



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

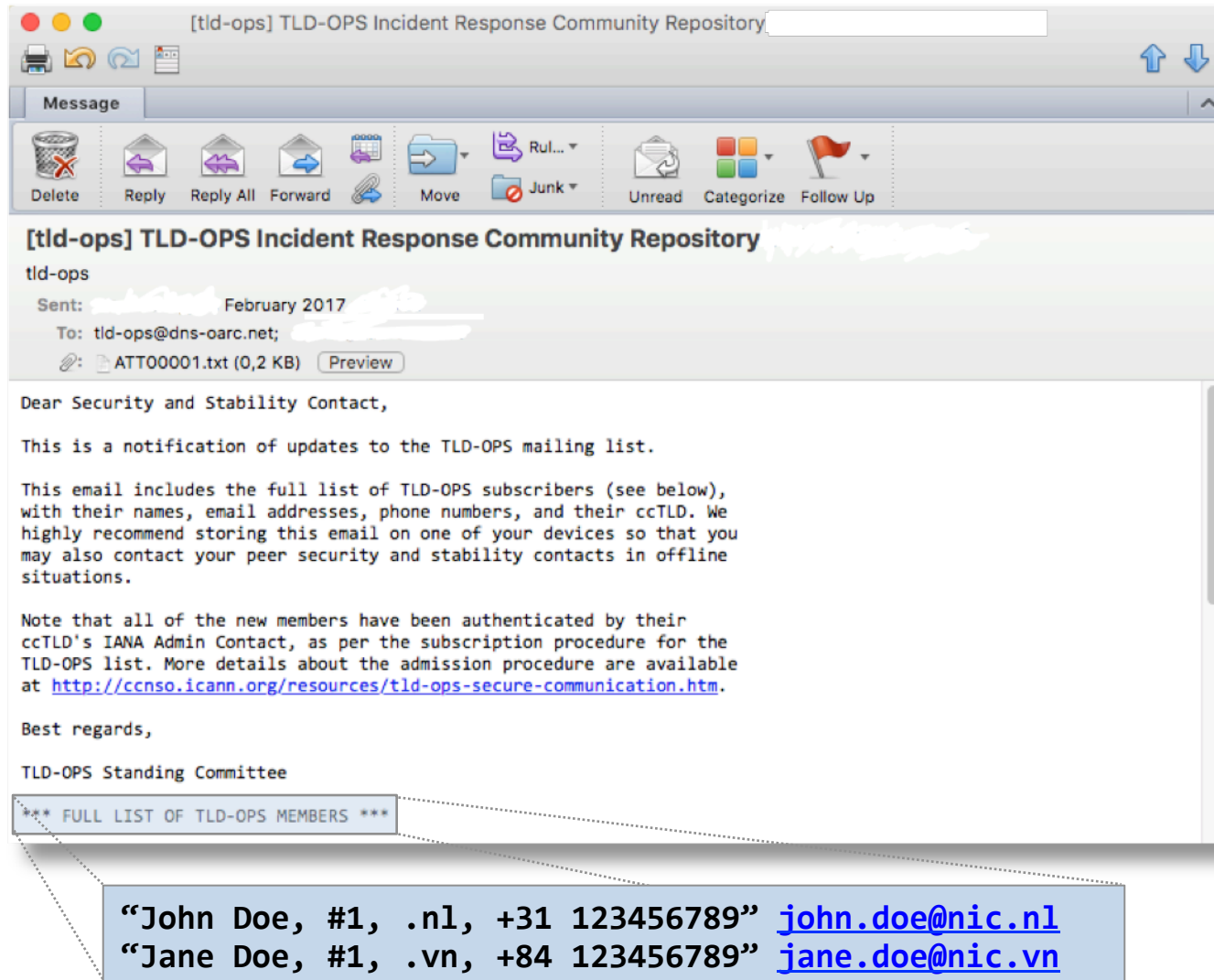
**ccNSO Members Day**  
**June 27, 2017**  
**ICANN59, Johannesburg**

Jacques Latour, .ca (incoming TLD-OPS Standing Committee Chair)  
Cristian Hesselman, .nl (outgoing TLD-OPS Standing Committee Chair)

# TLD-OPS

- Global technical incident response community *for and by* ccTLDs, open to *all* ccTLDs
- Brings together 340+ people who are responsible for the operational security and stability of 189 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



# Security Alerts and Queries

#	Description	Month
11	Two DDoS attacks on a registry's name servers	Mar-17
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>189</b>	65%	<b>102</b>	35%	<b>291</b>

ASCII	Members	%	Missing	%	Total
<b>Total</b>	<b>160</b>	<b>65%</b>	<b>85</b>	<b>35%</b>	<b>245</b>
AF	23	45%	28	55%	51
AP	50	61%	32	39%	82
EU	65	100%	0	0%	65
LAC	18	43%	24	57%	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: June 2, 2017

# TLD-OPS Operations Since ICANN58

- Security alerts
  - Two DDoS attacks on a registry's name servers (March)
- Membership updates
  - Joined: .ir (Islamic Republic Of Iran), .gp (Guadeloupe)
  - Contact updates: 8 (new, removal)

# Contact Us If Your ccTLD is on This List!

AF	AP	LAC	NA
.ac Ascension Islands	.az Azerbaijan	.ag Antigua and Barbuda	.gl Greenland
.ao Angola	.bd Bangladesh	.ai Anguilla	
.bj Benin	.bt Bhutan	.bo Bolivia	
.cd Congo, the Democratic Rep	.ck Cook Islands	.bs Bahamas	
.cf Central African Republic	.cx Christmas Islands	.bz Belize	
.cg Congo, Republic of	.dj Djibouti	.cu Cuba	
.ci Cote d'Ivoire	.gu Guam	.ec Ecuador	
.cm Cameroon	.hm Heard and McDonald Islar	.gf French Guiana	
.er Eritrea	.io British Indian Ocean Ter	.gs S. Georgia & the S. Sandwich Islands	
.et Ethiopia	.kg Kyrgystan	.gy Guyana	
.ga Gabon	.kp Korea, Democratic Peop	.ht Haiti	
.gn Guinea	.kz Kazakhstan	.hn Honduras	
.gq Equatorial Guinea	.mh Marshall Islands	.jm Jamaica	
.gw Guinea--Bissau	.mm Myanmar	.kn Saint Kitts and Nevis	
.lr Liberia	.mp Northern Mariana Islar	.ky Cayman Islands	
.ls Lesotho	.mv Maldives	.mq Martinique	
.ml Mali	.nc New Caledonia	.ms Montserrat	
.mr Mauritania	.nf Norfolk Island	.mx Mexico	
.na Namibia	.np Nepal	.pe Peru	
.ne Niger	.nr Nauru	.sr Suriname	
.sd Sudan	.om Oman	.sv El Salvador	
.sl Sierra Leone	.pf French Polynesia	.sx Sint Maarten	
.so Somalia	.pk Pakistan	.tc Turks and Caicos Islands	
.st Sao Tome and Principe	.pw Palau	.vc Saint Vincent and the Grenadines	
.sz Swaziland	.tc Turks and Caicos Islands		
.td Chad	.tj Tajikistan		
.tg Togo	.tk Tokelau		
.zw Zimbabwe	.tm Turkmenistan		
	.to Tonga		
	.tv Tuvalu		
	.ws Samoa		
	.ye Yemen		

# Standing Committee Results Since ICANN58

- Published membership update procedure
- Shared summary of TLD-OPS workshop at ICANN58
  - TLD-OPS community, ccNSO, SSAC, RSSAC
- Shared results of TLD-OPS membership survey
  - Over 80% of respondents value TLD-OPS highly (60%) to moderately (20%).
- Updated TLD-OPS leaflet (currently being translated)
- Minor update of TLD-OPS website
- Drafted DDoS mitigation framework based on ICANN58 workshop



# 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

# 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

# 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

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](mailto:jacques.latour@cira.ca)