   - Japan input
   - Improved contract provisions
   - Study/assessments/best practices

DNS Abuse Mitigation: Background

Why this is important for the GAC

- **Abuse of the DNS** understood as Security Threats such as *Phishing, Malware, Botnets* (GAC Beijing Safeguard Advice) and as "*intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names*" (CCT Review definition quoted in the GAC Statement on DNS Abuse, 18 September 2019) **constitute**:
  - **A threat to consumers and Internet users** (individual and commercial) and their trust in the DNS
  - **A threat to the security, stability and resiliency of DNS Infrastructure**

- Recognizing the importance of such threats, **the GAC established a Public Safety Working Group** (PSWG) in the ICANN52 Singapore Communiqué (11 February 2015)
  - to focus aspects of ICANN's policies and procedures that implicate the safety of the Public (see ToR)
  - As part of its strategic objectives, as reflected in its Work Plan 2020-2021, the PSWG seeks to: ***Develop capabilities of the ICANN and Law Enforcement communities to prevent and mitigate abuse*** *involving the DNS as a key resource*

- The GAC, the GAC Public Safety Working Group and **many ICANN stakeholder groups prioritize curbing DNS Abuse**, recognizing in particular that **current ICANN contracts do not provide sufficiently clear and enforceable obligations** to mitigate DNS Abuse and need to be improved. This is has been evidenced in:
  - Community discussions with - and statements from - ICANN Contractual Compliance
  - Board correspondence (in particular with the Business Constituency in 2020/2019, see 12 Feb. 2020)
  - GAC Inputs in Reviews (CCT, RDS-WHOIS2, SSR2) and in GNSO PDPs (New gTLD Subsequent Procedures)

Recent Developments: EC DNS Abuse Study (introduction)

- New DNS Abuse Study commissioned by the European Commission (31 January 2022)
- Conducted by a team including a researcher of the CCT Review's mandated Statistical Analysis of DNS Abuse in gTLDs (9 Aug. 2017) of which the GAC lauded the contribution to the *safety, security and stability* of the DNS in a Public Comment (19 Sep. 2017)
- Communicated to the GAC (3 Feb. 2022) and presented during the Pre-ICANN73 PSWG Conference Call (17 February 2022)
- General Observations:
  - Practical perspectives focusing on roles and responsibilities (abused parties; attackers/abusers; intermediaries): Who should Take Action and Why?
  - Echoes recommendations/observations offered by SSAC, CCT and SSR2 Review teams
  - Observes difficulty in making "clear cut distinction between technical (security) and content-related abuses" because in many cases "the borderline is blurred due to the great deal of overlap between different types of abuse."
    - ex: phishing may involve malicious registration and also may involve websites serving malicious content; malware may exploit web vulnerabilities and serve harmful content

EC DNS Abuse Study (presentation by a Study Author)

- Some of the **findings** were presented during the [Pre-ICANN73 PSWG Conference Call] (17 Feb.):
  - **New gTLDs** are "*the most abused group of TLDs*" in relative terms (contrary to **ccTLDs**).
    Two of the most abused New gTLDs concentrate 41% of all abused names in gTLDs
  - The *top 5 most abused **registrars** account for 48% of all maliciously registered domain names*
    There is evidence that registrars and **service providers** being abused can be very responsive to reports of abuse and can take rapid and decisive action, which reduces the impact and harm of the abuse

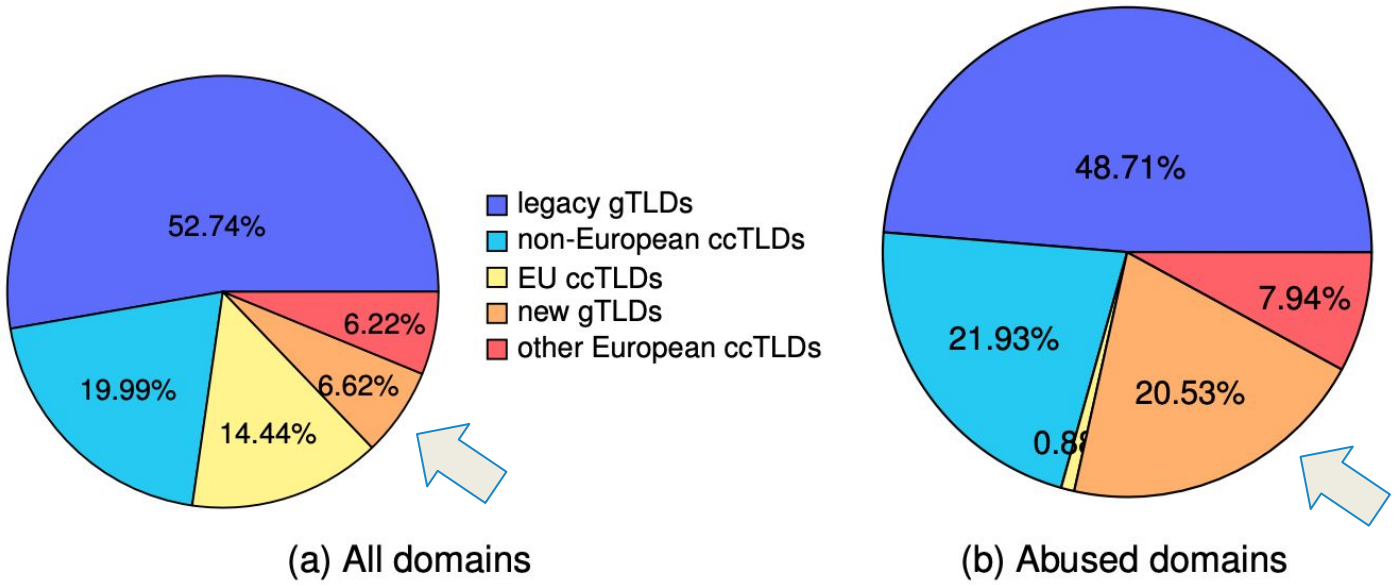


Figure 1: Divison of the domain namespace per TLD type

Recent Developments: DNS Security Facilitation Initiative

DNS Security Facilitation Initiative Technical Study Group

- Report issued mid-October 2021 offering 12 recommended actions ICANN org can take to facilitate and promote better security practices throughout the DNS
- Process: This Study Group examined **real and known** threats to the DNS, focusing on real world incidents (including the "Sea Turtle" DNS hijacking and "DNSpionage" attacks).
- Prioritized Recommendations were:
  - Investigate Appropriate Best Practice for Authentication
    - *ICANN org… should … offer a report on what should be considered best practice for authentication when considered against the different roles and risks in the DNS*
  - Incident Response
    - *ICANN org should, together with relevant parties, encourage the development and deployment of a formalized incident-response process across the DNS industry…*

Recent Developments in DNS Abuse Reporting

19 March 2021, the Stability and Security Advisory Committee (SSAC) published SAC115 , a Report on an **Interoperable Approach to Addressing Abuse Handling** in the Domain Name System.

> **Recommendation 1:** The SSAC recommends that the ICANN community continue to work together with the extended DNS infrastructure community in an effort to (1) examine and refine the proposal for a **Common Abuse Response Facilitator** to be created to streamline abuse reporting and minimize abuse victimization; and (2) define the role and scope of work for the Common Abuse Response Facilitator, using SAC115 as an input.

DNS Abuse Institute's Centralized Abuse Reporting Tool (CART)

- Scheduled for beta testing in March
  - Public launch in ~June?
- Automates routing of abuse complaints
- Enriches reporting

Other Recent Developments

GNSO Small Team on DNS Abuse

- **to consider "*what policy efforts, if any, the GNSO Council should consider undertaking*** *to support the efforts already underway in the different parts of the community to tackle DNS abuse"*
- **to** "***Reach out to others in the community that have been vocal on the topic (such as the Governmental Advisory Committee*** *[...]) to better understand what its expectations are of the GNSO and if/how it expects further policy work to contribute (or not) to the already ongoing initiatives."*
- **Issued invitation to GAC to provide input** by March 21 on:
    - details on what specific problem(s) policy development in particular would be expected to address/why you believe policy development is the right mechanism to solve those problems?
    - expected outcomes if policy development would be undertaken, taking into account the remit of ICANN and more specifically GNSO policy development in this context?
    - any expectations with regards to possible next steps the GNSO Council could or should undertake in the context of policy development?

Upcoming: Plenary Session on DNS Abuse

ICANN73 Plenary Session to discuss Maliciously registered domains and Compromised domains on Wednesday 9 March at 1430 UTC

PST	EST	AST (UTC-4)	UTC	UTC+1	UTC+8	Tuesday 8 March (Day 2)	Wednesday 9 March (Day 3)	Thursday 10 March (Day 4)	AST (UTC-4)
3:30	6:30	7:30	11:30	12:30	19:30	GAC Daily Updates (30 mins) - 07:30-08:00 AST/11:30-12:00 UTC			7:30
3:45	6:45	7:45	11:45	12:45	19:45				7:45
4:00	7:00	8:00	12:00	13:00	20:00				8:00
4:15	7:15	8:15	12:15	13:15	20:15	GAC Leadership Meetings (30 mins) - 08:15-08:45 AST/12:15-12:45 UTC			8:15
4:30	7:30	8:30	12:30	13:30	20:30				8:30
4:45	7:45	8:45	12:45	13:45	20:45				8:45
5:00	8:00	9:00	13:00	14:00	21:00	5. GAC Meeting with the ccNSO (60 mins)	13. GAC Meeting with the ICANN Board (60 mins)	15. GAC Meeting with the ALAC (60 mins)	9:00
5:15	8:15	9:15	13:15	14:15	21:15				9:15
5:30	8:30	9:30	13:30	14:30	21:30				9:30
5:45	8:45	9:45	13:45	14:45	21:45				9:45
6:00	9:00	10:00	14:00	15:00	22:00	Break	Break	Break	10:00
6:15	9:15	10:15	14:15	15:15	22:15				10:15
6:30	9:30	10:30	14:30	15:30	22:30	6. GAC Operating Principles WG (45 mins)	Plenary Session 2: Evolving the DNS Abuse Conversation: Maliciously Registered versus Compromised Domains (90 mins)	14. GAC Communique (4/4) (60 mins)	10:30
6:45	9:45	10:45	14:45	15:45	22:45				10:45
7:00	10:00	11:00	15:00	16:00	23:00				11:00
7:15	10:15	11:15	15:15	16:15	23:15	7. GAC Discussion on WS2 Matters (45 mins)		16. GAC Wrap-Up (30 mins)	11:15
7:30	10:30	11:30	15:30	16:30	23:30				11:30
7:45	10:45	11:45	15:45	16:45	23:45				11:45
8:00	11:00	12:00	16:00	17:00	0:00	Break	Virtual Coffee / Fika	Break	12:00
8:15	11:15	12:15	16:15	17:15	0:15				12:15
8:30	11:30	12:30	16:30	17:30	0:30	8. GAC Discussions on IGO Matters (30 mins)	14. GAC Communique (1/4) (90 mins)	Discussion Forum on Geopolitical Legislative & Regulatory Developments (90 mins)	12:30
8:45	11:45	12:45	16:45	17:45	0:45				12:45
9:00	12:00	13:00	17:00	18:00	1:00				13:00
9:15	12:15	13:15	17:15	18:15	1:15	9. GAC Discussions on WHOIS/Data Protection (60 mins)			13:15
9:30	12:30	13:30	17:30	18:30	1:30				13:30
9:45	12:45	13:45	17:45	18:45	1:45				13:45
10:00	13:00	14:00	18:00	19:00	2:00	Break	Break	Virtual Coffee / Fika	14:00
10:15	13:15	14:15	18:15	19:15	2:15				14:15
10:30	13:30	14:30	18:30	19:30	2:30	10. GAC Public Safety WG Update/DNS Abuse (45 mins)	14. GAC Communique (2/4) (90 mins)	ICANN Public Forum (90 mins)	14:30
10:45	13:45	14:45	18:45	19:45	2:45				14:45
11:00	14:00	15:00	19:00	20:00	3:00				15:00
11:15	14:15	15:15	19:15	20:15	3:15	11. GAC Discussions on Subsequent Rounds (45 mins)			15:15
11:30	14:30	15:30	19:30	20:30	3:30				15:30
11:45	14:45	15:45	19:45	20:45	3:45				15:45
12:00	15:00	16:00	20:00	21:00	4:00	Virtual Coffee / Fika	Break	Break	16:00
12:15	15:15	16:15	20:15	21:15	4:15				16:15
12:30	15:30	16:30	20:30	21:30	4:30	12. GAC Communique Review (60 mins)	14. GAC Communique (3/4) (60 mins)	ICANN Board Meeting	16:30
12:45	15:45	16:45	20:45	21:45	4:45				16:45
13:00	16:00	17:00	21:00	22:00	5:00				17:00
13:15	16;15	17:15	21:15	22:15	5:15				17:15
13:30	16:30	17:30	21:30	22:30	5:30				17:30

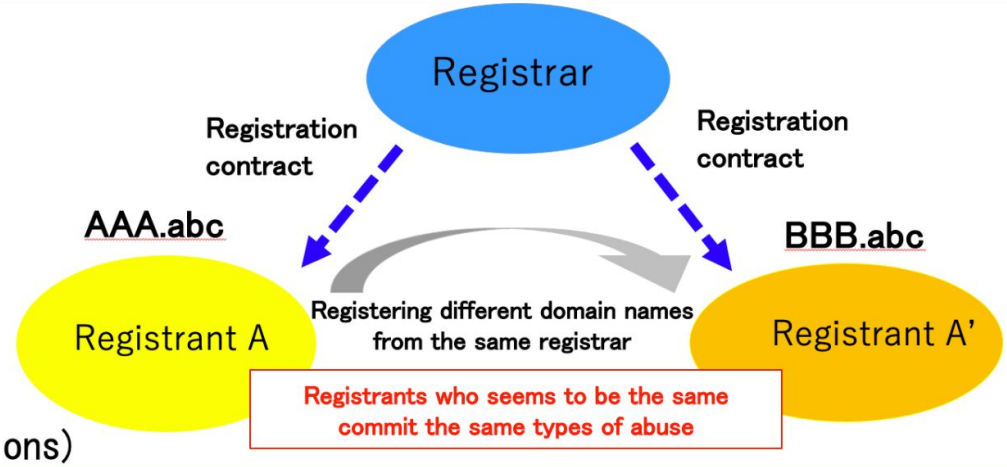
Presentation by Japan (ICANN73)

Current issues of abuse using domain names

0

(Current issues)

- The last ICANN72/GAC meeting, we shared the issue of "Registra Hopping" which a registrant is continuing abuse by transferring the same domain names from one registrar to other registrars.
- As a current issue, we would like to share a case which the registrant who seems to be the same continues abuse by using **different domain names** registered to the same registrar.



(Our suggestions)

○ **Ensuring compliance between ICANN and Registry/ Registrar**

- Collecting information from registrants at the time of domain registration and ensuring the accuracy of the information.
- Conducting an effective and continuous audit on registrars compliance by ICANN Contractual Compliance.

○ **Considering effective measures against abuse using domain names**

- Considering the possibility of using a Trusted Notifier Program.
- Cooperating and discussing against abuse with ICANN's other SO/AC (e.g. Discussions with ALAC)

Future Work

Relevant to any next round of new gTLDs

1. **Improved contract provisions:**

   GAC ICANN72 Communiqué (1 November 202) highlighted as important:

   - "***the need for improved contract requirements to address the issue of DNS Abuse more effectively****. In this regard, ICANN's role under the Bylaws includes duly taking into account the public policy concerns of governments and public authorities and acting for the benefit of the public.*
   - ***The Bylaws also authorize ICANN to negotiate agreements****, including Public Interest Commitments, in service of its Mission. H****ence, ICANN is particularly well placed to negotiate improvements to existing contract****s to more effectively curb DNS Abuse, as informed by the GAC and other stakeholders advocating in the public interest*."

2. **Further assessments of DNS Abuse (causes/responses/best practices)**

   SSAC 114 report recommended "*a study of the causes of, responses to, and best practices for the mitigation of the domain name abuse that proliferates in the new gTLDs from the 2012 round*" ***prior to launching the next round of New gTLDs.***

- interest in quantifying/understanding DNS abuse in certain New gTLDs in order to determine possible mitigations in future rounds

DNS Abuse Mitigation: ICANN73

ICANN73 Objectives (Leadership Proposal For GAC Action in GAC Session Briefing)

1. **Consider the** findings and recommendations of the **DNS Abuse Study published by the European Commission** and presented to the GAC Public Safety Working Group prior to ICANN73 (17 February 2022) **and the DNS Security Facilitation Initiative Technical Study Group - Final Report**
2. Technical Study Group's October 2021 Report
3. **Review progress of ICANN org activities** in relation to DNS Abuse under its DNS Security Threat Mitigation and Contractual Compliance programs, as reported most recently in the Pre-ICANN73 ICANN CEO Briefing to the GAC (16 February 2022).
4. **Assess progress in ICANN community discussions and implementation efforts related to** relevant recommendations from the CCT Review Team, SSR2 Review Team, SSAC Working Party on DNS Abuse, as well voluntary initiatives by Contracted Parties.

Potential ICANN73 GAC Communiqué Issues and Text

- Welcome invitation to GAC by GNSO to provide input to GNSO small group on DNS Abuse
- Welcome voluntary initiatives by contracted parties including Registries Stakeholder group to provide ICANN Org with the data it needs to improve its domain activity abuse reporting tool (DAAR); Domain Generating Algorithms (DGAs) Associated with Malware and Botnets (link) and ongoing cooperation between registrars and law enforcement to respond to abuse

Review our Expected Standards of Behavior when participating in ICANN Meetings.

Go to:
http://go.icann.org/expected-standards

Review the ICANN Community Anti-Harassment Policy when participating in ICANN Meetings.

Go to:
http://go.icann.org/anti-harassment

Do you have a question or concern for the ICANN Ombudsman?

Email ombudsman@icann.org to set up a meeting.

ICANN