TLD-OPS Update
ccTLD Security and Stability Together

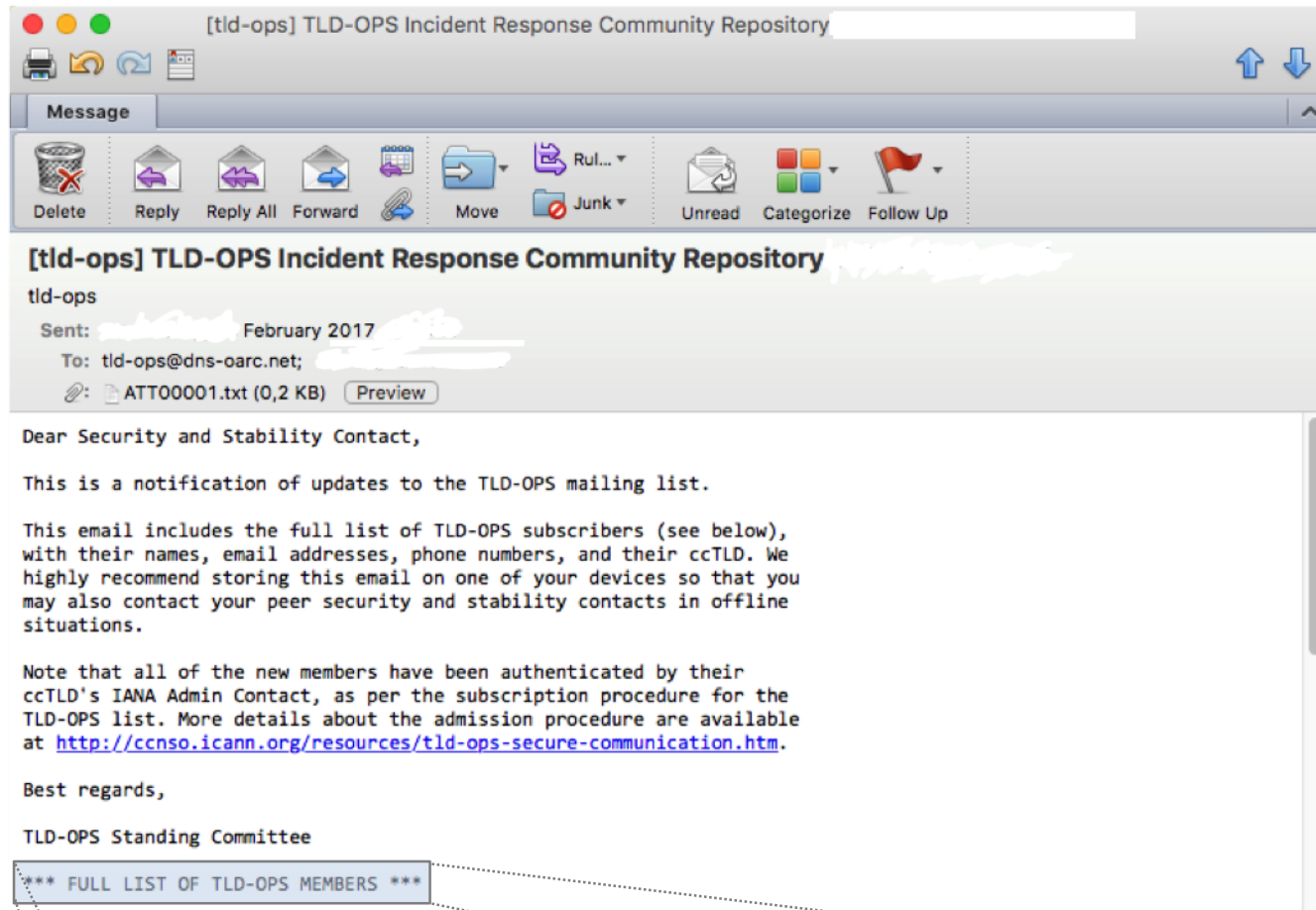**ccNSO Members Day**

March 11, 2018
ICANN61, San Juan

Jacques Latour, .ca (Chair)

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 193 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)

ccNSO   ICANN

Contact Repository Email

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

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

tld-ops

Sent: February 2017

To: tld-ops@dns-oarc.net;

ATTO0001.txt (0,2 KB) [Preview]

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: 345+ subscribers from 192 ccTLDs

ccNSO   ICANN

TLD-OPS Operations Since ICANN60

- Security alerts
  - No new alerts since last ICANN meeting

- Membership updates
  - Joined: .ag Antigua and Barbuda (LAC)
  - Contact updates: 2 (new, removal)

- Active standing committee outreach to missing members

Security Alerts and Workshops

#	Description	Month
12	Alert: Malware use DNS to steal personal info	Feb-18
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
	…	

- DDoS Mitigation Workshop @ ICANN59 and ICANN60
  - Draft DDoS mitigation playbook available

ccNSO   ICANN

TLD-OPS Membership Stats

All	Members	%	Missing	%	Total
Total	*193*	66%	*98*	34%	*291*

ASCII	Members	%	Missing	%	Total
Total	*164*	*67%*	*81*	*33%*	*245*
AF	25	49%	26	51%	51
AP	50	61%	32	39%	82
EU	65	100%	0	0%	65
LAC	19	45%	23	55%	42
NA	5	100%	0	0%	5

IDN	Members	%	Missing	%	Total
Total	*29*	63%	*17*	37%	*46*
Date: Feb 26, 2018					

ccNSO   ICANN

Standing Committee Results Since ICANN60

- ICANN59 and ICANN60 TLD-OPS DDoS Mitigation workshop outcome
  - Developed a draft document : DDoS mitigation playbook
  - Shared with TLD-OPS and soliciting feedback

ccNSO   ICANN

Contact Us If Your ccTLD is on This List!

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

TLD-OPS Standing Committee

ccNSO   ICANN

Objectives ICANN60

- Summarize the ICANN 60 TLD-OPS workshops outcome into a draft DDoS Mitigation playbook

- Develop a strategy for TLD-OPS workshops (ICANN workshop and participating in regional workshop)

- Increase membership by 3 to 195

ccNSO ICANN

Q&A

TLD-OPS Standing Committee
Frederico Neves, .br
Jacques Latour, .ca (chair)
Erwin Lansing, .dk
Régis Massé, .fr
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

ccNSO   ICANN