ICANN 71
VIRTUAL POLICY FORUM
14–17 June 2021

# CPH DNS Abuse Work Group Community Outreach

# CPH DNS Abuse WG Community Outreach

| No. | TOPIC | LEAD |
|---|---|---|
| 1 | Welcome and Introduction | James Galvin, Donuts |
| 2 | Summary of takeaways from CPH DNS Abuse outreach sessions | Chairs |
| 3 | Update on Work Outputs:<br>● RySG<br>● RrSG | Various |
| 4 | CPH Questions for the community | James Galvin, Donuts |

# Outreach Sessions - Key Takeaways

| GROUP | TAKEAWAYS FOR WORK OUTPUT |
|---|---|
| NCSG | *Kick off session, output to be considered at future meetings* |
| ALAC | Education materials for internet users on DNS Abuse |
| IPC | IDN homoglyph domain attacks; incentive programs; Framework on trusted notifiers |
| BC | Framework on trusted notifiers; Expand on guide to abuse reporting |
| Community | Website for DNS Abuse resources |

# Outreach Sessions - Upcoming Plans

- First meetings after ICANN71
  - ccNSO
  - ISPCP
  - SSAC
- Next meetings are being scheduled
  - BC
  - IPC
- Ongoing meetings
  - PSWG
  - OCTO

# RySG Output on DNS Abuse

| TOPIC | REFERENCE |
| --- | --- |
| Recommendations for DAAR | TTL on DAAR listed domains; Adding registrars |
| Education: Registry Actions for DNS Abuse | • Registry Operator Available Actions |
| Collaboration with PSWG | • Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets<br>• Framework for Registry Operators to Respond to Security Threats |
| Trusted Notifiers (joint with RRSG) | • Working group to develop Framework on Trusted Notifiers<br>○ Sets forth key aspects of relationship<br>○ Recommended practices for engaging |
| CCTRT Recommendations | • Review of CCTRT recommendations as relates to DNS Abuse |
| IDN Homoglyph Attack | • Issues associated with homoglyph attacks |

# Registry Operator Available Actions

- General community education materials
- Details the technical options available to a Registry Operator when DNS Abuse is identified (e.g., suspend, transfer, or lock)
- Notes the difference between maliciously registered domains vs. compromised domain names
- Touches on DGA mitigation (create/reserve domain names)

# Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets

- Some of the largest and most dangerous botnets - such as Conficker and Avalanche - have been controlled via the use of Domain Generation Algorithms (DGAs)
- Domain Generation Algorithms (DGAs)
  - are tools which ‘input’ a specific date and time, and ‘output’ a domain name for that specific time.
- Law Enforcement (LE) action vs Botnets
  - Low Frequency / High Impact events
  - each domain only needs to be seized for a short duration at the specific date/time specified by the DGA.
- Improving upon DGA referrals was identified by PSWG/RySG as “low hanging fruit” / attainable goal
  - Recommends voluntary & non-binding Best Practices
  - Streamlining for an **EVERGREEN** solution
    - One action / referral by LE to Ry’s, and by Ry’s to ICANN, enabling **EVERGREEN** action going forward for that DGA.
      - Avoiding wherever possible the need to keep "coming back to the well"
- Thanks to ICANN for willingness their feedback and guidance on engaging the “Expedited Registry Security Request” mechanism

# Framework on Trusted Notifiers

- Joint effort between RySG and RRSG DNS Abuse Working Groups
- Response in part from outreach, community concern regarding the need for clarity around the use of Trusted Notifiers
- Aims to provide clarity around the relationship between a Trusted Notifier and a registry or registrar that accepts notices from a TN
    - How does an entity become a TN?
    - What due diligence should a TN undertake?
    - How is the TN relationship documented?
    - What safeguards are in place for registrant protection?

# CCTRT Recommendations Working Group

- Recently formed working group; we know these recommendations are of great interest to the Community
- Seeks to review the recommendations as specifically related to DNS Abuse
  - What has been directly implemented?
  - What related community work has been done or is in progress?
- Chaired by Jeff Neuman

# IDN Homoglyph Attacks Working Group

- Also known as script spoofing, exploits Unicode “letters” that look identical or nearly identical to deceive the end user
  - icɑnn.org (xn--icnn-r5b.org) uses Latin small alpha A
  - icann.org (xn--iann-513a.org) uses Latin small capital C
- Identified in outreach with IPC as area of shared concern
- Jointly chaired by Dennis Tan (RYSG) and Brian King (IPC/RRSG)

# RrSG Output on DNS Abuse

| TOPIC | STATUS |
|---|---|
| Guide to Registrar Abuse Reporting<br>https://rrsg.org/wp-content/uploads/2020/03/Guide-to-Registrar-Abuse-Reporting-v1.8.pdf | **PUBLISHED** |
| Registrar Approaches to the COVID-19 crisis<br>https://rrsg.org/wp-content/uploads/2020/03/Registrar-approaches-to-the-COVID-19-Crisis.pdf | **PUBLISHED** |
| Minimum Required Information for whois Data Requests<br>https://rrsg.org/wp-content/uploads/2020/10/CPH-Minimum-Required-Information-for-a-Whois-Data-Requests.docx.pdf | **PUBLISHED** |
| Incentive Programs for Combatting DNS Abuse<br>Questionnaire: https://forms.gle/AgiHgbgrg2wixJrSA | **Questionnaire out for community response** |
| Registrant Protections | **Draft in review with ALAC, NCUC & PSWG** |
| Approaches to business email compromise (BEC) scams | **Draft in review with BC & PSWG** |
| Triage tool for registrants dealing with DNS Abuse | **IN DISCUSSION** |
| Registrar attributes for trusted notifiers | **IN PROGRESS WITH RYSG** |
| IDN homoglyph domain attacks | **IN PROGRESS WITH RYSG** |

# RrSG Published Papers

**Guide to Registrar Abuse Reporting**

https://rrsg.org/wp-content/uploads/2020/03/Guide-to-Registrar-Abuse-Reporting-v1.8.pdf

**Registrar Approaches to the COVID-19 crisis**

https://rrsg.org/wp-content/uploads/2020/03/Registrar-approaches-to-the-COVID-19-Crisis.pdf

**Minimum Required Information for whois Data Requests**

https://rrsg.org/wp-content/uploads/2020/10/CPH-Minimum-Required-Information-for-a-Whois-Data-Requests.docx.pdf

# RrSG Draft Papers out for Review

## Incentive Programs for Combatting DNS Abuse

- the RrSG is in process of drafting a discussion paper that frames key issues and attributes associated with incentivization programs
- Before publishing, we would like community input on some very basic questions (see https://forms.gle/AgiHgbqrq2wixJrSA):
  - Are anti-DNS Abuse incentivization programs desirable?
  - What protections should be in place for Registrants?
  - What additional aspects should be considered for an effective incentives program?
- Once the paper is completed, we hope to publish it for further discussion with the ultimate goal being to develop a set of guidelines for a robust approach for a potential incentivization mechanisms for reducing DNS abuse.

# RrSG Draft Papers out for Review

**Registrant Protections**

- Highlights protections to ensure registrants are not subject to unfounded abuse complaints and have the ability to “appeal” actions against abuse through various mechanisms:
  - All DNS abuse complaints should be based on material, actionable reports that include verifiable evidence.
  - Internal, support-based appeals (e.g. through customer support flow)
  - Internal ombuds
  - Courts of competent jurisdiction (including public ombuds, consumer agencies, or law enforcement)
- Not intended to facilitate or protect abuse
- Draft paper is currently in review with ALAC, NCUC & PSWG

# RrSG Draft Papers out for Review

**Approaches to Business Email Compromise (BEC) scams**

- Draft paper is currently in review with BC & PSWG
- BEC Fraud: how to hack humans/people
- Not as frequent as phishing, but has the highest impact
- Example of simplicity
- Approaches to combat BEC Fraud
- Tooling
- Procedures and education

# RrSG Topics In Progress

**Triage tool for registrants dealing with DNS Abuse**

For malware, botnet, phishing and farming the best point of contact is:
* Hosting provider details

For spamming the best point of contact is:
* Email provider details

If you want to contact the registrant and report the abuse to the registrar please refer to:
* RDAP output

# Other RrSG Papers/Topics In Progress

Work on the following topics is a joint effort between RrSG & RySG DNS Abuse Groups:

**Registrar attributes for trusted notifiers**

**IDN homoglyph domain attacks**

# CPH Definition of DNS Abuse

**DNS Abuse** is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the other forms of DNS Abuse.

Full details are available on the RrSG website and the RySG website:

**DNS Abuse** is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the other forms of DNS Abuse.

1) What information do you use and how do you use it to assess DNS Abuse levels?
2) What are your concerns regarding DNS Abuse?
3) Are you seeing practices from registrars or registries you find helpful?