TLD-OPS

Enhanced Incident Response Capabilities for and by ccTLDs

Need Help?

tld-ops@lists.dns-oarc.net

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

175 Members*

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

28 IDN ccTLDs
From .中国 (China) to .فلسطين (Palestine)

Governance
100% by ccTLDs, support from ICANN and DNS-OARC

Subscription
Through email, CC'ing your IANA Admin Contact address

Usage
Make your ccTLD's incident response contacts easy to lookup by your peers, receive and share relevant security alerts

The goal of the TLD-OPS community is to enable ccTLD operators worldwide to collaboratively strengthen their incident response capabilities. Our targeted impact is a further increased level of security and stability of ccTLD services (DNS and registration) worldwide and of the Internet infrastructure at large. TLD-OPS is open to every ccTLD, irrespective of ccNSO membership.

Contact Repository

The TLD-OPS community revolves around the TLD-OPS mailing list, which serves as a contact repository for ccTLDs. Subscribers regularly receive an automated email from the list that contains an overview of all subscribed ccTLDs and their incident response contact information (contact persons, phone numbers, and email addresses). This allows them to (i) use their inbox to look up another ccTLD's contact information, which is both easy and quick and (ii) to store contact information locally on their device (local inbox), which enables them to lookup contact information in offline situations. Subscribers thus improve their reachability in incident response situations, allowing them to detect and resolve threats more quickly with the help of their peers.

Security Alerts

TLD-OPS represents 61% of all ccTLDs worldwide, which also makes it an excellent forum for sharing security alerts, for instance to report on malware that uses the name space of ccTLDs. We therefore encourage all subscribers to put such alerts on the list. To bootstrap this process, we have teamed with ICANN's security team, who packages generic security alerts for us to share on the TLD-OPS list.

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 representatives of ccTLDs that cover all five geographic regions (Africa, Asia-Pacific, Europe, North America, and Latin America-Caribbean) and liaisons 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". The ccNSO Secretariat provides administrative support. The list server runs at DNS-OARC.

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

* As of April 14, 2016. Current list of members is on the TLD-OPS homepage.

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 overall 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, 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. 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. Information on your administrative contact is available from the IANA database at https://www.iana.org/domains/root/db.

Personal Trust

The TLD-OPS list is based on personal trust, which means that subscribers can only join with their personal 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. Role-based email addresses are not allowed on the list.

The vouching model that is typically used in the incident response community is unsuitable for the TLD-OPS list. This is because the ccTLD community is a large group, which means that it will be hard to get relatively unknown people on the list 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.

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].

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

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 <ccnsosecretariat@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: <EmailAddress1>
Mobile phone number: +<country code> <number>

Contact Person #2 (secondary):
Name: <FirstName2> <LastName2>
Email address: <EmailAddress2>
Mobile phone number: +<country code> <number>

Contact Person #3:
Name: <FirstName3> <LastName3>
Email address: <EmailAddress3>
Mobile phone number: +<country code> <number>
-- End of message --
```

References

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

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

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

About

Leaflet by the TLD-OPS Standing Committee. Version 2.3, April 14, 2016.