TLD-OPS Update
DR/BCP Workshop Update
ccNSO Meeting

October 24, 2018
ICANN63, Barcelona

Jacques Latour, .ca (Chair)
Régis Massé, .fr (Vice Chair)
TLD-OPS introduction

• Global technical incident response community *for and by* ccTLDs, open to *all* ccTLDs (ASCII and IDN)

• Brings together 380+ people who are responsible for the operational security and stability of 201 different ccTLDs

• Goal: enable ccTLD operators to collaboratively detect and mitigate incidents that may affect the operational security and stability of ccTLD services and of the wider Internet

• Further *extends* members’ existing incident response structures, processes, and tools and *does not* replace them

• Guidance by TLD-OPS Standing Committee
  – ccTLD reps and Liaisons (SSAC, IANA, ICANN’s security team)
Contact Repository Email

"John Doe, #1, .nl, +31 123456789"  john.doe@nic.nl, john@oarc.net
"Jane Doe, #1, .vn, +84 123456789"  jane.doe@nic.vn, jane@oarc.net
## Security Alerts and Workshops

<table>
<thead>
<tr>
<th>Description (example)</th>
<th>Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert: Malware use DNS to steal personal info</td>
<td>Feb-18</td>
</tr>
<tr>
<td>Two DDoS attacks on a registry’s name servers</td>
<td>Mar-17</td>
</tr>
<tr>
<td>Registry front-end compromise due to 0-day vulnerability</td>
<td>Mar-17</td>
</tr>
<tr>
<td>Queries on latency problems with DNS anycast operator</td>
<td>Dec-16</td>
</tr>
<tr>
<td>Security warning regarding large volumes of Cutwail Traffic</td>
<td>Nov-16</td>
</tr>
<tr>
<td>Alert: several members reporting large DNS traffic spikes</td>
<td>Nov-16</td>
</tr>
<tr>
<td>Security warning for a ccTLD that was hacked</td>
<td>Aug-16</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>

- **Disaster Recovery Workshop @ ICANN63**
  - Leave with more questions than answers
  - Share information, experience, real or hypothetical
  - Collecting the collective experience / Share best practices

TLD-OPS Standing Committee
It’s time to join the TLD-OPS community

- **Easy**: Just send an email to join
- **Secure**: Identified and trusted contacts
- **Helpful**: Community help in case of an incident
TLD-OPS Operations Since ICANN62

• Security alerts
  – One notification

• Membership updates – Objective met 😊
  – Added 6 new ccTLD to the list
    • .pe Peru
    • .gu Guam
    • .mx Mexico
    • .sv San Salvadore/El Salvador
    • .mr Mauritania
    • .ci Cote d'Ivoire
  – 5 TLD-OPS contact changes/updates

• Active standing committee outreach to missing members
  – Remote participation to the APTLD 74 Meeting (Tashkent, Uzbekistan)
OVER 200 MEMBERS

TLD-OPS Standing Committee
TLD-OPS all over the world

ASCII 172 (+6 / 70%) & IDN: 29 (63%)

5 (100%)

65 (100%)

51 (+1 / 62%)

27 (+2 / 53%)

24 (+3 / 57%)

Total: 201 (+6 / 69%)
Objectives for ICANN63

- Host a DR/BCP workshop
- Increase membership by 3 to 198 (ICANN62/63)
  - We added 6 new members, now at 201

Objectives for ICANN64

- First DR/BCP draft playbook delivery
- Increase membership by 3 to 204
We are here
Disaster Recovery Workshop Updates

- **Workshop:** ~ 52 registered attendees

- **Agenda:**
  13:30 - 13:45 - Introductions - ‘be prepared’
  
  13:45 - 14:15 - Disaster Recovery / Business Continuity
  
  14:15 - 15:15 - Workshop breakout #1 - Scope: Registry & DNS
  45 min: Group 1: Detection, Analysis / Group 2: Activation, Action Plan/Communications
  15 min: Summary / present outcome:
  Group 1: Brett, Regis, Fred
  Group 2: Abibu, Jacques, Erwin
  
  15:30 - 16:30 - Workshop breakout #2 - Scope: Corporate IT & People
  45 min: Group 2: Detection, Analysis / Group 1: Activation, Action Plan/Communications
  15 min: Summary / present outcome:
  
  16:30 - 17:00 – Conclusion & Summary / Summarise final outcome / Develop message to ccNSO
  
  TLD-OPS Standing Committee
Workshop Flip Charts
Initial Workshop Summary

• At the beginning half of ccTLD present felt they were prepared to handle a disaster

• At the end of the session only a few raised their hands confidently

• There’s a need to develop a playbook with the basic concepts of DR/BCP (Disaster Recovery and Business Continuity) and Business Impact Assessment (BIA) processes

• There’s a need to develop ccTLD specific action plan procedures specific to the registry and DNS operations

• We need to compile all the notes and start development of the playbook
We Have Volunteers 😊
Raise your hand if the workshop was worth your time
TLD-OPS Standing Committee

Jacques Latour, .ca / Chair

Régis Massé, .fr / Vice Chair

Frederico Neves, .br / Member
Erwin Lansing, .dk / Member
Ali Hadji Mmadi, .km / Member
Abibu Ntahigiye, .tz / Member
Brett Carr, .uk / Member

Warren Kumari, SSAC Liaison
John Crain, SSR Liaison
Kim Davis, IANA Liaison
Kimberly Carlson, ICANN Staff
Ressources & Contacts

http://ccnso.icann.org/resources/tld-ops-secure-communication.htm

Jacques Latour
Standing Committee Chair
+1.613.291.1619
jacques.latour@cira.ca

Régis Massé
Standing Committee Vice Chair
+1.6.83.12.43.49
regis.masse@afnic.fr

TLD-OPS Standing Committee
Thank you!