TLD-OPS: ccTLD Security and Stability Together

security alerts | incident contact repository | global collaboration

APTLD71
Ho Chi Minh City, Vietnam
March 2, 2017

Cristian Hesselman, .nl (chair)

Feel free to ask questions right away, no need to wait until the end of the presentation!
TLD-OPS

• Global technical incident response community for and by ccTLDs, open to all ccTLDs, not a commercial enterprise

• Brings together people who are responsible for the operational security and stability of their ccTLD

• 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
# 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>186</td>
<td>64%</td>
<td>105</td>
<td>36%</td>
<td>291</td>
</tr>
<tr>
<td><strong>ASCII</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>157</td>
<td>64%</td>
<td>88</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>48</td>
<td>59%</td>
<td>34</td>
<td>41%</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>
<tr>
<td><strong>IDN</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<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: November 6, 2016
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](http://ccso.icann.org/resources/tld-ops-secure-communication.htm).

Best regards,

TLD-OPS Standing Committee

"John Doe, #1, .nl, +31 123456789" john.doe@nic.nl
"Jane Doe, #1, .vn, +84 123456789" jane.doe@nic.vn

Stats: 328 subscribers from 186 ccTLDs
Examples of Security Alerts and Queries

- Spear-phishing attacks against ccTLD operators
- Large malvertising campaign targeting popular ccTLD websites
- A ransomware that used domain names of various ccTLDs
- Helped one ccTLD with problems with their DNS anycast service
- **Security warning for a ccTLD that got hacked**
- Security warning on DDoS attack on DNS root of June 25, 2016
- Security warning regarding large volumes of Cutwail Traffic
- Queries on latency problems with DNS anycast operators
Why Join?

• Increase reachability of your ccTLD in incident response situations
• Increase your ability to help your peers in these situations
• Increase your awareness of incidents and your security posture
• Learn from your peers how they solved incidents
• Contribute to security and stability of wider Internet infrastructure
• TLD-OPS is open to all ccTLDs
• TLD-OPS is an initiative for and by ccTLDs
• Joining only takes one email (through your IANA Admin Contact)!
TLD-OPS Workshop at ICANN58 (members only)

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

• Motivation: recent (IoT) attacks on DNS operators (e.g., Dyn, root)

• Approach
  – Facilitate dialog: sharing of experiences, discussion, generation of ideas
  – Considering perspectives such as technical, operational, and strategic

• 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

• March 12 09:00-12:00, Copenhagen (registration until March 5!)
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-communications

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
Summary

• Open and global incident response community for and by ccTLDs
• Builds on standard mailing list (186 ccTLDs, 328 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)
Q&A

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
http://ccnso.icann.org/resources/tld-ops-secure-communication.htm
Arabic, Chinese, English, French, Russian, Spanish, Russian

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