TLD-OPS Standing Committee Meeting

ccTLD Security and Stability Together

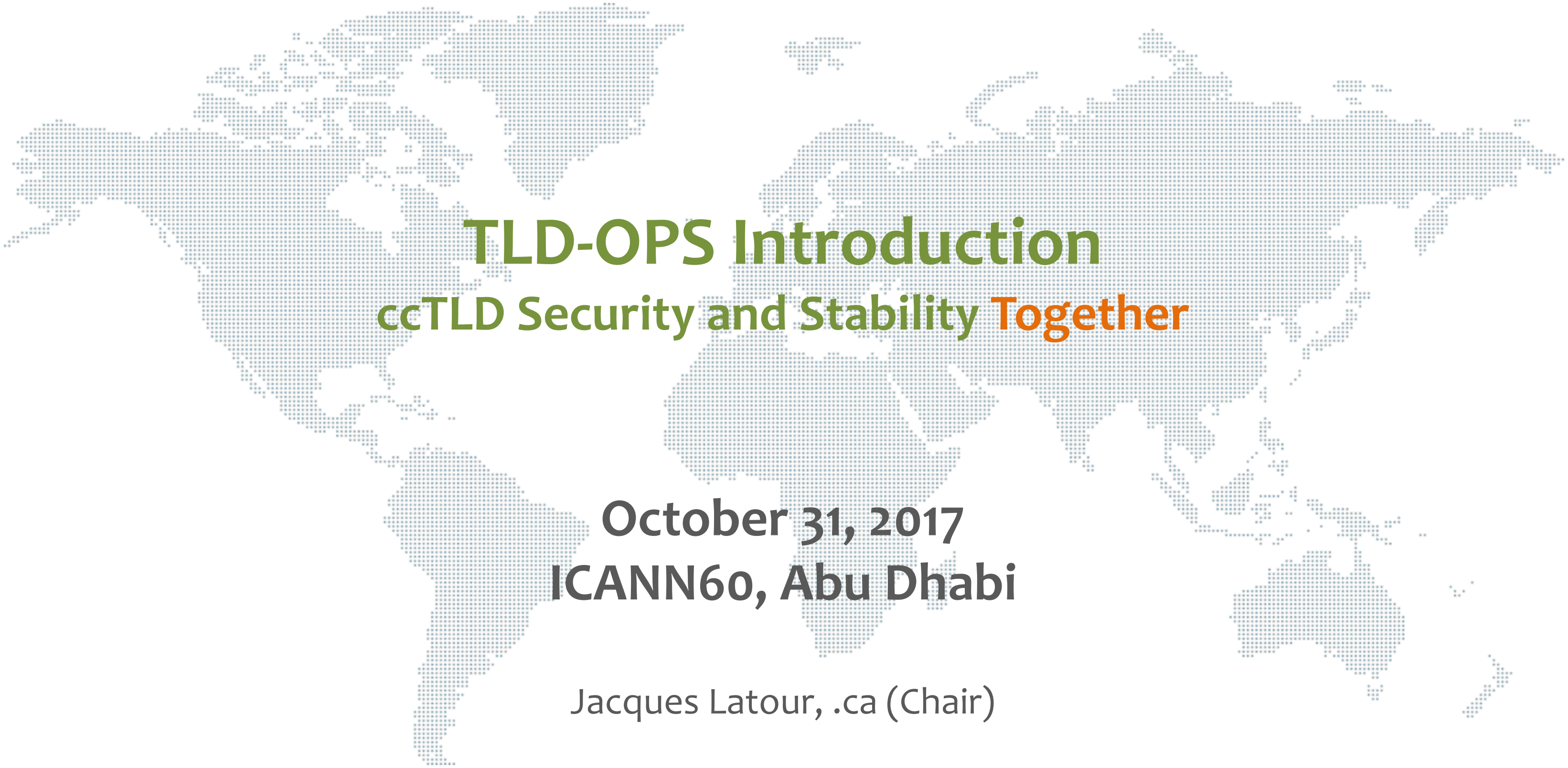
October 31, 2017
ICANN60, Abu Dhabi

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)

ccNSO ICANN

TLD-OPS

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

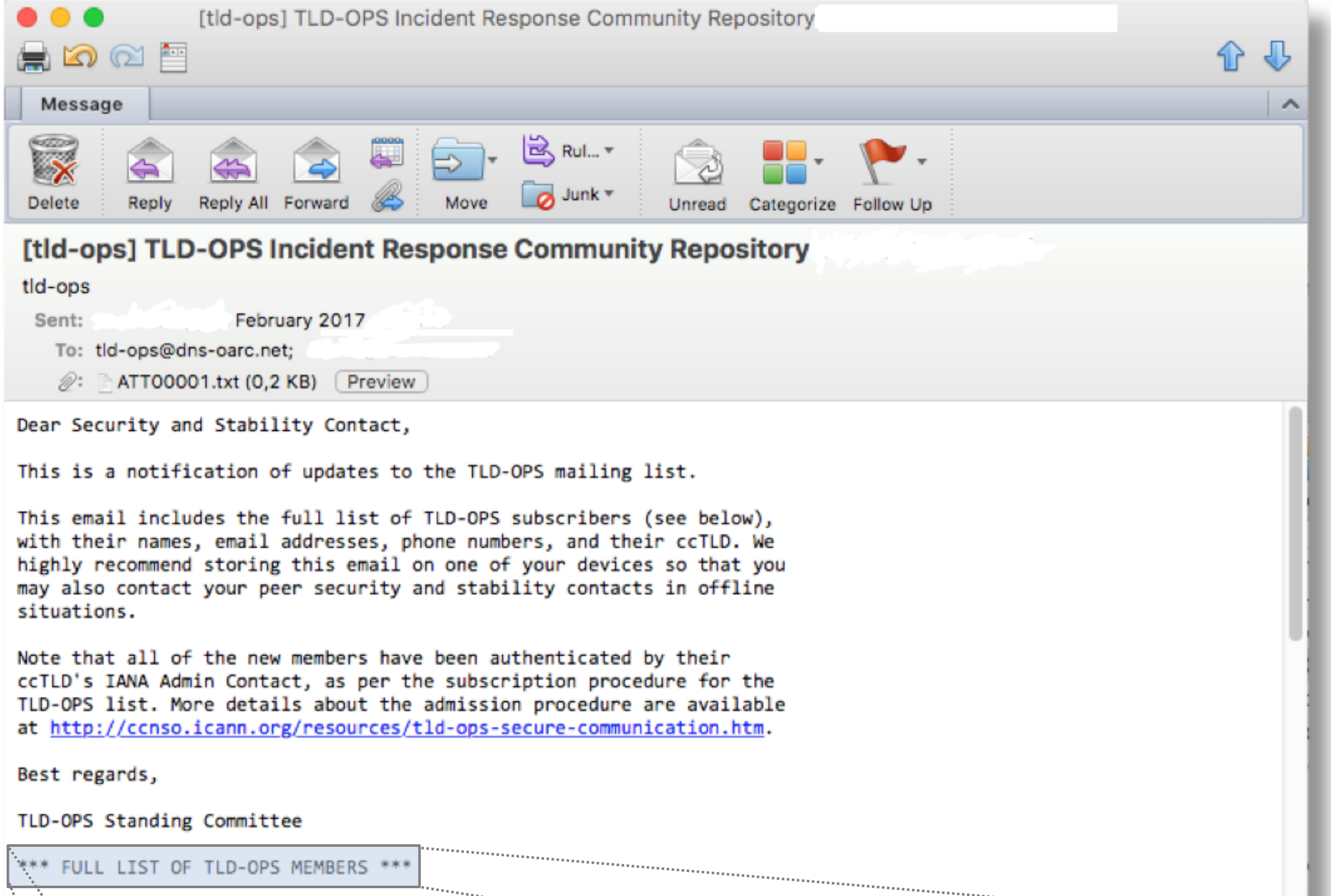
- Brings together 345+ people who are responsible for the operational security and stability of 192 different ccTLDs

- 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



[tld-ops] TLD-OPS Incident Response Community Repository [redacted]

[tld-ops] TLD-OPS Incident Response Community Repository [redacted]

tld-ops

Sent: [redacted] February 2017 [redacted]

To: tld-ops@dns-oarc.net; [redacted]

ATT00001.txt (0,2 KB)

```
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, john@oarc.net
“Jane Doe, #1, .vn, +84 123456789” jane.doe@nic.vn, jane@oarc.net
```

Stats: 328 subscribers from 186 ccTLDs

Security Alerts and Queries

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

TLD-OPS Membership Stats

All	Members	%	Missing	%	Total
Total	***192***	66%	***99***	34%	***291***

ASCII	Members	%	Missing	%	Total
Total	***163***	***67%***	***82***	***33%***	***245***
AF	25	49%	26	51%	51
AP	50	61%	32	39%	82
EU	65	100%	0	0%	65
LAC	18	43%	24	57%	42
NA	5	100%	0	0%	5

IDN	Members	%	Missing	%	Total
Total	***29***	63%	***17***	37%	***46***

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

Action Point

No.	Action	Who	Deadline	Status	Date created	Notes
66	Contact Greenland once more if they're willing to join	Erwin	1-Jun-17	Closed	24-Apr-17	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.
77	Review TLD-OPS Charter with evolving role	Brett, Erwin, Jacques	12-Oct-17	Closed	26-Jun-17	First draft was reviewed by committee and a new draft will include working around "non ccNSO member" committee member requirements and solicit feedback from Bart. Jacques sent charter to Katerine and Bart for review.
78	Provide outline of new process for "contact update" for secondary email address and other contact changes.	Kim Jacques	12-Oct-17	Open	01-Aug-17	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: TLD-OPS-Admin@icann.org - 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
80	The bi-monthly "TLD-OPS Incident Response Community Repository" email does not list one contact per line in outlook. We need to figure out how to have one contact per line.	Fred	9-Sep-17	Open	01-Jan-18	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.
81	Send Dave Piscitello email to present at TLD-OPS at beginning of block 5	Erwin	9-Sep-17	Closed	15-Oct-17	Erwin to send email asking Dave to present with focus on TLD-OPS attendees.

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
https://ccnso.icann.org/workinggroups/tld-ops-enhanced-incident-response-capabilities-cctlds-14apr16-en.pdf
Arabic, Chinese, English, French, Russian, Spanish, Russian

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