TLD-OPS
ccTLD Security and Stability Together

APTLD 74 – Tashkent, Uzbekistan
September 21, 2018

Régis Massé
Afnic (.fr) / TLD-OPS Vice-Chair
TLD-OPS, what is it?

• 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)
Together, we are stronger

- Open and global incident response community for and by ccTLDs
- Builds on standard mailing list (192 ccTLDs, 345+ subscribers, 99 ccTLDs missing)
- Enhances local incident response facilities, not a replacement
- 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
- Easy to join (through IANA Admin Contact)
Together, we create value for the community

New tools for the community
It’s time to join the TLD-OPS community

- **Easy**: Just send an email to join
- **Secure**: Identified and trusted contacts
- **Helpful**: Community help in case of an incident
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 Meetings 58 and 60 to share experiences, discussions, and generation of ideas.
- The topic has approached from multiple perspectives, such as technical, operational, compliance, and strategic.
What’s next?
Natural Disasters – DR/BCP Readiness

• Expand to general Disaster Recovery and Business Continuity Planning
  – Request from community following natural disasters
  – BCP is many things to many people
  – Where to start?
  – Where to focus?
  – Past Experience?

• Technical continuity plans for the DNS, Registry and corporate systems

• The Business part focuses on plans, initiation, testing, critical event, communications, simulation
Focus for the TLD-OPS community

DNS resolution infrastructure

Registry system (SRS, RDDS, Data Escrow ...)

IT infrastructure: network, storage, servers, softwares

Emergency communication tools
Feedback from the community

What does the community need? A playbook with advises, a synthesis of feedbacks...

Past experience from the ccTLDs

Different type of actions depending on the geographical area

Presentation of different types of technical continuity plans
Tentative action plan

- ICANN 62 – TechDay Presentation
- ICANN 62 ccNSO Presentation
- ICANN 63 Workshop
- Playbook delivery

NEXT STEP
Q&A

**TLD-OPS Standing Committee**
Frederico Neves, .br
Jacques Latour, .ca (chair)
Erwin Lansing, .dk
Régis Massé, .fr (vice-chair)
Ali Hadji Mmadi, .km
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**
Arabic, Chinese, French, Russian, Spanish

**Contacts**
Jacques Latour
Standing Committee Chair
+1.613.291.1619
jacques.latour@cira.ca

Régis Massé
Standing Committee Vice-Chair
+33.6.83.12.43.49
regis.masse@afnic.fr