About the ccNSO DNS Abuse Standing Committee (DASC)

1. Share information, insights and practices
2. Raise understanding and awareness
3. Promote open and constructive dialogue
4. Assist ccTLD managers in their efforts to mitigate the impact of DNS Abuse

DASC does not formulate any policy or standards: out of scope of the ccNSO policy remit
About the DASC survey

• Open: September ‘22 – end November ‘22
• All ccTLDs were invited to respond, regardless of ccNSO membership
• 57 unique responses. Estimate: representing approx. 100 ccTLDs
  • 316 delegated ccTLDs in total (ASCII & 61 IDN alike)
  • Some ccTLD managers provide services for multiple ccTLDs, but responded for 1 TLD only
  • Some ccTLD managers informed DASC they could not respond, for various reasons
  • Some ccTLDs responded multiple times: latest submission as final one
  • Some responses were incomplete
• About half of the respondents did not want their ccTLD mentioned
DEMOGRAPHICS
DEMOGRAPHICS
One size does not fit all: the ccTLD landscape is diverse

Select the ICANN geographical region for your ccTLD

- North America: 3
- Africa: 8
- Latin America/Caribbean islands: 13
- Asia/Australia/Pacific: 13
- Europe: 20

What is the governance model of your ccTLD?

- Not for profit organisation: 25
- For profit company: 12
- Governmental institution: 11
- Academic institution: 7
- Company Limited by Guarantee: 1
- Member-driven Statutory Organisation: 1
- Other (please specify): 6

Which registration model do you follow?

- Other (please specify): 3
- direct registrations: 6
- a combination of 3R and direct registrations: 16
- 3R: Registry-Registrar-Registrant: 32
DEMOGRAPHICS

One size does not fit all: the ccTLD landscape is diverse

What is the number of registered domain names by your ccTLD?

- more than 1 million
- 100,001 to 1 million
- 50,001 to 100,000
- 10,001 to 50,000
- 5,001 to 10,000
- 0 to 5000

A significant number of respondents have > 1 million domains. On average, respondents have over 10k domains.

Big diversity in terms of ccTLD staffing.

How many employees (Full Time Equivalents) work within the registry/registry department?

- more than 50
- 31 to 50
- 11 to 30
- 6 to 10
- 2 to 5
- 1

My ccTLD has an DNS Abuse Officer as part of the registry.

- Not sure
- Yes
- No

Over 75% of the respondents indicated they do not have a dedicated DNS Abuse Officer.
Most respondents indicated that less than 0.05% of their domain names under management are subject to DNS Abuse. 35% was not sure.

Over 80% of the respondents collaborate with either national Computer Security Incident Response Teams, Law Enforcement Agencies or Trusted Notifiers.

Close to 60% of the respondents stated they are affected by Data Protection legislation.

Most respondents indicated that less than 0.05% of their domain names under management are subject to DNS Abuse. 35% was not sure.
ACTIONABLE TYPES OF DNS ABUSE
**TYPES OF DNS ABUSE**

Where do the respondents take action?

Most respondents consider Malware, Phishing, Botnets and Pharming to be actionable, and Spam to a lesser extent.

Most respondents will take action on Child Sexual Abuse Materials.

Most respondents will take action on homograph infringements. Some respondents indicated they never take action on the listed types of abuse.
DNS ABUSE MITIGATION: TRENDS
DNS ABUSE MITIGATION: TRENDS

What do the numbers say?

Respondents indicated a high reliance on a Registration policies and Complaints procedures.

<table>
<thead>
<tr>
<th>Method</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>4</td>
<td>36%</td>
</tr>
<tr>
<td>Complaints procedures</td>
<td>36</td>
<td>36%</td>
</tr>
<tr>
<td>Consumer awareness</td>
<td>26</td>
<td>26%</td>
</tr>
<tr>
<td>Tools</td>
<td>28</td>
<td>28%</td>
</tr>
<tr>
<td>Procedures</td>
<td>29</td>
<td>29%</td>
</tr>
<tr>
<td>Registration Policies</td>
<td>36</td>
<td>36%</td>
</tr>
</tbody>
</table>

To mitigate DNS Abuse, my ccTLD uses the following methods:

My ccTLD has a collaborative relationship with:

<table>
<thead>
<tr>
<th>Relationship</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>11</td>
<td>11%</td>
</tr>
<tr>
<td>Trusted Notifiers</td>
<td>14</td>
<td>14%</td>
</tr>
<tr>
<td>Law enforcement</td>
<td>30</td>
<td>30%</td>
</tr>
<tr>
<td>CSIRTS</td>
<td>38</td>
<td>38%</td>
</tr>
</tbody>
</table>

Most respondents stated they have a collaborative relationship with national Computer Security Incident Response Teams and Law enforcement.

My ccTLD does outreach/education to registrars/registrants, related to DNS Abuse:

<table>
<thead>
<tr>
<th>Response</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blank</td>
<td>7</td>
<td>7%</td>
</tr>
<tr>
<td>Not Sure</td>
<td>7</td>
<td>7%</td>
</tr>
<tr>
<td>No</td>
<td>27</td>
<td>27%</td>
</tr>
<tr>
<td>Yes</td>
<td>22</td>
<td>22%</td>
</tr>
</tbody>
</table>

Most respondents do not have any outreach or educational activities regarding DNS Abuse.
TRENDS ON DNS ABUSE MITIGATION

What do the numbers say?

The majority of the respondents have not entered into a Trusted Notifier arrangement.

If my ccTLD detects abuse, post-registration, we take this action:

- We do not have the capability to detect abuse
- Our approach depends on the results of our risk assessment
- We give notice of suspension
- We immediately delete the domain name
- We immediately suspend the domain name

When an abuse issue is detected once the domain name is already registered, the type of action for most respondents depends on the results of their internal risk assessment.

Most respondents indicated the availability of reporting mechanisms regarding DNS abuse for members of the public.
TOOLS & FEEDS
Commercial, Open Source, or Both?
# Common tools used by ccTLDs

<table>
<thead>
<tr>
<th>Open Source</th>
<th>Commercial</th>
</tr>
</thead>
<tbody>
<tr>
<td>DGArchive</td>
<td>SURBL</td>
</tr>
<tr>
<td>Shadowserver</td>
<td>Spamhaus</td>
</tr>
<tr>
<td>OpenPhish (Community)</td>
<td>Anti-Phishing Working Group (APWG)</td>
</tr>
<tr>
<td>PhishTank</td>
<td>Netcraft</td>
</tr>
<tr>
<td></td>
<td>Sophos</td>
</tr>
<tr>
<td></td>
<td>Recorded Future</td>
</tr>
<tr>
<td></td>
<td>Malware Bytes</td>
</tr>
<tr>
<td></td>
<td>Malware Patrol</td>
</tr>
<tr>
<td></td>
<td>IQ Global (aggregation of feeds)</td>
</tr>
</tbody>
</table>
OTHER FINDINGS
Combining demographics and trends
Mitigation by demographics: region

- Count of Reg Policies
- Count of Tools
- Count of Consumer awareness
- Count of Complaints procedures
- Count of Collab With CSIRTS
- Count of Collab With Law enforcement

Regions:
- Africa
- Asia/Australia/Pacific
- Europe
- Latin America/Caribbean islands
- North America
More to come!

Stay tuned
DASC survey subgroup

- Angela Matlapeng (.bw)
- Bruce Tonkin (.au) | Chair DASC survey subgroup
- Tatiana Tropina (NomCom appointed ccNSO Council member)
- Nick Wenban Smith (.uk) | Chair DASC
- Brett Carr (former member)

https://ccnso.icann.org/en/workinggroups/dasc.htm
THANK YOU