



192 membres*

163 ccTLD ASCII

De .ad (Andorre) à .zm (Zambie)

29 ccTLD d'IDN

De .ଭାରତ (Inde) à .

ⵜⴰⴳⴷⵓⴷⴰ (Maroc)

Individus

Plus de 345 experts en matière de sécurité et stabilité opérationnelles des ccTLD

Gouvernance

Assurée à 100 % par les ccTLD via le Comité permanent du TLD-OPS

Valeur ajoutée

Renforcer l'accessibilité de votre ccTLD en cas d'intervention suite à un incident, recevoir et partager des alertes et requêtes de sécurité

Le TLD-OPS est la communauté mondiale qui intervient en cas d'incidents techniques pour et par les ccTLD. Il rassemble des individus responsables de la sécurité et la stabilité opérationnelles

L'objectif de la communauté du TLD-OPS est de permettre aux opérateurs de ccTLD de collaborer afin de détecter et d'atténuer les incidents qui pourraient affecter la sécurité et la stabilité opérationnelles des services de ccTLD et plus largement de l'Internet, tels que les attaques par DDoS, les infections par des logiciels malveillants et les attaques par hameçonnage. Le TLD-OPS est ouvert à tous les ccTLD et rassemble actuellement plus de 340 individus qui sont responsables de la sécurité et la stabilité opérationnelles de 192 ccTLD différents. Le TLD-OPS s'ajoute aux structures, processus et outils existants d'intervention en cas d'incidents des membres mais ne les remplace pas.

Référentiel de contacts

La communauté du TLD-OPS s'appuie sur une liste de diffusion standard qui fait office de référentiel de contacts d'intervention en cas d'incidents pour les ccTLD. Les abonnés reçoivent une fois par mois un e-mail généré automatiquement par la liste qui contient le référentiel de contacts de tous les ccTLD membres (personnes à contacter, numéros de téléphone et adresses e-mail). Cela renforce l'accessibilité des membres du TLD-OPS car tous les membres peuvent facilement recevoir les coordonnées de tout le monde, ce qui vaut en général aussi pour des situations d'urgence hors ligne.

Alertes de sécurité

Comme le TLD-OPS représente 65 % de tous les ccTLD du monde, les membres utilisent également activement la liste de diffusion pour le partage d'alertes et de requêtes de sécurité, par exemple en cas d'attaques par DDoS et de logiciels malveillants qui utilisent l'espace des noms des ccTLD. Dans la mesure où les interventions en cas d'incidents se fondent sur l'apprentissage, les membres sont encouragés à indiquer leur mode de gestion des incidents, soit sur la liste de diffusion soit lors des ateliers organisés par le TLD-OPS.

Gouvernance

La liste du TLD-OPS a été mise en place pour et par les ccTLD en 2014/2015[1]. Elle est totalement administrée par la communauté des ccTLD via le Comité permanent du TLD-OPS, qui est composé du personnel opérationnel des ccTLD des cinq régions géographiques (Afrique, Asie-Pacifique, Europe, Amérique du Nord et Amérique latine et Caraïbes) et des représentants du SSAC, de l'IANA et de l'équipe de sécurité de l'ICANN. Le Comité permanent supervise le fonctionnement quotidien de la liste et la poursuite du développement de « l'écosystème du TLD-OPS ». L'ICANN fournit un soutien administratif via le secrétariat de la ccNSO. Le serveur de la liste est basé « en terrain neutre » au DNS-OARC.

* Au 27 novembre 2017. La liste actuelle des membres est disponible sur la page d'accueil du

Il est facile de nous rejoindre !

Il est extrêmement facile de s'abonner à la liste du TLD-OPS parce qu'il s'agit d'une liste de diffusion par e-mail. Toutefois, la liste est exclusivement accessible aux personnes qui sont responsables de la sécurité et de la stabilité opérationnelles d'un ccTLD et qui ont été authentifiées comme telles par leur contact administratif de l'IANA.

Pour vous abonner à la liste, demandez à votre contact administratif de l'IANA d'envoyer un e-mail au secrétariat de la ccNSO avec les noms, les adresses e-mail et les numéros de téléphone des personnes à contacter chargées de la sécurité et de la stabilité de votre ccTLD. Veuillez utiliser le modèle d'abonnement de droite, que vous pouvez également copier et coller de la page d'accueil du TLD-OPS.

Important : votre e-mail de demande d'abonnement doit provenir de l'adresse de contact administratif qui est actuellement enregistrée dans la base de données de l'IANA[2]. Si cela n'est pas possible, vous devez mettre cette adresse électronique en copie dans votre e-mail de demande d'abonnement. Dans le cas contraire, nous ne pouvons pas vous abonner à la liste.

Confiance personnelle

La liste du TLD-OPS est basée sur la confiance personnelle, ce qui signifie que les abonnés ne peuvent s'abonner qu'avec leur numéro de téléphone et leur adresse électronique personnels. Le fondement de cette exigence est que le modèle de confiance personnelle contribuera à renforcer davantage la confiance au sein de la communauté des ccTLD, par exemple parce que les gens commencent à reconnaître les noms des autres et se sont rencontrés lors des ateliers du TLD-OPS. Les contacts correspondant à une fonction ne peuvent donc figurer sur la liste ; on accepte en revanche un contact disposant d'un e-mail primaire correspondant à une fonction.

Le modèle de recommandation qui est généralement utilisé dans la communauté qui intervient en cas d'incidents n'est pas approprié pour la liste du TLD-OPS étant donné que la communauté des ccTLD est un grand groupe (291 ccTLD au total) et qu'il serait difficile que des individus relativement inconnus soient admis dans la liste via ce modèle.

Règles de coordination

Toutes les informations échangées sur la liste pour obtenir les coordonnées de l'équipe d'intervention en cas d'incidents d'un ccTLD

Modèle d'abonnement

Veuillez utiliser le formulaire ci-dessous pour vous abonner à la liste du TLD-OPS. Il est également possible de le copier et coller depuis la page d'accueil du TLD-OPS.

-- Début du message --

De : Contact administratif de l'IANA du ccTLD ou son représentant autorisé

À : Secrétariat de la ccNSO < TLD-OPS-Admin@icann.org>

CC : adresse du contact administratif de l'IANA du ccTLD

Objet : demande d'abonnement à la liste de diffusion du TLD-OPS

Cher secrétariat de la ccNSO,

Je voudrais abonner les personnes ci-après à la liste du TLD-OPS. Je confirme par les présentes qu'elles sont responsables de la sécurité et la stabilité globales de mon ccTLD et que je suis le contact administratif de l'IANA de mon ccTLD ou que je suis autorisé à agir en son nom.

Cordialement,

Le contact administratif de l'IANA du <ccTLD>

== COORDONNÉES DE L'ÉQUIPE D'INTERVENTION EN CAS D'INCIDENTS ==

Personne à contacter n°1 (primaire) :

Nom : <Prénom1> <Nom1>

Adresse électronique : <Adresse électronique primaire1>, <Adresse électronique secondaire1>

Numéro de téléphone portable : +<code de pays> <numéro>

Personne à contacter n°2 (secondaire) :

Adresse électronique : <Adresse électronique primaire2>, <Adresse électronique secondaire2>

Adresse électronique : <AdresseÉlectronique2>

Numéro de téléphone portable : +<code de pays> <numéro>

< - - >

Personne à contacter n°6 :

Nom : <Prénom6> <Nom6>

Adresse électronique : <Adresse électronique primaire6>, <Adresse électronique secondaire6>

Numéro de téléphone portable : +<code de pays> <numéro>

-- Fin du message --

sont confidentielles et ne doivent pas être partagées en dehors de la communauté du TLD-OPS.

Les informations relatives à des incidents de sécurité réels doivent être signalées en utilisant les couleurs du protocole des feux de trafic (TLP)[2] : rouge (informations adressées uniquement aux destinataires désignés), jaune (diffusion limitée), vert (diffusion à l'échelle communautaire) ou blanc (diffusion illimitée). Le TLD-OPS suit les définitions du TLP d'US-CERT[3] et la couleur par défaut est TLP-AMBER.

Il est défendu aux membres de la liste de partager les informations générées automatiquement sur la liste. La liste du TLD-OPS n'est pas chiffrée afin de permettre à tous les ccTLD de s'y abonner. ■

Références

[1] Rapport final du SECIR WG : <http://ccnso.icann.org/workinggroups/secir.htm>

[2] Base de données de la zone racine de l'IANA : <https://www.iana.org/domains/root/db>

[3] Protocole des feux de trafic : http://en.wikipedia.org/wiki/Traffic_Light_Protocol

[4] Définition du TLP d'après US-CERT : <https://www.us-cert.gov/tlp>

À propos de

Dépliant du Comité permanent du TLD-OPS. Version 2.6, 27 novembre 2017.