TLD-OPS Standing Committee Meeting
ccTLD Security and Stability Together

October 31, 2017
ICANN60, Abu Dhabi

Jacques Latour, .ca (Chair)
Agenda TLD-OPS Meeting @ ICANN60, Oct 29, 2017

1. Opening and welcome (Jacques)
2. TLD-OPS introduction (Jacques)
3. Action points (All)
4. TLD-OPS status and operational issues (Kim C., everyone)
5. TLD-OPS DDoS mitigation Workshop readiness (Jacques)
6. Objectives ICANN60 / ICANN61 (All)
7. Summary for TLD-OPS members and ccNSO community (All)
8. AOB (All)
9. Closing (Jacques)

Open discussion: TLD-OPS DDoS mitigation Workshop readiness
TLD-OPS Introduction
ccTLD Security and Stability Together

October 31, 2017
ICANN60, Abu Dhabi

Jacques Latour, .ca (Chair)
TLD-OPS

• Global technical incident response community for and by ccTLDs, open to all ccTLDs

• Brings together 345+ people who are responsible for the operational security and stability of 192 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

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://censo.icann.org/resources/tld-ops-secure-communication.htm](http://censo.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](mailto:john.doe@nic.nl), [john@oarc.net](mailto:john@oarc.net)

“Jane Doe, #1, .vn, +84 123456789” [jane.doe@nic.vn](mailto:jane.doe@nic.vn), [jane@oarc.net](mailto:jane@oarc.net)

Stats: 328 subscribers from 186 ccTLDs
# Security Alerts and Queries

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Two DDoS attacks on a registry’s name servers</td>
<td>Mar-17</td>
</tr>
<tr>
<td>10</td>
<td>Registry front-end compromise due to 0-day vulnerability</td>
<td>Mar-17</td>
</tr>
<tr>
<td>9</td>
<td>Queries on latency problems with DNS anycast operator</td>
<td>Dec-16</td>
</tr>
<tr>
<td>8</td>
<td>Security warning regarding large volumes of Cutwail Traffic</td>
<td>Nov-16</td>
</tr>
<tr>
<td>7</td>
<td>Alert: several members reporting large DNS traffic spikes</td>
<td>Nov-16</td>
</tr>
<tr>
<td>6</td>
<td>Security warning for a ccTLD that was hacked</td>
<td>Aug-16</td>
</tr>
<tr>
<td>5</td>
<td>Helped ccTLD with problems with their DNS anycast service</td>
<td>Jul-16</td>
</tr>
<tr>
<td>4</td>
<td>Security warning on DDoS attack on DNS root</td>
<td>Jun-16</td>
</tr>
<tr>
<td>3</td>
<td>Alert: spear-phishing attacks against ccTLD operators</td>
<td>Apr-16</td>
</tr>
<tr>
<td>2</td>
<td>Large malvertising campaign targeting popular ccTLD websites</td>
<td>Apr-16</td>
</tr>
<tr>
<td>1</td>
<td>A ransomware that used domain names of various ccTLDs</td>
<td>Feb-16</td>
</tr>
</tbody>
</table>
## TLD-OPS Membership Stats

<table>
<thead>
<tr>
<th></th>
<th>Members</th>
<th>%</th>
<th>Missing</th>
<th>%</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All</strong></td>
<td><strong>192</strong></td>
<td>66%</td>
<td><strong>99</strong></td>
<td>34%</td>
<td><strong>291</strong></td>
</tr>
<tr>
<td><strong>ASCII</strong></td>
<td><strong>163</strong></td>
<td>67%</td>
<td><strong>82</strong></td>
<td>33%</td>
<td><strong>245</strong></td>
</tr>
<tr>
<td>AF</td>
<td>25</td>
<td>49%</td>
<td>26</td>
<td>51%</td>
<td>51</td>
</tr>
<tr>
<td>AP</td>
<td>50</td>
<td>61%</td>
<td>32</td>
<td>39%</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>18</td>
<td>43%</td>
<td>24</td>
<td>57%</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>
<tr>
<td><strong>IDN</strong></td>
<td><strong>29</strong></td>
<td>63%</td>
<td><strong>17</strong></td>
<td>37%</td>
<td><strong>46</strong></td>
</tr>
</tbody>
</table>

Last update: October 24, 2017
Summary

• Open and global incident response community for and by ccTLDs
• Builds on standard mailing list (192 ccTLDs, 345+ subscribers)
• Enhances local incident response facilities, not a replacement
• 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)
• Difficult to measure effectiveness of contact repository
Agenda TLD-OPS Meeting @ ICANN60, Oct 29, 2017

1. Opening and welcome (Jacques)
2. TLD-OPS introduction (Jacques)
3. **Action points (All)**
4. TLD-OPS status and operational issues (Kim C., everyone)
5. TLD-OPS DDoS mitigation Workshop readiness (Jacques)
6. Objectives ICANN60 / ICANN61 (All)
7. Summary for TLD-OPS members and ccNSO community (All)
8. AOB (All)
9. Closing (Jacques)

Open discussion: TLD-OPS DDoS mitigation Workshop readiness
<table>
<thead>
<tr>
<th>No.</th>
<th>Action</th>
<th>Who</th>
<th>Deadline</th>
<th>Status</th>
<th>Date created</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>66</td>
<td>Contact Greenland once more if they're willing to join</td>
<td>Erwin</td>
<td>1-Jun-17</td>
<td>Closed</td>
<td>24-Apr-17</td>
<td>Update 2017.06.02: Erwin will try to contact them through Patrick Miles of CENTR. Deadline: next conference call. Update 2017.06.19: Erwin will drop .gl another email. Update 2017.09.07: Erwin try one more tiem and we close this item.</td>
</tr>
<tr>
<td>77</td>
<td>Review TLD-OPS Charter with evolving role</td>
<td>Brett, Erwin, Jacques</td>
<td>12-Oct-17</td>
<td>Closed</td>
<td>26-Jun-17</td>
<td>First draft was reviewed by committee and a new draft will include working around &quot;non ccNSO member&quot; committee member requirements and solicit feedback from Bart. Jacques sent charter to Katerine and Bart for review.</td>
</tr>
<tr>
<td>78</td>
<td>Provide outline of new process for &quot;contact update&quot; for secondary email address and other contact changes.</td>
<td>Kim Jacques</td>
<td>12-Oct-17</td>
<td>Open</td>
<td>01-Aug-17</td>
<td>Contact update process to use a new ICANN TLD-OPS contact change address not to burden the ccNSO secretariat email address. - we accept changes from admin or TLD-OPS contact - create a new ICANN address - update documentation with new process Update 2017.09.07: Kim to provide updated documentation Update 2017.10.24: - Please announce we are now accepting secondary emails and to email us at: <a href="mailto:TLD-OPS-Admin@icann.org">TLD-OPS-Admin@icann.org</a> - Update the TLD-OPS web site with this new step - Update the leaflet with mention of secondary email address - Send TLD-OPS email with availability of new procedure/feature - Update ccNSO update with this mention</td>
</tr>
<tr>
<td>80</td>
<td>The bi-monthly &quot;TLD-OPS Incident Response Community Repository&quot; email does not list one contact per line in outlook. We need to figure out how to have one contact per line.</td>
<td>Fred</td>
<td>9-Sep-17</td>
<td>Open</td>
<td>01-Jan-18</td>
<td>Assigned to Fred? How do we fix mailman to show one line per contact? Update 2017-10-24: Sent email to Fred to propose a resolution solution.</td>
</tr>
<tr>
<td>81</td>
<td>Send Dave Piscitello email to present at TLD-OPS at beginning of block 5</td>
<td>Erwin</td>
<td>9-Sep-17</td>
<td>Closed</td>
<td>15-Oct-17</td>
<td>Erwin to send email asking Dave to present with focus on TLD-OPS attendees.</td>
</tr>
</tbody>
</table>
Agenda TLD-OPS Meeting @ ICANN60, Oct 29, 2017

1. Opening and welcome (Jacques)
2. TLD-OPS introduction (Jacques)
3. Action points (All)
4. TLD-OPS status and operational issues (Kim C., everyone)
5. TLD-OPS DDoS mitigation Workshop readiness (Jacques)
6. Objectives ICANN60 / ICANN61 (All)
7. Summary for TLD-OPS members and ccNSO community (All)
8. AOB (All)
9. Closing (Jacques)

Open discussion: TLD-OPS DDoS mitigation Workshop readiness
TLD-OPS Operations Since ICANN59 - Kim

• Security alerts
  – None

• Membership updates
  – Joined: Namibia, Lesotho and Greenland
  – Contact updates: 6 (new, removal)
  – All of Europe and North America now covered 😊 Good work!!

• Implemented support for secondary email addresses
Agenda TLD-OPS Meeting @ ICANN60, Oct 29, 2017

1. Opening and welcome (Jacques)
2. TLD-OPS introduction (Jacques)
3. Action points (All)
4. TLD-OPS status and operational issues (Kim C., everyone)
5. **TLD-OPS DDoS mitigation Workshop readiness (All)**
6. Objectives ICANN60 / ICANN61 (All)
7. Summary for TLD-OPS members and ccNSO community (All)
8. AOB (All)
9. Closing (Jacques)
Agenda TLD-OPS Meeting @ ICANN60, Oct 29, 2017

1. Opening and welcome (Jacques)
2. TLD-OPS introduction (Jacques)
3. Action points (All)
4. TLD-OPS status and operational issues (Kim C., everyone)
5. TLD-OPS DDoS mitigation Workshop readiness (All)
6. Objectives ICANN60 / ICANN61 (All)
7. Summary for TLD-OPS members and ccNSO community (All)
8. AOB (All)
9. Closing (Jacques)
Objectives ICANN60

- Develop and present a revised TLD-OPS charter
- Develop a strategy for TLD-OPS workshops (ICANN workshop and participating in regional workshop)
- Increase membership by 3 to 190 (now at 192)
Objectives for ICANN61

• Summarize the ICANN 60 TLD-OPS workshops outcome into a ...

• Document a TLD-OPS workshops strategy for ICANN and regional workshop.

• Increase membership by 3 to 195
Agenda TLD-OPS Meeting @ ICANN60, Oct 29, 2017

1. Opening and welcome (Jacques)
2. TLD-OPS introduction (Jacques)
3. Action points (All)
4. TLD-OPS status and operational issues (Kim C., everyone)
5. TLD-OPS DDoS mitigation Workshop readiness (All)
6. Objectives ICANN60 / ICANN61 (All)
7. Summary for TLD-OPS members and ccNSO community (All)
8. AOB (All)
9. Closing (Jacques)
Q&A

TLD-OPS Standing Committee
Frederico Neves, .br
Jacques Latour, .ca (chair)
Erwin Lansing, .dk
Ali Hadji Mmadi, .km
Jay Daley, .nz
Abibu Ntahigiye, .tz
Brett Carr, .uk
Warren Kumari (SSAC contact)
John Crain (ICANN’s security team contact)
Kim Davies (IANA contact)

ICANN Staff
Kim Carlson

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

TLD-OPS Leaflet
Arabic, Chinese, English, French, Russian, Spanish, Russian

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