** Call for Participation **

TLD-OPS Workshop on the Collaborative Detection and Mitigation of DDoS Attacks on ccTLDs

ICANN58, Copenhagen, Denmark
Sunday March 12, 2017, 09:00-12:00 Local Time
Room: to be confirmed

Goal

The goal of the workshop is to explore how TLD-OPS members can collaborate to detect and mitigate DDoS attacks.

Motivation

The TLD-OPS Standing Committee is organizing the workshop because of the recent large-scale attacks on the DNS, such as on Dyn's DNS services (October 2016) and on the DNS root (July 2016 and November 2015), which may increasingly target ccTLDs as well.

TLD-OPS is the incident response community for and by ccTLDs. Its purpose is to enable TLD-OPS members to collaboratively detect and mitigate relevant security and stability-related incidents on a global level, including DDoS attacks. The aim of TLD-OPS is to further extend members' existing incident response structures, processes, and tools and not to replace them.

Since DDoS attacks may have a severe impact on the target (and potentially collateral damage for others), the TLD-OPS Standing Committee believes it is important to mobilize the collective experience of the TLD-OPS community on how to detect and mitigate DDoS attacks within TLD-OPS. The workshop facilitates this dialog through sharing of experiences, discussion, and generation of ideas. We will be looking the topic from multiple perspectives, such as technical, operational, compliance, and strategic.

Targeted Results

- A shared understanding of the role of TLD-OPS in collaboratively detecting and handling DDoS attacks on ccTLDs.
- A list of best practices and tools for TLD-OPS members, such as templates for DDoS alerts (email, SMS) and guidelines on how to integrate TLD-OPS in ccTLD's existing incident response structures, processes, and tools.
- Items that need to be discussed further within the TLD-OPS community or the larger ICANN incident response community.

The TLD-OPS Standing Committee will share a summary of the outcome of the workshop on the TLD-OPS mailing list and a high-level abstract with the broader ccNSO community, SSAC, and RSSAC.

Admittance
This will be an *invite-only* workshop for everyone on the TLD-OPS mailing list and authorized proxies (see Registration). We will also invite two representatives of the Security and Stability Advisory Committee (SSAC) and two people of the Root Server System Advisory Committee (RSSAC).

The meeting will not be recorded, streamed, or transcribed and there will be no remote participation. Attendees must bring a printout of their invitation. We will also check your badge against our attendee list.

The workshop depends on interactive audience and we therefore expect attendees to actively participate in discussions, both during the plenary sessions and in breakout groups.

Registration
If you would like to attend, then please register by sending an email to the TLD-OPS Standing Committee chair at cristian.hesselman@sidn.nl by March 5, 2017.

If you won't be attending ICANN58 but someone else from your ccTLD will, then you may authorize this person to attend the workshop on your behalf. In this case, you as a TLD-OPS subscriber will need to register the other person for the workshop by providing the person's contact information in the registration email and indicate that this person will be acting on your behalf at the workshop. Each TLD-OPS subscriber can register at most one such proxy.

Preliminary Agenda

Time	Description	Who
09:00	Opening and introduction	Chair
09:05	Inspiration talk: "DDoS DNS attacks – Feedback, prevention and countermeasures at .FR"	Régis Massé, AFNIC
09:30	Working session 1: brainstorm • Breakout in four groups, each using one flip chart • How could TLD-OPS help improving the detection and handling of DDoS attacks in a collaborative way? • Taking into account other incident response structures and tools that members are using • Collect ideas using post-its, inspired by presentation of AFNIC and experience of attendees	All
10:00	Coffee break • Standing Committee groups post-its in four categories • Such as technical, operational, compliance, strategic	
10:30	Working session 2: further exploration • Again breakout in four groups, one per flip chart • Discuss concrete actions, new insights, and items for	All

	further discussion	
11:15	Plenary discussion • Groups report back in plenary session (5 min each) • Using flip charts to present and discuss	All
11:45	Wrap up and next steps • Standing Committee takes pics of flip charts • Share on TLD-OPS list plus a short summary	Chair
12:00	Closing	Chair

Venue
Bella Center, Copenhagen, Denmark
Sunday March 12, 2017
09:00-12:00 Local Time
Room: to be confirmed

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 (Liaison to SSAC)
John Crain (Liaison to ICANN's security team)
Kim Davies (Liaison to IANA)

ICANN Staff: Kimberly Carlson

TLD-OPS Homepage
https://ccnso.icann.org/resources/tld-ops-secure-communication.htm