ccNSO DNS Abuse Standing Committee

DASC survey webinar, 28 September 2023

ICANN | ccNSO
Country Code Names Supporting Organization
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
Timeline

September-November 2022:
- survey open

March ‘23 at ICANN76:
- DASC shares survey results, part 1

June ‘23 at ICANN77:
- DASC shares survey results, part 2

September ’23, prior to ICANN78:
- DASC shares final survey results
What makes ccTLDs different?

- Region
- Governance model
- Registry model
- % domains exposed to DNS Abuse
- Number of domains
- Number of employees
- ccTLD has Abuse Officer
- ccTLD is affected by DPL

ICANN | ccNSO
What was shared previously?

**ICANN76**

- Where and when do respondents take action?
- What are the DNS Abuse mitigation trends?
  - Mitigation methods, outreach & education to registrars
  - Trusted notifier arrangements, type of action when abuse is detected, reporting mechanisms for the public
- Tools & feeds
- Combined results: mitigation methods vs region, registry model, size

**ICANN77**

- Pre-registration
  - Which information is being collected?
  - Do respondents perform pre-registration verifications?
  - Do respondents perform checks at time of registration, and if so, for which data?
- Post-registration
  - Methods: manual vs automated
  - When do post-registration verifications happen?
- Mid-cycle
  - Type of action when abuse is detected, based on: Feed, LEA request, due diligence verifications
  - Measures to keep registration data accurate over time
- Renewal
  - Do respondents perform verifications?
What stood out?

Comparison: survey responses vs DNSAI data

- Many respondents unsure about level of Abuse in their TLD. Hence, comparison with DNS Abuse Institute (DNSAI) data.
- DNSAI Compass data refers to phishing and malware only.
- Vast majority: less than 0.05% of abusive domains, less than 20 names reported as DNS Abuse.
- DNS Abuse rate of 0.05% means: only noticeable number (e.g. >100) for ccTLDs with large domain portfolio. This may explain why respondents were unsure about levels of abuse in their ccTLDs.
What stood out?

Pricing variation across ccTLDs

- Largest ccTLDs in terms of volume of names generally in the low price range
- No discernible correlation of price with the level of DNS Abuse
- Data based on registrar and ccTLD registry pricing, where publicly available (44 ccTLDs)

Legend
At retail level

- High: > 100 USD
- Medium: 21-99 USD
- Low: 6-20 USD
- Very Low: < 5 USD
Today: comparisons

- ccTLDs affected by
  - Malware and Unwanted Software
  - Child Sexual Abuse Materials (CSAM)
  - Homograph attacks
  - Abuse (percentage of ccTLD domain name registrations)

- ccTLDs performing pre-registration verifications

- ccTLDs having mitigation techniques

- region
- governance model
- registry model
- domain portfolio
- number of employees
- presence of an abuse officer
- subject to Data Protection Legislation
- cooperation (e.g. with Computer Security Incident Response Team)
- domains affected by abuse
ccTLDs affected by Malware and Unwanted Software
ccTLDs affected by Malware and Unwanted Software

<table>
<thead>
<tr>
<th>Region</th>
<th>Governance model</th>
<th>Registry model</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF</td>
<td>academic</td>
<td>3R</td>
</tr>
<tr>
<td>AP</td>
<td>limited</td>
<td>direct</td>
</tr>
<tr>
<td>EU</td>
<td>for profit</td>
<td>3R &amp; direct</td>
</tr>
<tr>
<td>LAC</td>
<td>governmental</td>
<td></td>
</tr>
<tr>
<td>NA</td>
<td>statutory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>non-profit</td>
<td></td>
</tr>
</tbody>
</table>
ccTLDs affected by Malware and Unwanted Software

<table>
<thead>
<tr>
<th>Domain portfolio</th>
<th>Employees</th>
<th>Abuse officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 5000</td>
<td>0 to 5000</td>
<td>0</td>
</tr>
<tr>
<td>50,001 to 100,000</td>
<td>50,001 to 100,000</td>
<td>50,001 to 100,000</td>
</tr>
<tr>
<td>10,001 to 50,000</td>
<td>10,001 to 50,000</td>
<td>10,001 to 50,000</td>
</tr>
<tr>
<td>5,001 to 10,000</td>
<td>5,001 to 10,000</td>
<td>5,001 to 10,000</td>
</tr>
<tr>
<td>100,001 to 1 million</td>
<td>100,001 to 1 million</td>
<td>100,001 to 1 million</td>
</tr>
<tr>
<td>&gt; 1 million</td>
<td>&gt; 1 million</td>
<td>&gt; 1 million</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain portfolio</th>
<th>Employees</th>
<th>Abuse officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 5000</td>
<td>0 to 5000</td>
<td>0</td>
</tr>
<tr>
<td>50,001 to 100,000</td>
<td>50,001 to 100,000</td>
<td>50,001 to 100,000</td>
</tr>
<tr>
<td>10,001 to 50,000</td>
<td>10,001 to 50,000</td>
<td>10,001 to 50,000</td>
</tr>
<tr>
<td>5,001 to 10,000</td>
<td>5,001 to 10,000</td>
<td>5,001 to 10,000</td>
</tr>
<tr>
<td>100,001 to 1 million</td>
<td>100,001 to 1 million</td>
<td>100,001 to 1 million</td>
</tr>
<tr>
<td>&gt; 1 million</td>
<td>&gt; 1 million</td>
<td>&gt; 1 million</td>
</tr>
</tbody>
</table>

ICANN | ccNSO
ccTLDs affected by Malware and Unwanted Software

Subject to Data Protection Legislation

Cooperation (e.g. Computer Security Incident Response Team)

Domains affected by abuse
ccTLDs affected by Child Sexual Abuse Material (CSAM)
## ccTLDs affected by Child Sexual Abuse Material (CSAM)

<table>
<thead>
<tr>
<th>Region</th>
<th>Governance model</th>
<th>Registry model</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF</td>
<td>non-profit</td>
<td>3R</td>
</tr>
<tr>
<td>AP</td>
<td>statutory</td>
<td>direct</td>
</tr>
<tr>
<td>EU</td>
<td>governmental</td>
<td>3R &amp; direct</td>
</tr>
<tr>
<td>LAC</td>
<td>for profit</td>
<td></td>
</tr>
<tr>
<td>NA</td>
<td>limited</td>
<td></td>
</tr>
<tr>
<td></td>
<td>academic</td>
<td></td>
</tr>
</tbody>
</table>

![Bar chart showing the distribution of ccTLDs affected by CSAM across regions, governance models, and registry models.](chart.png)
ccTLDs affected by Child Sexual Abuse Material (CSAM)

<table>
<thead>
<tr>
<th>Domain portfolio</th>
<th>Employees</th>
<th>Abuse officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; 1 million</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>100,001 to 1 million</td>
<td>2</td>
<td>No</td>
</tr>
<tr>
<td>5,001 to 10,000</td>
<td>4</td>
<td>Not sure</td>
</tr>
<tr>
<td>10,001 to 50,000</td>
<td>6</td>
<td>Yes</td>
</tr>
<tr>
<td>50,001 to 100,000</td>
<td>5</td>
<td>No</td>
</tr>
<tr>
<td>0 to 5,000</td>
<td>3</td>
<td>Not sure</td>
</tr>
</tbody>
</table>

ICANN | ccNSO
ccTLDs affected by Child Sexual Abuse Material (CSAM)

- Subject to Data Protection Legislation
- Cooperation (e.g. Computer Security Incident Response Team)
- Domains affected by abuse
ccTLDs affected by Homograph Attacks
What is a homograph attack?

Homograph (also known as homoglyph) phishing attacks are based on the idea of using similar characters to pretend to be another site. While most of them are easily recognizable by end-users with proper training, the homograph attacks based on international domain names (IDN) can be unrecognizable from the domains they are spoofing.

Example:
- g00gle.com
- replacing the Latin "a" with the Cyrillic "а" (U+0430) creates a visually identical but distinct character
ccTLDs affected by Homograph Attacks

<table>
<thead>
<tr>
<th>Region</th>
<th>Governance model</th>
<th>Registry model</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF</td>
<td>academic</td>
<td>3R</td>
</tr>
<tr>
<td>AP</td>
<td>limited</td>
<td>direct</td>
</tr>
<tr>
<td>EU</td>
<td>for profit</td>
<td>3R &amp; direct</td>
</tr>
<tr>
<td>LAC</td>
<td>governmental</td>
<td></td>
</tr>
<tr>
<td>NA</td>
<td>statutory</td>
<td></td>
</tr>
</tbody>
</table>
ccTLDs affected by Homograph Attacks

<table>
<thead>
<tr>
<th>Domain portfolio</th>
<th>Employees</th>
<th>Abuse officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 5000</td>
<td>0 to 5000</td>
<td>0 to 5000</td>
</tr>
<tr>
<td>50,001 to 100,000</td>
<td>1 to 5</td>
<td>1 to 5</td>
</tr>
<tr>
<td>10,001 to 50,000</td>
<td>2 to 10</td>
<td>2 to 10</td>
</tr>
<tr>
<td>5,001 to 10,000</td>
<td>3 to 11</td>
<td>3 to 11</td>
</tr>
<tr>
<td>100,001 to 1 million</td>
<td>4 to 30</td>
<td>4 to 30</td>
</tr>
<tr>
<td>&gt; 1 million</td>
<td>&gt; 30</td>
<td>&gt; 30</td>
</tr>
</tbody>
</table>
ccTLDs affected by Homograph Attacks

<table>
<thead>
<tr>
<th>Subject to Data Protection Legislation</th>
<th>Cooperation (e.g. Computer Security Incident Response Team)</th>
<th>Domains affected by abuse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>&lt; 0.05%</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>0.05-0.1%</td>
</tr>
<tr>
<td>Not sure</td>
<td>No</td>
<td>0.1-0.15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.15-0.20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt; 0.20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>not sure</td>
</tr>
</tbody>
</table>
Comparing the percentage of ccTLD registrations exposed to abuse
% of domains exposed to DNS abuse

<table>
<thead>
<tr>
<th>Region</th>
<th>Governance model</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td>academic</td>
</tr>
<tr>
<td>LAC</td>
<td>limited</td>
</tr>
<tr>
<td>EU</td>
<td>for profit</td>
</tr>
<tr>
<td>AP</td>
<td>governmental</td>
</tr>
<tr>
<td>AF</td>
<td>statutory</td>
</tr>
<tr>
<td></td>
<td>non-profit</td>
</tr>
</tbody>
</table>

![Bar chart showing the percentage of domains exposed to DNS abuse by region and governance model.](chart.png)
% of domains exposed to DNS abuse

### Domain portfolio

- **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**

### Registry model

- **3R & direct**
- **direct**
- **3R**

---

**ICANN | ccNSO**
% of domains exposed to DNS abuse

<table>
<thead>
<tr>
<th>Employees</th>
<th>Abuse officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;50</td>
<td>yes</td>
</tr>
<tr>
<td>31-50</td>
<td>no</td>
</tr>
<tr>
<td>11-30</td>
<td>not sure</td>
</tr>
<tr>
<td>6-10</td>
<td>yes</td>
</tr>
<tr>
<td>2-5</td>
<td>yes</td>
</tr>
<tr>
<td>1</td>
<td>yes</td>
</tr>
</tbody>
</table>

- < 0.05%
- 0.05-0.1%
- 0.15-0.20
- > 0.20
- not sure
% of domains exposed to DNS abuse

Subject to Data Protection Legislation (DPL)

Cooperation (e.g. Computer Incident Response Team)
My ccTLD performs pre-registration verifications
My ccTLD performs pre-registration verifications
Pre-registration verifications: how?
My ccTLD performs pre-registration verifications

### Domain portfolio

- > 1 million: 25
- 100,001 to 1 million: 15
- 5,001 to 10,000: 10
- 10,001 to 50,000: 5
- 50,001 to 100,000: 1
- 0 to 5000: 0

### Employees

- 1: 2
- 2-5: 4
- 6-10: 6
- 11-30: 8
- 31-50: 10
- >50: 14

---

**ICANN | ccNSO**

---

31
My ccTLD performs pre-registration verifications

Domains affected by abuse

- not sure
- more than 0.20%
- less than 0.05%
- between 0.15 and 0.20%
- between 0.1 and 0.15%
- between 0.05% and 0.1%

Subject to Data Protection Legislation

- Yes
- Not sure
- No

ICANN|ccNSO
My ccTLD has abuse mitigation techniques in place
ccTLDs with mitigation techniques

Region

Domains affected by abuse

- more than 0.20%
- less than 0.05%
- between 0.15 and 0.20%
- between 0.1 and 0.15%
- between 0.05% and 0.1%
- not sure
ccTLDs with mitigation techniques

Domain portfolio

Employees

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

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

reg. policies
consumer awareness
collab with CSIRTS
collab with LEA
Collab with trusted notifiers
Procedures
Main Findings

● Overall, relatively low levels of abuse for ccTLDs
  ○ Many ccTLDs do take action, despite respondents saying they have limited resources, and do not have access to tools
  ○ Different types of ccTLDs do perform checks, regardless of their region, governance model, registration model, domain portfolio size, number of staff.

● Checks could happen prior to registration, but are more often done shortly after registration, or when abuse is being detected
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)

Info about DASC and its two subgroups:
https://ccnso.icann.org/en/workinggroups/dasc.htm
Learn more about different perspectives on tools and measurements of DNS Abuse. DASC reminds the ccTLD community about its repository and invites ccTLDs globally to contribute. Finally, DASC is proud to launch a dedicated email list at ICANN78, as a useful resource for ccTLDs.

Session chair: Nick Wenban-Smith (.uk)
1. Welcome & introductions
2. DASC resources for ccTLDs: repository and e-mail list
3. Tools & Measurements: different perspectives
4. Dialogue between GNSO and ccNSO DNS Abuse Working Groups on similarities and differences
5. Wrap-up & Closure
Thank you!

ccnsosecretariat@icann.org