

CPH DNS Abuse Community Outreach

CPH DNS Abuse Community Outreach Agenda

No.	ΤΟΡΙΟ	LEAD
1	Welcome and Introduction (5 mins)	Brian Cimbolic, PIR & Reg Levy, Tucows
2	ICANN DNS Abuse Report (10 mins)	Samaneh Tajalizadehkhoob, ICANN
3	Malicious vs Compromised Domains Update (5 mins)	Graeme Bunton, DNSAI
4	RrSG's <u>www.abusetool.org</u> (5 mins)	Reg Levy, Tucows
5	Spec 11 (3)(b) Reporting Update (5 mins)	Alan Woods, Donuts
6	NetBeacon: DNSAI's centralized abuse reporting tool (5 mins)	Graeme Bunton, DNSAI
7	'Outreach' questions on DNS Abuse for the community (30 mins)	Keith Drazek, Verisign

Questions to Consider

- What initiatives are the SG/ACs engaging in outside of CPH (hosting providers/email providers/CDNs)? Is there scope for the CPH to help in such discussions?
- Are there any areas of concern that an SG/AC continues to hold? What joint efforts can the CPH and the SG/AC engage in to investigate and address it?
- Looking at existing CPH efforts (botnets, malware at scale, etc.): is there any additional clarity needed or can next steps be identified?

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 <u>RrSG website</u> and the <u>RySG website</u>.



ICANN | RrSG

Registrar Stakeholder Group

ICANN DNS Abuse Report

• Overview of the report on published by ICANN Org on 22 March 2022:

The Last Four Years in Retrospect: A Brief Review of DNS Abuse Trends

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

Malicious vs Compromised Domains Update

- Continuing the work started at the Plenary at ICANN73
- Working on a paper that discusses the distinction, and elaborates options for mitigating each type
- Invited individuals from the security community to participate
- Less best practice, more discussion
- Aiming for publication at ICANN75



Domain name		
rrsg.org		

Online Abuse Tool

HOSTING PROVIDER DETAILS:

You should contact them in case of phishing, malware, botnet and more generally content issue.

Role: Blacknight RIPE AdministratorAbuse-mailbox: abuse@blacknight.ie Abuse-mailbox: abuse@blacknight.ie Address:: Unit 12a, Barrowside Business Park Sleaty Road Carlow Town Ireland

EMAIL SERVICE PROVIDER:

You should contact them in case of spamming or any email related issue.

Role:Blacknight RIPE AdministratorAbuse-mailbox:abuse@blacknight.ie Abuse-mailbox:abuse@blacknight.ie Address:Unit 12a, Barrowside Business Park Sleaty Road Carlow Town Ireland

REGISTRAR AND REGISTRANT DETAILS:

You should contact them for any other abuse-related issue.

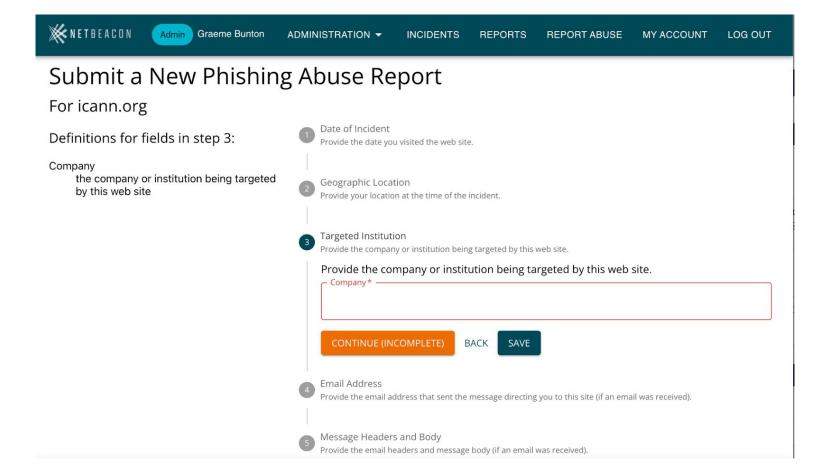
Spec 11 (3)(b) Reporting Update

- Wholly voluntary endeavor to promote transparency in Spec 11(3)(b) reporting
- We have define a simple document based on the obligations providing a simple notification of identified security threats to ICANN.
- We have shared the draft with ICANN for any further refinements and tweaks.

COMPLETION: Aim to have the process completed and perhaps even implemented by ICANN 75

NetBeacon: DNSAI's centralized abuse reporting tool

- Free service to report malware, botnets, phishing, and spam to gTLD registrars and registries
- Reduces barriers to report abuse, improves the quality of abuse reports received
 - Standardization, Enrichment, Automatic delivery
- Live and delivering actionable abuse reports as of last week
- ToDo: ccTLDs, hosting, other harms, reporter reputation, escalation paths
- Supported by PIR and CleanDNS



Our questions for the community

- What initiatives are the SG/ACs engaging in outside of CPH (hosting providers/email providers/CDNs)? Is there scope for the CPH to help in such discussions?
- Are there any areas of concern that an SG/AC continues to hold? What joint efforts can the CPH and the SG/AC engage in to investigate and address it?
- Looking at existing CPH efforts (botnets, malware at scale, etc.): is there any additional clarity needed or can next steps be identified?