TLD-OPS Update
ccNSO Meeting

June 25, 2019
ICANN65, Marrakech

Jacques Latour, .ca (Chair)
Régis Massé, .fr (Vice Chair)
Ahhh!! Not another boring TLD-OPS update!

- What can I do:
  A. Run away
  B. Sleep
  C. Daydream
  D. Play solitaire

  
  E. Read emails
TLD-OPS introduction

Raise your hand if you don’t know what TLD-OPS is!

• 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 200+ different ccTLDs

• 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

• **All TLD-OPS Playbook will be publicly available** on TLD-OPS website

• **Guidance** by TLD-OPS Standing Committee
  – ccTLD reps and Liaisons (SSAC, IANA, ICANN’s security team)
“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
Disaster Recovery Workshop Update

ICANN 62 - TechDay Presentation
ICANN 62 - ccNSO Presentation
ICANN 63 Workshop
ICANN 64 DT Review
ICANN65 First Draft

We are here

TLD-OPS Standing Committee
DR/BCP - Drafting Team Status Report

• Dirk Jumpertz, .EU, unanimously approved as DR/BCP Drafting Team fearless leader :-)  

• TLD-OPS SC and DT meeting this Thursday to review first draft

• Agreed on Playbook Goals
  – How to bring DR, BCP, BIA discipline to a small ccTLD
  – Focus only on ccTLD relevant activities
  – Simple templates for top 5 major DR/BCP scenarios
  – Template usable as is for a table top exercise

• The TLD-OPS Standing Committee assessment is we’re making really good progress 😊
Next Steps: Thinking of having a DR/BCP Table Top / Simulation Workshop @ ICANN66 Montreal

• Simulate a registry compromise

• Test the DR/BCP Playbook against the scenario

• Update the DR/BCP Playbook against the gaps, observations and lessons learned

• **Closed to TLD-OPS Members only?**
Security Alerts and Workshops

<table>
<thead>
<tr>
<th>Description (a few example)</th>
<th>Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious Activity Targeting the DNS</td>
<td>Feb-19</td>
</tr>
<tr>
<td>Vulnerability in DNS software</td>
<td>Oct-18</td>
</tr>
<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>
</tbody>
</table>

- Disaster Recovery / BCP Workshop @ ICANN63 Barcelona
- DDoS Mitigation Workshop @ICANN58 Copenhagen
TLD-OPS Operations Since ICANN64

• Security alerts
  – none

• Membership updates
  – ccTLD Added: none
  – Contact updates: 5 updates
Objectives for ICANN65 / ICANN66

• **Objectives for ICANN65**
  
  – Ensure coherence between web site and contact repository

  – First Draft of DR/BCP Playbook

• **Objectives for ICANN66**

  – TLD-OPS Workshop: DR/BCP Tabletop simulation exercise (Registry compromise)
TLD-OPS Standing Committee

TLD-OPS all over the world

ASCII 173 (71%) & IDN: 29 (63%)

5 (100%)

65 (100%)

27 (53%)

25 (60%)

51 (62%)

Total: 202 (69%)
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 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!