ICANN 75
ANNUAL GENERAL
KUALA LUMPUR

CPH DNS Abuse Community Outreach

CPH DNS Abuse Community Outreach Agenda

No.	TOPIC	LEAD
1	Overview & Welcome (5 mins)	Brian Cimbolic, PIR & Reg Levy, Tucows
2	Malicious vs Compromised Domains (5 mins)	Graeme Bunton, DNSAI
3	Spec 11 3(b) (5 mins)	Alan Woods, Identity Digital
4	DNSAI Project on measuring DNS Abuse (10 mins)	Rowena Schoo, DNSAI
5	RrSG's Abuse Contact IDentifier (ACID) Tool (5 mins)	Reg Levy, Tucows
4	Q&A (45 mins)	

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

Malicious vs Compromised Domains Update

- ICANN73 Plenary highlighted need for more work
- CPH DNS Abuse Working Group, plus invited members of SSAC, ccNSO DASC
- Discussion Paper
  - Less what operational, not a best practice
  - Why is the distinction important?
  - What are the potential actions and considerations for malicious domains?
  - What are the potential actions and considerations for compromised websites?
  - What goes into a balance of harms test?
- Aiming for Early Nov.

Spec 11 (3)(b) Voluntary Reporting Update

- Voluntary process to provide statistics relating to ‘identified’ security threats under our Spec 11 (3)(b) obligations.
- Purpose is to identify a uniform and scalable means to allow voluntary sharing of statistics relating to evidenced and escalated instances of DNS Abuse
- Document is in a draft form and ICANN input being invited to ensure alignment

Aim is to complete the document shortly and seek broad participation in the pilot

DNS Abuse Institute: Project for Measuring DNS Abuse

DNSAI Intelligence is a collaboration with KOR Labs, led by Maciej Korczynski from Grenoble INP-UGA - an independent academic

Measures **phishing** and **malware**

- **Phishing** is an attempt to trick people into sharing important personal information— banking information, logins, passwords, credit card numbers.

- **Malware** is malicious software designed to compromise a device on which it is installed.

Methodology is **transparent** - published and reproducible

DNS Abuse Institute: Project for Measuring DNS Abuse

Intended to measures **prevalence** and **persistence,** and if **mitigation** has occurred, how long has it taken?

In creating these reports, we have optimized for **accuracy** and **reliability**.

We hope future iterations of this report create an opportunity to **celebrate** and recognize good practice, as well as shine a spotlight on potential for areas of improvement in the industry.

We have also included a process to determine if the domain name has been **compromised** or is **maliciously** registered.

Future iterations of the report will be more granular, we're starting high level with aggregate data. Thank you to our Advisory Council, early reviewers, and the wider academic community.

We're here all week, contact us to chat: rowena@dnsabuseinstitute.org

ICANN | RrSG
Registrar Stakeholder Group

Abuse Contact IDentifier (ACID) Tool

acidtool.com

The Registrar Stakeholder Group (RrSG) offers this tool free of charge to anyone trying to identify the appropriate party (e.g. hosting provider) to report abuse to.

This tool, which relies on public data provided by third parties, is provided for informational purposes only; the RrSG makes no warranty regarding the accuracy of such data. The data retrieved and displayed does not imply any obligation, duty, or liability on the part of the Registrar Stakeholder Group, including with regard to any use that may be made of such data.

Domain name

ICANN | RrSG
Registrar Stakeholder Group

Abuse Contact IDentifier (ACID) Tool

acidtool.com

HOSTING PROVIDER:

You should contact them about phishing, malware, botnet and general content issues.

EMAIL SERVICE PROVIDER:

You should contact them about spam or any email related issue.

REGISTRAR AND REGISTRANT DETAILS:

You should contact them about any other abuse-related issue, including specific content issues.

ICANN | RrSG
Registrar Stakeholder Group

Abuse Contact IDentifier (ACID) Tool

acidtool.com

(formerly abusetool.org)

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?