ICANN | RrSG
Registrar Stakeholder Group

RySG
gTLD Registries
Stakeholder Group

CPH DNS Abuse Group
GNSO Council Briefing

CPH DNS Abuse Group Briefing Agenda

No.	Topic	Lead
1	Introduction	James Galvin, Donuts
2	RySG DNS Abuse Group Work	Brian Cimbolic, PIR
3	RrSG DNS Abuse Group Work	Reg Levy, Tucows
4	CPH DNS Abuse Group Outreach	Reg Levy, Tucows
5	Comments on SAC115 - RySG DNS Abuse Working Group	James Galvin, Donuts
6	Q&A	

Introduction

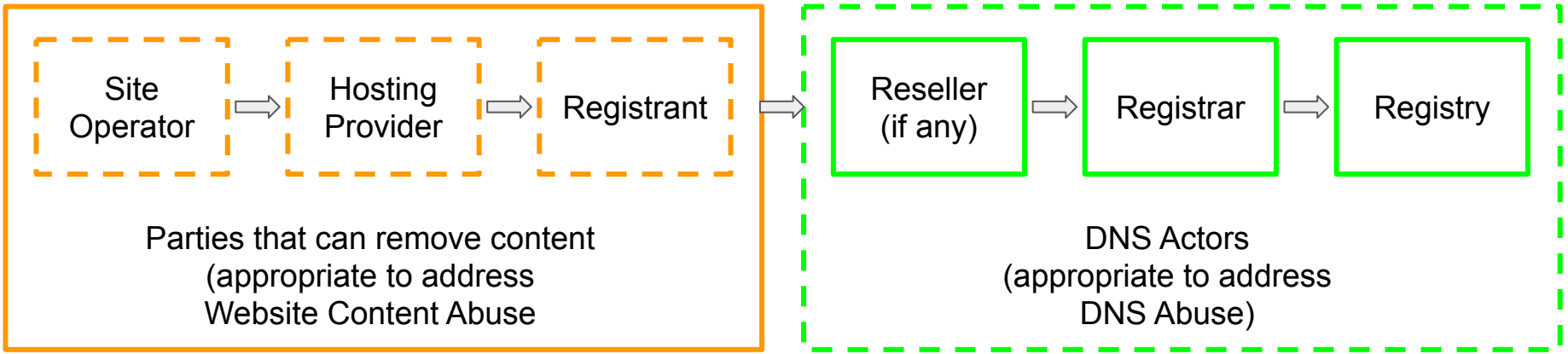
- CPH is proactively combating abuse
- DAAR statistics
  - Last year downward trend
  - This year a bit of upward movement
- This is normal - we do not control the existence of abuse
- Framework for DNS Abuse
  - DNS Abuse Definition endorsed by RySG and RrSG

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 Ecosystem



RySG Abuse Work

TOPIC	REFERENCE / STATUS
Collaboration with OCTO regarding DAAR	RYSG DAAR Working Group Report Additional work pending - TTL on DAAR listed domains
Outreach	Looking for opportunities to work together, starting with understanding their concerns: • NCSG, ALAC, BC - first meeting completed • IPC - scheduled • SSAC and ccNSO - scheduling in progress
Outputs: Registry Operator Available Actions	Explains the technical options available to registries to mitigate DNS Abuse: completed.
Future Outputs	Framework on Trusted Notifiers Evidentiary Guidelines for Reporting Abuse
Collaboration with PSWG	Continuation of previous work • Framework for Registry Operators to Respond to Security Threats • New Framework to Address Malware and Botnets at Scale

RrSG Abuse Work

TOPIC	REFERENCE / STATUS
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
Incentivisation Programs	White paper in progress
Registrant Protections	White paper in progress
Approaches to business email compromise (BEC) scams	White paper in progress
Central resource for registrants dealing with DNS Abuse	In consideration

CPH DNS Abuse Group Outreach

Outreach Summary

- Individual meetings with other constituency (NCSG, ALAC, BC to date)
- Q&A (information used, concerns and helpful practices)

Outreach Output

- Guide to registry abuse reporting (similar to existing registrar guide)
- Trusted Notifiers Framework
- At-Large education materials
- Evidentiary guidance for reporting abuse - registries will add guidance to registrar work

Future Work in Consideration

- Community questionnaire on helpful outputs/guidance
- DNS Abuse ‘newsletter’
- DNS Abuse ‘trifold’ information pamphlet

Comments on SAC115
RySG DNS Abuse Working Group

- Note that two RySG members contributed to the SSAC Work Party that produced this document, along with a PSWG member
- We took note of the following points about the document
  - Took note of varying definitions of abuse but did bias its discussion around the definition in the DNS Abuse Framework and our contracts
  - Much of the discussion is from the point of the victim, which is also the case in much of the discussion in the ICANN community
  - Identified need for greater interoperability between all parties - including some that are not an ordinary part of the ICANN community
- Actions we are considering
  - Evidentiary guidelines for abuse reporting
  - Trusted notifier framework

ICANN | RrSG
Registrar Stakeholder Group

RySG
gTLD Registries
Stakeholder Group

Any Questions?