TLD-OPS Update
ccTLD Security and Stability Together

ccNSO Members Day
March 14, 2017
ICANN58, Copenhagen

Cristian Hesselman, .nl (TLD-OPS Standing Committee Chair)
TLD-OPS

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

• Brings together ~330 people who are responsible for the operational security and stability of 187 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)
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://ccnso.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
“Jane Doe, #1, .vn, +84 123456789”  jane.doe@nic.vn
```
## Security Alerts and Queries

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Month</th>
</tr>
</thead>
<tbody>
<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>Total</strong></td>
<td>187</td>
<td>64%</td>
<td>104</td>
<td>36%</td>
<td>291</td>
</tr>
</tbody>
</table>

### ASCII

<table>
<thead>
<tr>
<th>Region</th>
<th>Members</th>
<th>%</th>
<th>Missing</th>
<th>%</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
<td>158</td>
<td>64%</td>
<td>87</td>
<td>36%</td>
<td>245</td>
</tr>
<tr>
<td>AF</td>
<td>23</td>
<td>45%</td>
<td>28</td>
<td>55%</td>
<td>51</td>
</tr>
<tr>
<td>AP</td>
<td>49</td>
<td>60%</td>
<td>33</td>
<td>40%</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>17</td>
<td>40%</td>
<td>25</td>
<td>60%</td>
<td>42</td>
</tr>
<tr>
<td>NA</td>
<td>4</td>
<td>80%</td>
<td>1</td>
<td>20%</td>
<td>5</td>
</tr>
</tbody>
</table>

### IDN

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

Last update: February 27, 2017
Progress Since ICANN57

• Security alerts
  – Registry front-end compromise due to 0-day vulnerability (Mar)
  – Queries on latency problems with DNS anycast operators (Dec)
  – Security warning regarding large volumes of Cutwail Traffic (Nov)
  – Large traffic spikes at three ccTLDs, likely a reflection attack (Nov)

• Membership updates
  – Joined: .as (American Samoa), .ir (Islamic Republic Of Iran)
  – Contact updates: 5 (new/removal)
  – Put two ccTLDs back on the list after excess bounces
Outreach: TLD-OPS Workshop, March 12

- **Goal:** explore how TLD-OPS members can collaborate to detect and mitigate DDoS attacks

- **Motivation:**
  - Recent large-scale (IoT) attacks on the DNS (such as Dyn, root)
  - Need to mobilize the collective experience of the TLD-OPS community

- **Approach**
  - Facilitate dialog: sharing of experiences, discussion, generation of ideas
  - Considering perspectives such as technical, operational, and strategic
  - Closed workshop for member ccTLDs only

- **Targeted results**
  - Shared understanding of role of TLD-OPS in handling DDoS events
  - Guidelines and tools to integrate TLD-OPS into ccTLD operations
  - Items for further discussion
# Workshop Stats

<table>
<thead>
<tr>
<th>Attendees</th>
<th>55 (61 registrations)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII ccTLDs</td>
<td>35</td>
</tr>
<tr>
<td>IDN ccTLDs</td>
<td>11</td>
</tr>
<tr>
<td>ccTLD reps</td>
<td>52 (4 also on the SSAC, but ccTLD reps today)</td>
</tr>
<tr>
<td>Proxies</td>
<td>9</td>
</tr>
<tr>
<td>SSAC members</td>
<td>2</td>
</tr>
<tr>
<td>RSSAC members</td>
<td>1</td>
</tr>
<tr>
<td>Regions</td>
<td>AF, AP, EUR, LAC, NA</td>
</tr>
<tr>
<td>Expertise</td>
<td>operational, technical, strategic</td>
</tr>
<tr>
<td>SC members</td>
<td>6 (Fred, Jacques, Erwin, Cristian, Jay, Warren)</td>
</tr>
</tbody>
</table>

Last update: March 12, 2017
Breakout Groups and Lots of Interaction!
Workshop Results (First Selection)

- Initial feedback: increased trust among TLD-OPS members
- Excellent participation and attendance
- Workshop format worked well
- Secondary email address for every incident response contact
- Live communication facilities during an attack (chat, bridge)
- Share best practices and enable peers to learn
- Longer term: shared services (sinkhole, threat analysis, monitoring)
- Next step: look into flip charts in more detail and put into action
Was It Useful?
Outreach: TLD-OPS Postcard (January 2017)

TLD-OPS: ccTLD Security and Stability Together
security alerts • incident contact repository • global collaboration

Number of Member ccTLDs: 186 (63%)
https://ccnso.icann.org/resources/tld-ops-secure-communication

Dear ccTLD Manager,

Please accept this postcard as a kind invitation to join TLD-OPS, the incident response community for and by ccTLDs. We currently have 186 members (63% of all ccTLDs) from across the globe, but we’re still missing you!

The purpose of TLD-OPS is to enable its members to help each other to detect and mitigate incidents that may affect the security and stability of ccTLD services, such as DDoS attacks, malware infections, and phishing attacks. The aim of TLD-OPS is to further extend members’ existing incident response structures, processes, and tools and not to replace them.

TLD-OPS builds on a standard mailing list, which members actively use to share and receive security alerts and queries. The list also acts as a contact repository in that subscribers receive a monthly automated email that contains the incident response information (names, phone numbers, email addresses) of all member ccTLDs.

The contact repository improves the reachability of TLD-OPS members because everyone has everyone else’s contact information readily available in their inboxes, which typically also works in offline emergency situations.

TLD-OPS is open to every ccTLD and joining only takes a few minutes. Please check the TLD-OPS Homepage (URL on the front of this card) and download our leaflet, which is available in Arabic, Chinese, English, French, Russian, and Spanish.

We hope to welcome you on board soon!

Best regards,
TLD-OPS Standing Committee

TLD-OPS Standing Committee
Objectives ICANN58

• Increase the number of ASCII ccTLDs members by 5% to 194 through webinars for LAC and AF and possibly AP regions

• Organize a TLD-OPS workshop at ICANN58 to discuss how ccTLDs collaboratively detect and mitigate DDoS attacks
Objectives ICANN59

- Potentially organize 2\textsuperscript{nd} TLD-OPS workshop (focus on AF region)
- Put outcomes Sunday’s workshop and survey into action
- Finalize TLD-OPS membership update procedure
- Increase membership by 3 to 190
TLD-OPS Standing Committee
Frederico Neves, .br
Jacques Latour, .ca
Erwin Lansing, .dk
Ali Hadji Mmadi, .km
Cristian Hesselman, .nl (chair)
Jay Daley, .nz
Abibu Ntahigiye, .tz
Warren Kumari (SSAC liaison)
John Crain (ICANN’s security team liaison)
Kim Davies (IANA liaison)

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
Cristian Hesselman
Standing Committee Chair
+31 6 25 07 87 33
cristian.hesselman@sidn.nl
@hesselma