Registry Policy for Abuse Mitigation

ICANN75

ccNSO

Techday

Jeff Bedser, CleanDNS Inc.

Policy	Awareness	Effort	Measure
• What types of abuse will you address? What types need to be referred, refused and impact of harm	• How do you find out about abuse?	• How do you track and respond to reports	• How do you measure the abuse volume by registrant

Policy

What types of abuse will you address?

- Clear, concise information of what is permissible

What will constitute a valid set of evidence?

- For each type of abuse, what will be acceptable as evidence of the abuse
- Infrastructure relevance, screen shots, demonstration of abuse being conducted. Intent?

What actions will you take?

- Suspension, notification, action against registrant/registrar

Tracking, Managing, Reporting

- What will you retain in this process and for what period of time

Additional Policy Points

A Registry Operator ensure that our mitigating action is not causing more harm that the abuse alleged reported

Timing, we should only intervene immediately when the imprecision of our action (the serverhold) is justifiable, given the either the proven lack of collateral damage (clearly malicious) or the demonstrable need to disrupt a great harm is also temporal in nature and immediate action is necessary.

Consider policy balance for the above points when considering policy and actions regarding malicious registration vs compromised domains

Awareness
Receive or buy or find

Getting the reports of abuse related to your zones

Several Methods of Ingest for Reports

- Abuse @ Email account
  - Pro: Very inexpensive
  - Con: free text. Variable evidence profile, reports may not match policy, duplicate reports
- Abuse Ingest Form (Net Beacon et al)
  - Pro: forced evidence upload to policy, Clear reports
  - Con: Costs associated with maintenance or outsource
  - API
- Blocklists $
  - Pro: Significantly more volume of data
  - Con: can be expensive and most are lacking adequate evidence
- Reporters (gratis)
  - Pro: No or minimal cost
  - Con: Not very comprehensive, duplicative reporting
- Hybrid – do a combination of all of the above ← best practice

Effort

Have someone review each report

- Does it meet policy of types of abuse?
- Does it meet the evidence thresholds?
- Relay it to the appropriate party for action

Follow Through

- Has the report been actioned appropriately
- Have the necessary parties been notified

Tracking

- Take the necessary steps to ensure the process of report through notification has been recorded to policy

Measure

Points of measurement

Reports (on reports)

- Number/volume of reports received by source
- Number of reports actioned under policy
- Number of reports of domains suspended
- Number of reports of domains referred to other parties
- Number of false reports
- Number of under–evidenced reports
- All of this measured monthly/weekly/quarterly

Measure -2

Entities

- Measure by registrar
- Measure (if possible) by registrant

Campaign/Marketing/Sales

- Abuse volume within various incentive programs

Discussions

Jeff Bedser

CleanDNS Inc