

ccTLD Security and Stability Together



TLD-OPS ccTLD Security and Stability Together

May 24, 2022 ccTLD News Sessions on Cybersecurity

Régis Massé, .fr (Vice Chair)



TLD-OPS introduction

- Global technical incident response community for and by ccTLDs, open to all ccTLDs (ASCII and IDN)
- Brings together **400+ people** who are responsible for the operational security and stability of 200+ different ccTLDs
- 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
- Builds on standard mailing list
- 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



Together, we create value for the community



New tools for the community



A first delivery: the DDOS Mitigation Playbook

- The goal of the first workshop was to explore how TLD-OPS members can collaborate to detect and mitigate DDOS attack
- Two sessions took place during ICANN Mettings 58 and 60 to share experiences, discussions and generation of ideas
- The topic has approched from multiple persepctives, such as technical, operational, compliance and strategic

DDoS Mitigation Playbook

DDoS Scope: ccTLD DNS infrastructure

TLD-OPS Workshop

Version 1.0 - April 25, 2018

Workshop Overview

The goal of the workshop was to explore how TLD-OPS members can collaborate to develop a DDoS Mitigation Playbook. The focus was on DDoS targeted at the unicast and anycast Authoritative DNS infrastructure, operated by the ccTLD and their DNS provider partners.

This workshop was in response to the TLD-OPS DDoS Mitigation workshop held at ICANN58 in Copenhagen on March 12, 2017. 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 to develop and document a framework to better prepare the ccTLDs in responding to DDoS attacks.

The workshop facilitated this dialog through sharing of experiences, discussion, and generation of ideas

TLD-OPS DDoS Mitigation Workshop #2- ICANN61, 2017-10-29, General Observations

We had a smaller group for this workshop: 22 people. This allowed for good dynamics & collaboration. We gathered in front of a single flipchart, went through previous workshop results, and expanded each topic to focus on elements that would be part of the guidebook, for each lifecycle stage. The results that were captured in flip charts are interpreted in this document.

The life cycles for 'effective' DDoS mitigation are:

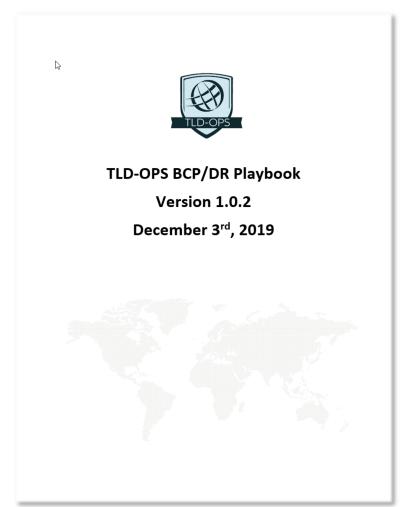
- Protect
- Detect Respond

The scope of this document is not to develop a complex security framework for DDoS mitigation. The goal is to highlight the important components in each life cycle for a ccTLD to be effective in mitigating a DDoS attack (if and when implemented).

It was mentioned in the workshop that it's always a good idea to implement best practice such as IT (ITIL) Service Operations and Information Security Management (cybersecurity).

The second project – DR/BCP Playbook

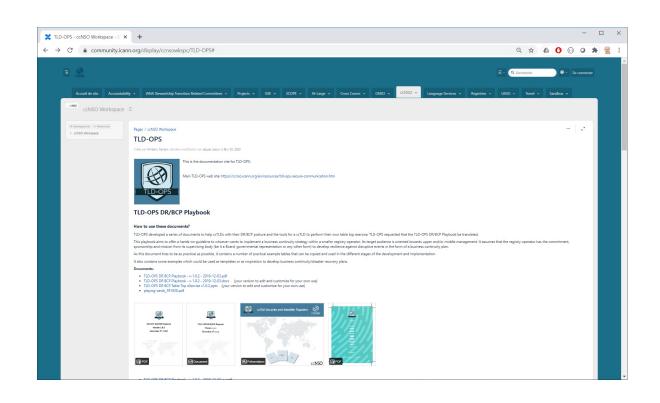
- The Playbook Goals
 - How to bring DR, BCP to small ccTLD
 - Focus only on ccTLD relevant activities
 - Step by step by scenario
 - Simplicity
- It is practical with minimal emphasis on theory
- It focusses on exceptional, disruptive incidents; not on operational issue
- This is **not** an IT project it requires guidance & commitment by top management





Where can I download these documents?

https://community.icann.org/display/ccnsowkspc/TLD-OPS#

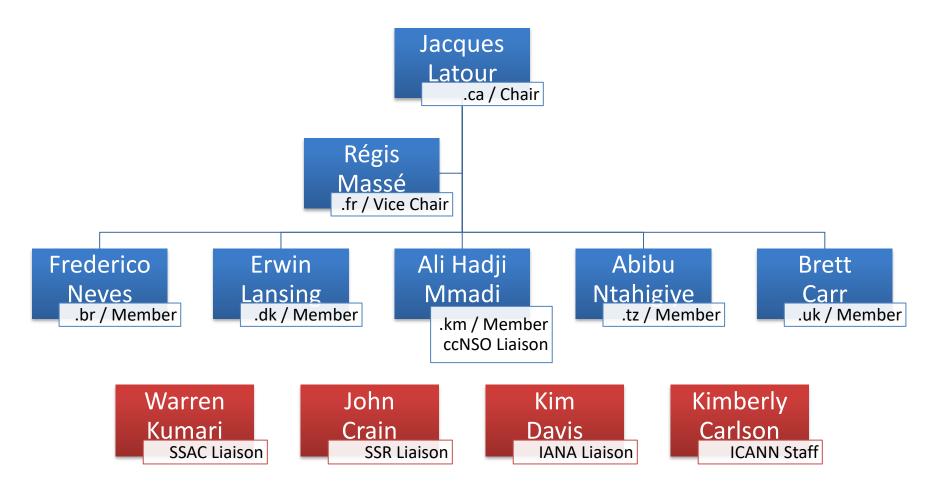




All the documents are translated and free to download



TLD-OPS Standing Committee Comité permanent TLD-OPS





Ressources & Contacts



http://ccnso.icann.org/resources/tld-ops-secure-communication.htm









ccTLD Security and Stability Together





