ICANN 74
POLICY FORUM
THE HAGUE

# CPH DNS Abuse Community Outreach

# CPH DNS Abuse Community Outreach Agenda

| No. | TOPIC | 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 | Spec 11 (3)(b) Reporting Update (5 mins) | Alan Woods, Donuts |
| 5 | RrSG's www.abusetool.org (5 mins) | Reg Levy, Tucows |
| 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 RrSG website and the RySG website.

RySG
gTLD Registries Stakeholder Group

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-review-dns-abuse-trends-22mar22-en.pdf

# Malicious vs Compromised Domains Update

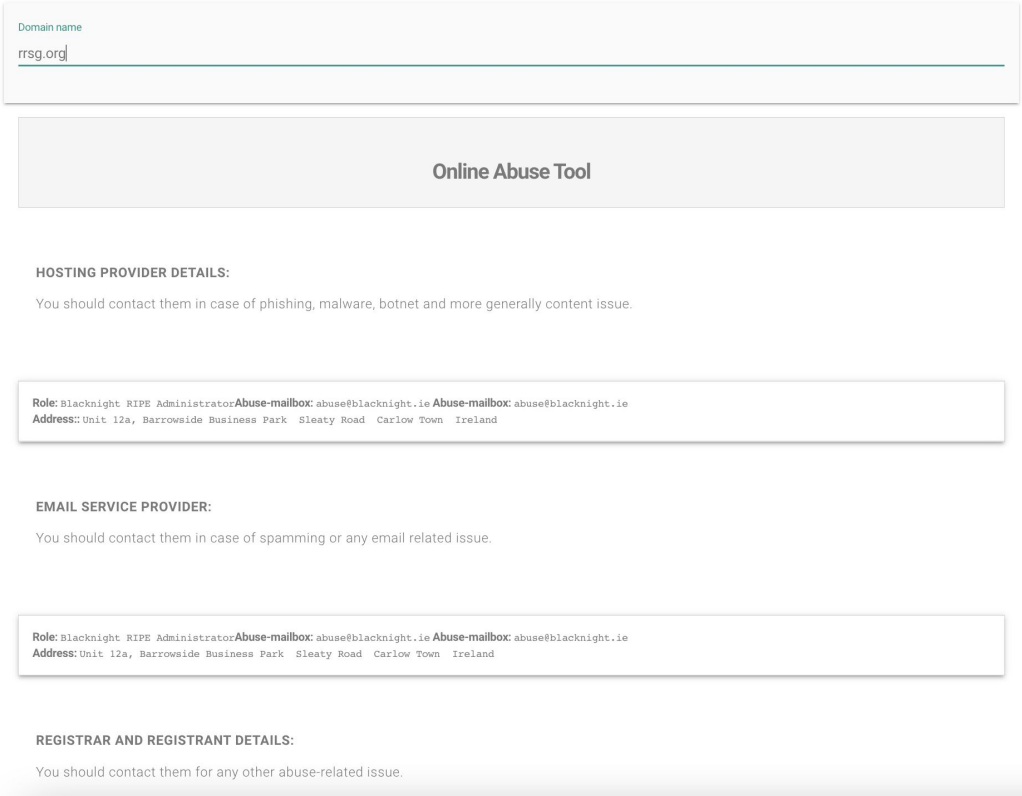
- Continuing the work started at the Plenary at ICANN73
- Working on a paper that discusses the distinction, and elaborates options for mitigating each type
- Invited individuals from the security community to participate
- Less best practice, more discussion
- Aiming for publication at ICANN75

# 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.

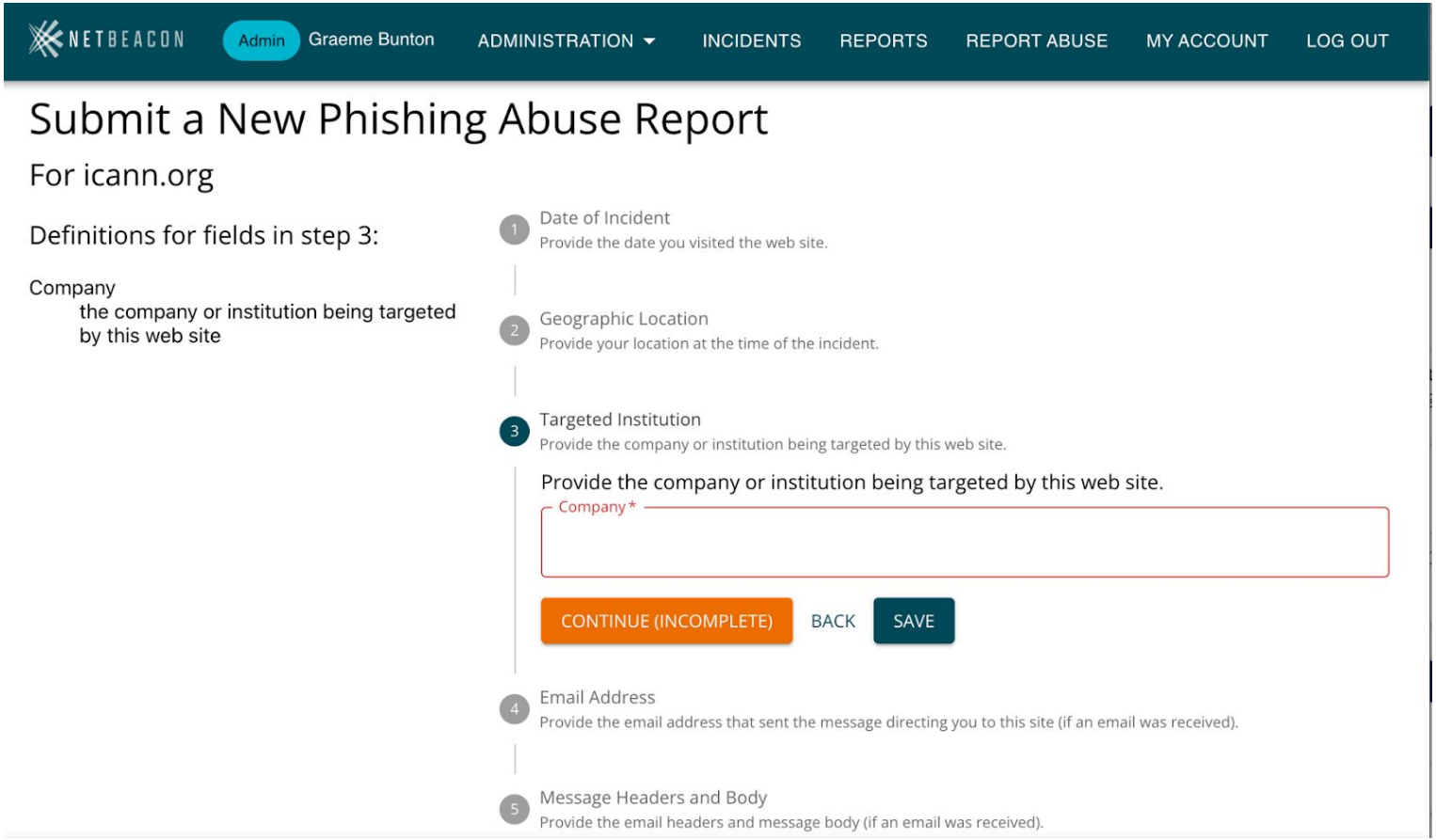
COMPLETION: Aim to have the process completed and perhaps even implemented by ICANN 75

# RrSG's abusetool.org



# 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


NETBEACON
Admin
Graeme Bunton
ADMINISTRATION
INCIDENTS
REPORTS
REPORT ABUSE
MY ACCOUNT
LOG OUT
Submit a New Phishing Abuse Report
For icann.org
Definitions for fields in step 3:
Company
the company or institution being targeted by this web site
1
Date of Incident
Provide the date you visited the web site.
2
Geographic Location
Provide your location at the time of the incident.
3
Targeted Institution
Provide the company or institution being targeted by this web site.
Provide the company or institution being targeted by this web site.
Company *
CONTINUE (INCOMPLETE)
BACK
SAVE
4
Email Address
Provide the email address that sent the message directing you to this site (if an email was received).
5
Message Headers and Body
Provide the email headers and message body (if an email was received).

# 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?