



**TLD-OPS Update**  
**ccTLD Security and Stability Together**

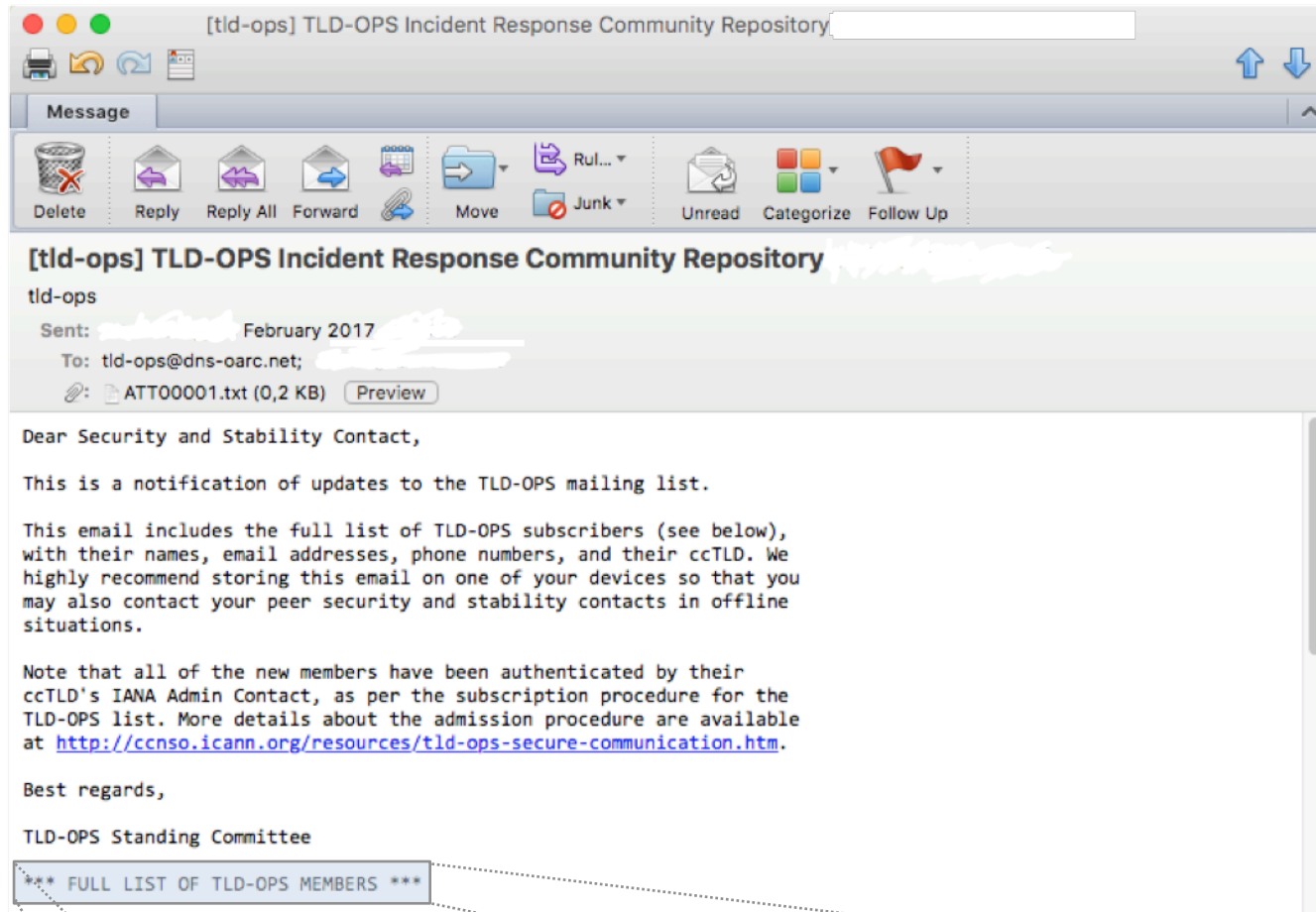
**ccNSO Members Day**  
**March 14, 2017**  
**ICANN58, Copenhagen**

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)

# Contact Repository Email



“John Doe, #1, .nl, +31 123456789” [john.doe@nic.nl](mailto:john.doe@nic.nl)  
“Jane Doe, #1, .vn, +84 123456789” [jane.doe@nic.vn](mailto:jane.doe@nic.vn)

# Security Alerts and Queries

#	Description	Month
10	Registry front-end compromise 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
<b>Total</b>	<b>187</b>	64%	<b>104</b>	36%	<b>291</b>

ASCII	Members	%	Missing	%	Total
<b>Total</b>	<b>158</b>	<b>64%</b>	<b>87</b>	<b>36%</b>	<b>245</b>
AF	23	45%	28	55%	51
AP	49	60%	33	40%	82
EU	65	100%	0	0%	65
LAC	17	40%	25	60%	42
NA	4	80%	1	20%	5

IDN	Members	%	Missing	%	Total
<b>Total</b>	<b>29</b>	63%	<b>17</b>	37%	<b>46</b>

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

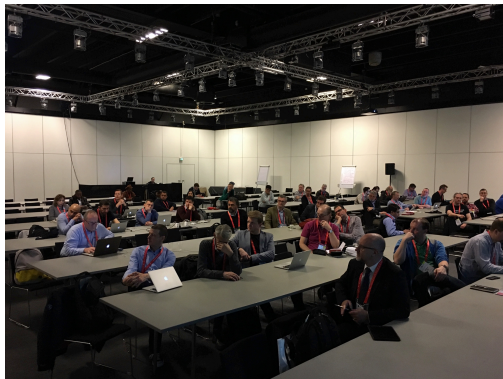
# Workshop Stats

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

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)



## 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** (65% 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 inbox, 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

Place  
Stamp  
Here

© 2017 ICANN. All Rights Reserved. ccTLD

We obtained your address from the IANA root zone database at <http://www.iana.org/domains/root/db>

# 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<sup>nd</sup> 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

# 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**

<https://ccnso.icann.org/workinggroups/tld-ops-enhanced-incident-response-capabilities-cctlds-14apr16-en.pdf>

Arabic, Chinese, English, French, Russian, Spanish, Russian

## **Contact**

Cristian Hesselman

Standing Committee Chair

+31 6 25 07 87 33

[cristian.hesselman@sidn.nl](mailto:cristian.hesselman@sidn.nl)

@hesselma