TLD-OPS

ccTLD Security and Stability Together

Incident contact repository • Security alerts • Global collaboration • Workshops

Need Help?
tld-ops@lists.dns-oarc.net

TLD-OPS is the global technical incident response community for and by ccTLDs. It brings together folks who are responsible for the operational security and stability of their ccTLD.

192 Members*

163 ASCII ccTLDs
From .ad (Andorra) to .zm (Zambia)

29 IDN ccTLDs
From .ভারত (India) to . المغرب (Morocco)

People
345+ experts on operational ccTLD security and stability

Governance
100% by ccTLDs, through the TLD-OPS Standing Committee

Added value
Improve your ccTLD's reachability in incident response situations, receive and share relevant security alerts and queries

The goal of the TLD-OPS community is to enable ccTLD operators worldwide to collaboratively detect and mitigate incidents that may affect the operational security and stability of ccTLD services and of the wider Internet, such as DDoS attacks, malware infections, and phishing attacks. TLD-OPS is open to all ccTLDs and currently brings together 340+ people who are responsible for the operational security and stability of 192 different ccTLDs. TLD-OPS further extends members' existing incident response structures, processes, and tools and does not replace them.

Contact Repository

The TLD-OPS community builds on a standard mailing list that acts as an incident response contact repository for ccTLDs. Subscribers receive an automatically generated email from the list once a month that contains the contact repository of all member ccTLDs (contact persons, phone numbers, and email addresses). This improves the reachability of TLD-OPS members because everyone has everyone else's contact information readily available in their inbox, which typically also works in offline emergency situations.

Security Alerts

Because TLD-OPS represents ~65% of all ccTLDs worldwide, members also actively use the mailing list to share security alerts and queries, for instance on DDoS attacks and malware that uses the name space of ccTLDs. Since incident response is all about learning, members are encouraged to share how they handled certain incidents, either on the mailing list or at scheduled TLD-OPS workshops.

Governance

The TLD-OPS list was set up for and by ccTLDs in 2014/2015 [1]. It is fully governed by the ccTLD community through the TLD-OPS Standing Committee, which consists of operational people of ccTLDs that cover all five geographic regions (Africa, Asia-Pacific, Europe, North America, and Latin America-Caribbean) as well as of representatives from SSAC, IANA, and ICANN's security team. The Standing Committee oversees the list's daily operation and the further development of the "TLD-OPS ecosystem". ICANN provides administrative support through the ccNSO Secretariat. The list server runs on "neutral ground" at DNS-OARC.

* As of Nov 27, 2017. Current list of members is on the TLD-OPS homepage.

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

Joining is Easy!

Joining the TLD-OPS list is extremely easy because it's an email list. The list is however only accessible to people who are responsible for the operational security and stability of a ccTLD and who have been authenticated as such by their IANA administrative contact.

To join the list, ask your IANA administrative contact to send an email with the names, email addresses (primary and secondary), and phone numbers of the security and stability contacts of your ccTLD to the ccNSO Secretariat. Please use the subscription template on the right, which is also available for copying and pasting on the TLD-OPS homepage.

Important: your subscription request email must come from the administrative contact address you have currently registered in the IANA database [2]. If this is not possible, then you must copy this email address in your subscription request email. Otherwise, we cannot subscribe you to the list.

Personal Trust

The TLD-OPS list is based on personal trust, which means that subscribers can only join with their own email address and phone number. The underlying rationale is that a personal trust model will contribute to further increasing trust within the ccTLD community, for instance because people start recognizing each other's names and have met each other at the TLD-OPS workshops. Role-based contacts are therefore not allowed on the list, however a contact with a role based primary email address is acceptable.

The vouching model that is typically used in the incident response community is unsuitable for TLD-OPS because the ccTLD community is such a large group (291 ccTLDs in total) that it will be hard to onboard relatively unknown people using this model.

Rules of Engagement

All information exchanged on the list to obtain the incident response contact information of a ccTLD is confidential and must not be shared outside the TLD-OPS community.

Subscription Template

Please use the format below to subscribe to the TLD-OPS list. It's also available from the TLD-OPS homepage for copying and pasting.

```
-- Start of message --
From: ccTLD IANA Admin Contact or authorized delegate
To: ccNSO Secretariat < TLD-OPS-Admin@icann.org>
Cc: ccTLD IANA Admin Contact Address
Subject: Request to join the TLD-OPS mailing list

Dear ccNSO Secretariat,

I would like to subscribe the people below to the TLD-OPS list.
I hereby confirm that they are responsible for the overall
security and stability of my ccTLD, and that I am the IANA
Admin Contact of my ccTLD or that I am authorized to act on
his/her behalf.

Best regards,

IANA Admin Contact of <ccTLD>

== INCIDENT RESPONSE CONTACT INFORMATION ==

Contact Person #1 (primary):
Name: <FirstName1> <LastName1>
Email address: <PrimaryEmailAddress1>, <SecondaryEmailAddress1>
Mobile phone number: +<country code> <number>

Contact Person #2 (secondary):
Email address: <PrimaryEmailAddress2>, <SecondaryEmailAddress2>
Email address: <EmailAddress2>
Mobile phone number: +<country code> <number>
<- - ->
Contact Person #6:
Name: <FirstName6> <LastName6>
Email address: <PrimaryEmailAddress6>, <SecondaryEmailAddress6>
Mobile phone number: +<country code> <number>
-- End of message --
```

Information on actual security incidents must be flagged using the colors of the Traffic Light Protocol (TLP) [2]: red (information for named recipients only), amber (limited distribution), green (community-wide distribution), or white (unlimited distribution). TLD-OPS follows the TLP definitions of US-CERT [3] and the default color is TLP-AMBER.

List members must not share automatically generated information on the list. The TLD-OPS list is unencrypted to enable every ccTLD to join. ■

References

[1] SECIR WG Final Report, http://ccnso.icann.org/workinggroups/secir.htm

[2] IANA Root Database, https://www.iana.org/domains/root/db

[3] Traffic Light Protocol, http://en.wikipedia.org/wiki/Traffic_Light_Protocol

[4] US-CERT definition of the TLP, https://www.us-cert.gov/tlp

About

Leaflet by the TLD-OPS Standing Committee. Version 2.6, Nov 27, 2017.