Update on work by the GNSO Council Small Team on DNS Abuse

Fourth Presentation to the At-Large CPWG

Justine Chew
Member, GNSO Council Small Team on DNS Abuse

19 April 2023

Recap: Outreach on DNS Abuse

- Work assignment of Small Team of GNSO Councilors includes:
  - Outreach to ACs, SG/Cs, ICANN Contractual Compliance, DNS Abuse Institute (DNSAI)
  - Understanding landscape of DNS Abuse – which elements appear inadequately mitigated
  - Identify what might be in scope for GNSO policy making
  - Recommending to Council on next steps

- Feb 2022 – 7 Oct 2022 Report to GNSO Council [1], action based 3 buckets:
  - Issues that may benefit from GNSO policy development
  - Issues that may benefit from education/communication/outreach
  - Issues that may benefit from ICANN org - Contracted Parties contractual negotiations

- 6 Jan 2023 further targeted outreach [2] [3] on:
  - Targeted contractual amendments with (i) RySG (RA Spec 11(3)(a)) and (ii) RrSG (on RAA sec 3.18.1)
  - Bulk registrations with (i) RrSG, (ii) RySG, (iii) DNSAI, (iv) ICANN Contractual Compliance
    - Role of bulk registrations in DNS Abuse?
    - What further work to address potential issues with bulk registrations in DNS Abuse?
    - What measure are in place wrt bulk registrations (threshold, restrictions, checks etc)? What have been effective in constraining malicious actors? Might adoption of these be encouraged on voluntary basis or mandatory through policy? Any harm on adoption?

1- https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf

2- https://gnso.icann.org/sites/default/files/policy/2023/correspondence/ducos-to-demetriou-et-al-06jan23-en.pdf

3- https://gnso.icann.org/sites/default/files/policy/2023/correspondence/ducos-to-heineman-et-al-06jan23-en.pdf

Feedback on Contractual Amendments Negotiations

- 7 Mar 2023 CPH (RySG & RrSG) combined reply [4]
  - RySG (RA Spec 11(3)(a))

    On *"include a provision in their agreement with registrars,". This requirement is limited to the inclusion of the provision. However, further consideration may need to be given to what Registries are doing to ensure the text is indeed included in the Registration Agreement (i.e. Registries enforcing their own Registry-Registrar Agreements).*

    - CPH do not believe there are any interpretation of enforceability gaps – obligations are audited by ICANN Contractual Compliance
    - The pass-through provisions extend beyond DNS Abuse and include website content abuse falling outside current effort by CPH to better address DNS Abuse
  - *Cf* Prior feedback from ICANN Contractual Compliance [5]
    - RAA does not prescribe specific consequences that Rrs must impose on DN that are subject to abuse report – so, CC has no contractual authority to demand imposition or specific action by Rrs
    - RA Spec. 11, s. 3(a) only requires RO to compel Rr-registrant agreement to prohibit registrants from engaging in certain activities with threat of DN suspension – does not provide ICANN org with authority to instruct Rr to impose consequences.
    - In summary, CC does not face any challenges in enforcing the RAA and RA obligations as they are written. If and when new obligations are imposed either through community policy development or new contractual terms, CC will enforce those as well so long as they are unambiguous and enforceable

4- https://gnso.icann.org/sites/default/files/policy/2023/correspondence/bacon-to-ducos-et-al-13mar23-en.pdf
5- https://gnso.icann.org/sites/default/files/policy/2023/correspondence/hedlund-to-ducos-22feb23-en.pdf

Feedback on Contractual Amendments Negotiations

- 7 Mar 2023 CPH (RySG & RrSG) combined reply [4]
  - RrSG (on RAA sec 3.18.1)

    On "Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse"), it is unclear what "reasonable", "prompt", and "appropriately" mean, even though ICANN Compliance indicated that they enforce in the case of inaction. The ICANN Compliance response also indicated that "(t)he RAA does not require registrars to take any specific action on the domain names that are subject to abuse reports." And that "(t)he RAA does not prescribe the specific consequences that registrars must impose on domain names that are subject to abuse reports though". This interpretation may allow DNS abuse to remain unmitigated, depending upon the registrar's specific domain name use and abuse policies.

    - Part of current ongoing contractual negotiations with ICANN

4- https://gnso.icann.org/sites/default/files/policy/2023/correspondence/bacon-to-ducos-et-al-13mar23-en.pdf

Also on Contractual Amendments Negotiations

- Parallel Developments
  - 20 Jan 2023 BC-IPC-ALAC letter to the Board [6]
    - On enhancements to DNS Abuse obligations for RA and RAA – encourage ICANN Org and Contracted Parties to remain open to future negotiations to address existing and evolving types of abuse which fall outside the Contracted Parties' proposed definition of DNS abuse.
    - Requested for transparency of contractual negotiations to the community and opportunity to contribute to efforts.
  - 27 Mar 2023 Reply from Board to BC-IPC-ALAC [7]
    - Taking this approach to make focused improvements to the Agreements, to add a clear obligation for registries and registrars to mitigate DNS abuse, will be an important building block in a longer journey that envisions potential policy discussions open to the full ICANN community, and potentially future negotiations between the CPH and ICANN org
    - ICANN org – Contracted Parties proposed amendments will be available for public comment when ready
    - Board considering coordinating a listening session once proposed amendments are available for public comment

4- https://gnso.icann.org/sites/default/files/policy/2023/correspondence/bacon-to-ducos-et-al-13mar23-en.pdf
6- https://www.icann.org/en/system/files/correspondence/cole-et-al-to-sinha-costerton-20jan23-en.pdf
7- https://www.icann.org/en/system/files/correspondence/sinha-to-cole-et-al-27mar23-en.pdf

Feedback on Bulk Registrations

- ICANN Contractual Compliance [8]
  - ICANN agreements and policies do not contain requirements or limitations related to registering domain names in bulk. As a result, ICANN Contractual Compliance does not collect or track information on bulk registrations.
  - Complaints involving large numbers of domain names are addressed through the same process as those involving single domain names.

- DNS Abuse Institute - DNSAI [9]
  - DNSAI does not currently have any statistics or evidence on bulk registrations – to conduct some exploratory research on their existing data to see if can identify bulk registrations – can do the same if others have data.
  - But there's no consistent definition of bulk registrations – no particular effort to define concept clearly – difficult to scope research needed to determine scale of issues related to bulk registrations
  - Points to some work done on Domain Generating Algorithms (DGAs) but DGAs are small subset of what could be "bulk registrations"
  - Substantial diversity within Rr ecosystem on how registrars address this and architects their registration flow – anti-fraud tools in processing payments, transactional attributes to flag fraudulent transactions
  - Supportive of payment-based techniques and technologies being voluntarily adopted
  - Maybe encourage Rrs to investigate all domains in customer account where one is identified as malicious?

8- https://gnso.icann.org/sites/default/files/policy/2023/correspondence/hedlund-to-ducos-22feb23-en.pdf
9- https://gnso.icann.org/sites/default/files/policy/2023/correspondence/bunton-to-ducos-27feb23-en.pdf

Feedback on Bulk Registrations

- Registry Stakeholders Group - RySG [10]
  - Hard to comment because no definition of “Bulk registrations”
  - DNS Abuse management is resource-heavy endeavor, evidence based escalation remains preferred avenue for management and escalation processes at registry level
  - Also points to some work done on Domain Generating Algorithms (DGAs) but use of DGAs are rarely carried out in bulk – DGAs sometimes result in large number of registrations spread across a prolonged period, various registrars, and multiple registrant accounts – reliance on third party expertise
  - Examples of effective responses to DGAs as part of existing, established anti-abuse escalation paths – international coordinated law enforcement actions (eg. Conficker, Avalanche etc) - existing work by RySG – GAC PSWG in defining prudent and effective framework in handling such DGA type situations.
  - Not sure of Council’s expectations on this

- Registrar Stakeholders Group - RrSG [11]
  - “Bulk registration” not defined or definable, not considered to be a trackable statistic for measuring or otherwise addressing DNS Abuse – changing landscape of malicious activity
  - Rrs have better ways to combat malicious registrations – fraudulent banking transactions a significant flag, IP address tracking, KYC/personal relationship with customers
  - Restricting domain purchases or adopting policies against “bulk registrations” may not be effective, and may harm diversity of business models

10- https://gnso.icann.org/sites/default/files/policy/2023/correspondence/woods-to-ducos-03mar23-en.pdf
11- https://gnso.icann.org/sites/default/files/policy/2023/correspondence/heineman-to-ducos-13mar23-en.pdf