ICANN 78 ANNUAL GENERAL MEETING

CPH DNS Abuse Community Outreach

22 October 2023

ICANN | RrSG
Registrar Stakeholder Group

RySG
gTLD Registries Stakeholder Group

01

Welcome and Overview

Brian Cimbolic (RySG DNS Abuse Group co-Chair)

Meeting Agenda

No.	Topic	Lead
1	Welcome and Overview (5 mins)	Brian Cimbolic (RySG DNS Group co-chair)
2	RA/RAA DNS Abuse Amendments (40 mins) - Why is it happening? - What changes are being made? - Voting on the amendments - What does it all mean?	Owen Smigelski (CPH Negotiation Lead) & CPH DNS Abuse Group co-Chairs: ● Alan Woods (RySG) ● Brian Cimbolic (RySG) ● Reg Levy (RrSG)
3	ACIDTool.com (5 mins)	Reg Levy, RrSG DNS Abuse Group co-Chair
4	Wrap Up & Questions (25 mins)	Brian Cimbolic (RySG DNS Group co-chair)

02

RA/RAA DNS Abuse Amendments

Owen Smigelski (CPH Amendment Negotiation Lead)
CPH DNS Abuse Group co-Chairs: Reg Levy (RrSG) Alan Woods & Brian Cimbolic (RySG)

What are the Amendments?

- ★ Targeted & specific updates to the 2013 Registrar Accreditation Agreement and Registry Agreement
- ★ **Meaningful baseline obligations** for Contracted Parties to take **reasonable and appropriate action** to **disrupt and/or mitigate DNS Abuse** and that allow ICANN Compliance to enforce these obligations
- ★ Remaining within boundaries of ICANN policy and processes

What is DNS Abuse?

- Malware is malicious software, installed and/or executed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.
- Botnets are collections of Internet-connected computers that have been infected with malware and can be commanded to perform activities under the control of a remote attacker.
- Phishing occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g., account numbers, login IDs, passwords), whether through sending fraudulent or look-alike emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install malware.

What is DNS Abuse?

- Pharming is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking can occur when attackers use malware to redirect victims to the perpetrator's site instead of the one initially requested. DNS poisoning causes a DNS server (or resolver) to respond with a false Internet Protocol address bearing malware. Phishing differs from pharming in that pharming involves modifying DNS entries, while phishing tricks users into entering personal information.

- Spam is unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message is sent as part of a larger collection of messages, all having substantively identical content. Spam is only considered to be DNS Abuse when it is being used as a delivery mechanism for the other types of DNS abuse.

What will the RAA say?

01

Definition

Malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse)

02

Request methods

Updated methods to receive requests: webforms and emails are both permitted

03

Required action

Required action following report submission: confirm receipt; mitigate, stop or otherwise disrupt the DNS Abuse

BLUE = NEW

3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse.

3.18.1 Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of DNS Abuse and Illegal Activity. Registrar shall publish an email address or webform to receive such reports on, or conspicuously and readily accessible from, the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). Upon receipt of such reports, Registrar shall provide the reporter with confirmation that it has received the report. Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse. For the purposes of this Agreement, "DNS Abuse" means malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse listed in this Section) as those terms are defined in Section 2.1 of SAC115 (<https://www.icann.org/en/system/files/files/sac-115-en.pdf>).

3.18.2 When Registrar has actionable evidence that a Registered Name sponsored by Registrar is being used for DNS Abuse, Registrar must promptly take the appropriate mitigation action(s) that are reasonably necessary to stop, or otherwise disrupt, the Registered Name from being used for DNS Abuse. Action(s) may vary depending on the circumstances, taking into account the cause and severity of the harm from the DNS Abuse and the possibility of associated collateral damage.

Registry Amendment Highlights

New Specification 6 Section 4.2 / Slight amendment to Spec 11(3)(b)

Addition of a positive obligation to take ‘an’ action where :

- Reasonable determination of DNS Abuse can be made
- Actionable Evidence is available to support that determination
- The action to be taken, contributes to stopping or otherwise disrupting a domain from being used for DNS Abuse.
- Includes the definition of DNS Abuse for the purpose of clarity/enforceability in the contracts.
- Provides reasonable clarity for the appropriateness of actions
    a. Must take into account the severity of the harm, the circumstances of the case, and potential for collateral Damage

DNS Abuse Advisory

- ICANN Org, in consultation with the CPH Negotiation Team, drafted "**Advisory: Compliance With DNS Abuse Obligations in the Registrar Accreditation Agreement and the Registry Agreement**"

- Also known as "The Advisory", provides guidance on what is DNS Abuse, potential responses to DNS Abuse, and ICANN Compliance investigations. Is not binding, and as envisioned as a living document.

- Available at: https://itp.cdn.icann.org/en/files/registry-agreement/draft-icann-advisory-dns-abuse-amendments-25-05-2023-en.pdf

Why vote yes?

- Demonstrate registrars and registries can take meaningful steps to reduce DNS Abuse globally
- Every registrar and registry will need to address DNS Abuse
- Reduce likelihood of external action to address DNS Abuse
- Improve DNS Abuse report quality
  - Allow for webforms which standardize submissions
  - Require actionable evidence
- Registrars and registries determine the outcome of the vote. Failure to approve these changes will likely result in:
  - Delays in addressing DNS Abuse
  - Less predictable contracts/policy changes

All about voting

Not voting is counted as a vote for “no”. Have your opinion heard by voting on the Amendments!

- ★ **Who votes?** The **Primary Contact** for each registrar and registry will be able to vote on this Amendment. If that Primary Contact represents a registrar family, they vote once and it is applied to all associated registrars in that family.
- ★ **When do I vote?** Voting opened on **9 October** and will close on **8 December 2023** (60 days).
- ★ **How do I vote?** The voting process is run by “eBallot”. The Primary Contact email for each registrar and registry should have received the voting link from noreply@eballot.com, they must follow the link to go to the webpage and vote.
- ★ **What are my choices?** The options are **yes** (approve the Amendments) or no (do not approve). If you do not vote, that is counted as a “no” vote.

Current Voting Statistics

As of 21 October 2023:

RO Fee Approval Threshold (66.67%) = 49.6%

RO Majority Threshold (51%) = 47.24

Rr Threshold (90%) = 61.08

Voting results are periodically published on the 2024 Global Amendment webpage. The results on that page are as of 16 October 2023

https://www.icann.org/resources/pages/global-amendment-2024-en

Need help with voting?

If you need help with:

- ★ Finding your voting notification email or link
- ★ Updating your registrar’s Primary Contact
- ★ Anything else relating to your ability to vote

You can contact:

- ★ GlobalSupport@ICANN.org
- ★ Your ICANN Account Manager

Timeline for RA/RAA DNS Abuse Amendment

Negotiations Triggered

Letter sent from CPH to ICANN in December 2022

01

Public Comment Process on Proposed Amendment

RA/RAA amendments were put out to ICANN Community for public comment May - July 2023. Following the ICANN Report and review by the Negotiation team, no changes were deemed necessary

02

RA/RAA Proposed Amendment Agreed by CPH & ICANN

Amendment redlines were developed by the Negotiation team and agreed by the full RrSG & RySG

03

Registrar & Registry Vote on Proposed Amendment

Voting by regisries and registrars on the RA & RAA amendment commenced on 9 October and will close 8 December. RAA voting threshold of 90% needs to be met for the amendment to pass

04

ICANN Board Vote on Proposed Amendment

Board will have final review and vote on the amendments before they become effective

05

What does it all mean?

- ★ Actionable evidence
- ★ Reasonable action / mitigation
- ★ Compromised website or third level domain
- ★ Webforms / responses
- ★ Raising the floor

Helpful resources at the RrSG website:

- ★ Webform Tips: https://rrsg.org/wp-content/uploads/2023/10/Webform-Tips.pdf
- ★ Understanding RDDS responses: https://rrsg.org/wp-content/uploads/2023/10/Understanding-RDDS-Responses.pdf

03

Abuse Contact Identifier acidtool.com

Reg Levy, RrSG Abuse Group co-chair

What Data Abuse Contact IDentifier (acidtool.com) Provides?

- Hosting provider contact
- Email Service provider contact
- Creation date of domain
- Registrant data*
- Reseller name (if applicable)
- Registrar contact details

*Unless the registrant has opted out of privacy and made their information public

NEW! ACID TOOL EXPLAINERS!

For Users and Registrars

Available at
https://rrsg.org/rrsg-cph-guidance-and-information/

Some Statistics for ACID Tool

Unique Visits

June: 2,967
July: 4,107
August: 4,492
September: 4,100
October: 3,090

Number of Visits

June: 7,502
July: 9,976
August: 8,880
September: 7,828
October: 5,255

04

Wrap Up & Open Questions

Thanks!

Do you have any questions?