DNS Abuse Mitigation

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

GAC Speaker:
Teruyuki SHIBATA (Japan, Ministry of Internal Affairs and Communications)

Invited Speaker:
Graeme Bunton (DNS Abuse Institute)

ICANN74

14 June 2022

ICANN | GAC
Governmental Advisory Committee

Agenda

1. **Why Domain Name System (DNS) Abuse Mitigation is Important**
2. **Trends in Abuse**
   - Recent statistics
   - Presentation by Japan
3. **Operational perspective and initiatives**
4. **Briefing on Centralized Reporting of Abuse (DNS Abuse Institute)**
5. **ICANN and the community's roles**

DNS Abuse Mitigation: Background

Why this is important for the GAC

- **Existing definitions of Abuse of the DNS** include 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**

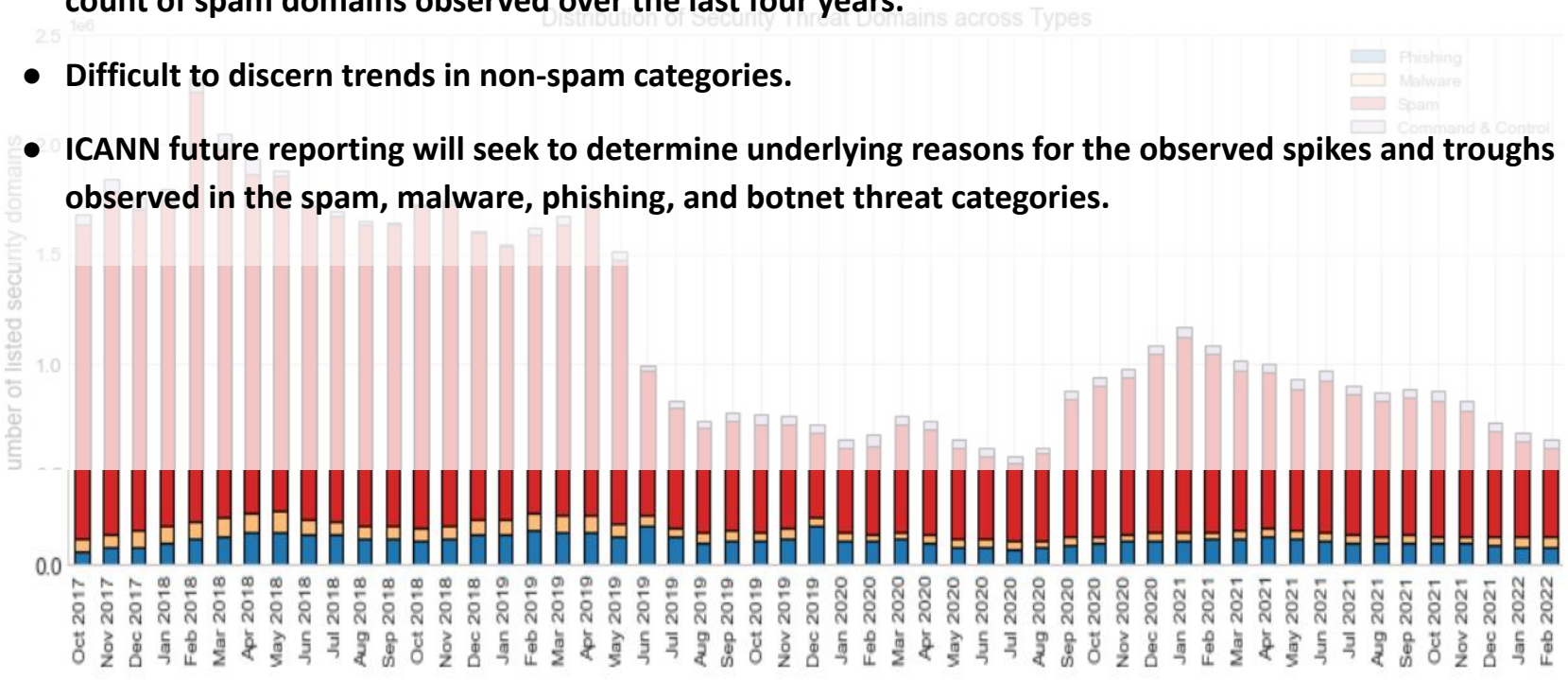
- Recognizing the importance of such threats, **the GAC established a Public Safety Working Group** (PSWG) in the ICANN52 Singapore Communiqué (11 February 2015)
  - to focus aspects of ICANN's policies and procedures that implicate the safety of the Public (see ToR)
  - As part of its strategic objectives, 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)

DNS Abuse Updates

ICANN Org Report: The Last Four years in Retrospect: A brief Review of DNS Abuse Trends

- **ICANN Org used Reputation Blocklists (RBLs) to count the number of domains having been reported as used in "phishing, malware, botnet command and control and spam as a delivery mechanism"**
- **Spam domains greatly outnumbered the other three categories combined, and indicated a decline in the count of spam domains observed over the last four years.**
- **Difficult to discern trends in non-spam categories.**
- **ICANN future reporting will seek to determine underlying reasons for the observed spikes and troughs observed in the spam, malware, phishing, and botnet threat categories.**



Close zoom of phishing and malware trends (Spam and botnet C2 data truncated)

Source: https://www.icann.org/en/system/files/files/last-four-years-retrospect-brief-review-dns-abuse-trends-22mar22-en.pdf

Presentation by Japan (1/2)

Recent trends **in** abuse using domain names

(Issues)

- **We would like to share cases in which registrants are abusing domain names and are "hopping" more rapidly.**
- **Abuse using domain names tends to be concentrated in a few specific registrars.**
- **Some registrars are not aware that they are being abused, so we have to carry out further publicity activities.**

Shifting of major piracy site (Ranking table indicates access counts)

	2021/12	2022/2	2022/4
Website A	1st	1st	**Shut down**
Website B	2nd	2nd	**Shut down**
Website C	3rd	3rd	**Out of range**
Website D	4th	5th	4th
Website E	5th	6th	5th
Website F	6th	4th	**Shut down**
Website G	7th	9th	**Shut down**
Website H	8th	10th	8th
Website I	9th	8th	**Out of range**
Website J	10th	7th	6th

Registrars used by major piracy sites
(10 most **accessed sites each month.**)

	2021/10	2021/12	2022/2	2022/4
Registrar V	**4**	**4**	**3**	**3**
Registrar W	**2**	**2**	**2**	**1**
Registrar X	**2**	**2**	**3**	**2**
Registrar Y	1	1	1	1
Registrar Z	0	1	1	2
Unknown	1	0	0	1

Some major sites have been shut down, but new similar sites have been opened and accessed by a large number of visitors in **2 months.**

Concentrated in specified **3 registrars**

(Suggestions)

○ **Ensuring compliance between ICANN and Registrars / Possibility of further application**
- **Confirm the accuracy of information collected from registrants.**
- **Take prompt steps to investigate and respond appropriately to reports of abuse.(RAA 3.18.1)**
- **Continually conduct audits and follow-up on registrar compliance by ICANN Contractual Compliance.**

○ **Amendment of Registrar Accreditation Agreement (RAA)**
- **Consider the addition of "registrars confirm the accuracy of information collected from registrants."**

Presentation by Japan (2/2)

What does “data free flow with trust” mean?

G20 Osaka Summit

Cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development. At the same time, we recognize that the free flow of data raises certain challenges. **By continuing to address challenges related to privacy, data protection, intellectual property rights, and security, we can further facilitate data free flow and strengthen consumer and business trust.** In order to build trust and facilitate the free flow of data, it is necessary that legal frameworks both domestic and international should be respected. Such **data free flow with trust** will harness the opportunities of the digital economy. **We will cooperate to encourage the interoperability of different frameworks, and we affirm the role of data for development.**

data free flow with trust

Data free flow should be facilitated to harness the opportunity of the digital economy.

Strengthening ‘trust’ by continuously addressing challenges related to privacy, data protection, intellectual property rights will facilitate data free flow.

Operational perspective and initiatives

- **Addressing DNS abuse remains a challenge**
  - PSWG met with Europol and EU law enforcement to discuss the value of participating in ICANN
    - Addressed the impact of DNS abuse
- **Current and future initiatives to address DNS abuse**
  - Voluntary initiatives (within and outside of ICANN)
    - DNS Security Facilitation Initiative Technical Study Group (DSFI-TSG)

      Recommendation E5 pointing towards a information sharing platform
  - Need for structural solutions, including improved contract provisions

Briefing on Centralized Reporting of Abuse

[Presentation by the DNS Abuse Institute]

DNS Abuse Mitigation: ICANN's Role and Contracts

What is ICANN's role?

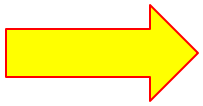
Defined in Articles of Incorporation, Bylaws and Contracts with Registries/Registrars

- Not-for-profit public benefit corporation, promoting the global public interest in the operational stability of the Internet
- Mission: ensure the stable and secure operation of the Internet's unique identifier systems
- May negotiate, enter into and enforce agreements, including public interest commitments, with any party in service of its Mission
- Commits to duly taking into account the public policy advice of governments and other public authorities

DNS Abuse Mitigation: ICANN's Role and Contracts

Current contracts:

- ICANN's standard Registry Agreement required new gTLD registry operators to include provisions in their Registry-Registrar Agreements (RRA) that prohibited registrants from:
  - distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law
    - but need more than obligations to include language in downstream contracts; need need enforceable provisions regarding how to respond to DNS abuse
- Registry Operators must "periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, **such as** pharming, phishing, malware, and botnets."
  - but what needs to happen next?
- ICANN's standard contract for Registrars requires registrars to promptly "investigate and respond appropriately to any reports of abuse"
  - Board 2/20 letter: "The RAA does not define, with any specificity, what "reasonable and prompt steps to investigate and respond appropriately" means.



Need for discussions focusing on reporting, handling, and enforcement of contract terms focusing on DNS Abuse