TLD-OPS
ccTLD Security and Stability Together

September 2019
LACTLD Technical Workshop

Alejandra Reynoso
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 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)
Together, we are stronger

- Open and global incident response community for and by ccTLDs
- Builds on standard mailing list
- Further extends members’ existing incident response structures, processes, and tools and does not replace them.
- Increases everyone’s reachability and security awareness
  - Everyone has everyone else’s contact info in their inbox, even offline
  - Exchange security alerts and queries (DDoS attacks, phishing, etc.)
  - Learn from each other
- Easy to join (through IANA Admin Contact)
Contact Repository Email

Dear Security and Stability Contact,

This is a notification of updates to the TLD-OPS mailing list.

This email includes the full list of TLD-OPS subscribers (see below), with their names, email addresses, phone numbers, and their ccTLD. We highly recommend storing this email on one of your devices so that you may also contact your peer security and stability contacts in offline situations.

Note that all of the new members have been authenticated by their ccTLD’s IANA Admin Contact, as per the subscription procedure for the TLD-OPS list. More details about the admission procedure are available at http://ccso.icann.org/resources/tld-ops-secure-communication.htm.

Best regards,
TLD-OPS Standing Committee

*** FULL LIST OF TLD-OPS MEMBERS ***

“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
Together, we create value for the community

New tools for the community

Mailing List

Workshops

Feedbacks
TLD-OPS all over the world

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

5 (100%)

65 (100%)

27 (53%)

51 (62%)

Total: 202 (69%)
# TLD-OPS Membership Stats

<table>
<thead>
<tr>
<th>All</th>
<th>Members</th>
<th>%</th>
<th>Missing</th>
<th>%</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>202</td>
<td>69%</td>
<td>89</td>
<td>31%</td>
<td>291</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ASCII</th>
<th>Members</th>
<th>%</th>
<th>Missing</th>
<th>%</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>173</td>
<td>71%</td>
<td>72</td>
<td>29%</td>
<td>245</td>
</tr>
<tr>
<td>AF</td>
<td>27</td>
<td>53%</td>
<td>24</td>
<td>47%</td>
<td>51</td>
</tr>
<tr>
<td>AP</td>
<td>51</td>
<td>62%</td>
<td>31</td>
<td>38%</td>
<td>82</td>
</tr>
<tr>
<td>EU</td>
<td>65</td>
<td>100%</td>
<td>0</td>
<td>0%</td>
<td>65</td>
</tr>
<tr>
<td>LAC</td>
<td>25</td>
<td>60%</td>
<td>17</td>
<td>40%</td>
<td>42</td>
</tr>
<tr>
<td>NA</td>
<td>5</td>
<td>100%</td>
<td>0</td>
<td>0%</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IDN</th>
<th>Members</th>
<th>%</th>
<th>Missing</th>
<th>%</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>29</td>
<td>63%</td>
<td>17</td>
<td>37%</td>
<td>46</td>
</tr>
</tbody>
</table>

**Missing LACTLD ccTLDs:**
- .ai Anguilla
- .bs Bahamas
- .bz Belize
- .cu Cuba
- .ec Ecuador
- .gf French Guiana
- .gs S. Georgia & the S. Sandwich Islands
- .gy Guyana
- .ht Haiti
- .jm Jamaica
- .kn Saint Kitts and Nevis
- .ky Cayman Islands
- .mq Martinique
- .ms Montserrat
- .sr Suriname
- .tc Turks and Caicos Islands
- .vc Saint Vincent and the Grenadines
It’s time to join the TLD-OPS community

- Easy: Just send an email to join
- Identified and trusted contacts
- Secure
- Helpful: Community help in case of an incident
A first delivery: the DDOS Mitigation Playbook

- The goal of the first workshop was to explore how TLD-OPS members can collaborate to detect and mitigate DDOS attack.
- Two sessions took place during ICANN Meetings 58 and 60 to share experiences, discussions and generation of ideas.
- The topic has approached from multiple perspectives, such as technical, operational, compliance and strategic.
Work in progress
Natural Disasters – DR/BCP Readiness

• Expand to general Disaster Recovery and Business Continuity Planning
  – Request from community following natural disasters
  – BCP is many things to many people
  – Where to start?
  – Where to focus?
  – Past Experience?

• Technical continuity plans for the DNS, Registry and corporate systems

• The Business part focuses on plans, initiation, testing, critical even, communications, simulation
Focus for the TLD-OPS community

- DNS resolution infrastructure
- Registry system (SRS, RDDS, Data Escrow …)
- IT infrastructure: network, storage, servers, softwares
- Emergency communication tools
Next Steps: 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
Ressources & Contacts

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 – LACTLD Technical Workshop

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