



TLD-OPS es la comunidad global de respuesta a incidentes técnicos para y por ccTLD. Reúne a personas que son responsables de la seguridad y estabilidad operativas de sus ccTLD.

192 Miembros

163 ccTLD en código ASCII

Desde .AD (Andorra) hasta .ZM (Zambia)

29 IDN ccTLD

Desde .ଭାରତ (India) hasta .مغرب (Marruecos)

Personas

Más de 345 expertos en estabilidad y seguridad operativas de ccTLD

Gobernanza

100 % por los ccTLD, a través del Comité Permanente de TLD-OPS

Valor agregado

Mejore la accesibilidad de su ccTLD en situaciones de respuesta a incidentes, reciba y comparta alertas de seguridad y consultas relevantes

El objetivo de la comunidad de TLD-OPS es permitir que los operadores de ccTLD de todo el mundo detecten y mitiguen, de manera colaborativa, incidentes que puedan afectar la estabilidad y seguridad operativas de los servicios de ccTLD y de Internet en general, tales como ataques de DDOS, infecciones de malware y ataques de phishing. La comunidad de TLD-OPS está abierta a todos los ccTLD y actualmente reúne a más de 340 personas responsables de la estabilidad y seguridad operativas de 192 ccTLD diferentes. TLD-OPS extiende aún más las estructuras, los procesos y las herramientas de respuesta a incidentes existentes y no los reemplaza.

Repositorio de contactos

La comunidad de TLD-OPS se basa en una lista de correo electrónico estándar que actúa como un repositorio de contactos para respuesta a incidentes para los ccTLD. Una vez al mes, los suscriptores reciben un correo electrónico generado automáticamente a partir de la lista, el cual contiene el repositorio de contactos de todos los ccTLD miembros (personas de contacto, números de teléfono y direcciones de correo electrónico). Esto mejora la accesibilidad de los miembros de TLD-OPS porque todos tienen la información de contacto de todos los demás a su disposición en su bandeja de entrada, la cual generalmente también funciona en situaciones de emergencia fuera de línea.

Alertas de seguridad

Debido a que TLD-OPS representa aproximadamente el 65 % de todos los ccTLD en todo el mundo, los miembros también usan activamente la lista de correo electrónico para compartir alertas de seguridad y consultas, por ejemplo, sobre ataques de DDOS y malware que usa el espacio de nombres de los ccTLD. Dado que la respuesta a incidentes se trata de aprender, se alienta a los miembros a compartir cómo manejaron ciertos incidentes, ya sea en la lista de correo electrónico o en los talleres programados por TLD-OPS.

Gobernanza

La lista de TLD-OPS se creó por y para los ccTLD en 2014/2015 [1]. Está completamente regida por la comunidad de ccTLD a través del Comité Permanente de TLD-OPS, que está conformado por personas operativas de los ccTLD que cubren las cinco regiones geográficas (África, Asia-Pacífico, Europa, América del Norte y América Latina-Caribe), así como por representantes del SSAC, la IANA y el equipo de seguridad de la ICANN. El Comité Permanente supervisa el funcionamiento diario de la lista y el desarrollo ulterior del "ecosistema de TLD-OPS". La ICANN proporciona soporte administrativo a través de la Secretaría de la ccNSO. El servidor de la lista funciona en "campo neutral" en el DNS-OARC.

* Al 27 de noviembre de 2017. La lista actualizada de los miembros está disponible en la página de inicio de TLD-OPS.

¡Participar es fácil!

Participar en la lista de TLD-OPS es muy fácil porque se trata de una lista de correo electrónico. Sin embargo, únicamente pueden acceder a la lista las personas que son responsables de la seguridad y la estabilidad operativas de un ccTLD y quienes han sido autenticados como tales por su contacto administrativo de la IANA.

Para suscribirse a la lista, solicite a su contacto administrativo de la IANA que envíe un correo electrónico con los nombres, direcciones de correo electrónico (primaria y secundaria) y números de teléfono de los contactos de seguridad y estabilidad de su ccTLD al Secretario de la ccNSO. Por favor, utilice la plantilla de suscripción ubicada a la derecha, que también está disponible para copiar y pegar en la página principal de TLD-OPS.

Importante: su correo electrónico de solicitud de suscripción debe provenir de la dirección del contacto administrativo que actualmente está registrada en la base de datos de la IANA [2]. Si esto no es posible, entonces debe copiar esta dirección de correo electrónico en su correo electrónico de solicitud de suscripción. De lo contrario, no podremos suscribirlo a la lista.

Confianza personal

La lista de TLD-OPS se basa en la confianza personal, lo cual significa que los suscriptores sólo pueden unirse con su propia dirección de correo electrónico y su propio número de teléfono. El fundamento subyacente es que un modelo de confianza personal contribuirá a aumentar aún más la confianza dentro de la comunidad de ccTLD, por ejemplo, porque las personas comienzan a reconocer el nombre de otras y se han conocido entre sí en los talleres de TLD-OPS. Por lo tanto, los contactos basados en roles no están permitidos en la lista; sin embargo, un contacto con un rol basado en una dirección de correo electrónico primario, es aceptable.

El modelo de acreditación que habitualmente se utiliza en la comunidad de respuesta a incidentes no es adecuado para la lista de TLD-OPS porque la comunidad de ccTLD es un grupo tan grande (291 ccTLD en total) que será difícil incorporar gente relativamente desconocida mediante este modelo.

Reglas de participación

Toda la información intercambiada en la lista para obtener la información del contacto para respuesta a incidentes de un ccTLD es confidencial y no debe ser compartida fuera de la comunidad de TLD-OPS.

Plantilla de suscripción

Por favor utilice el formato de abajo para suscribirse a la lista de TLD-OPS. También está disponible para copiar y pegar desde la página principal de TLD-OPS.

- Comienzo del mensaje -

De: Contacto administrativo de la IANA o delegado autorizado para el ccTLD
A: Secretario de la ccNSO <TLD-OPS-Admin@icann.org>
Cc: Dirección del contacto administrativo de la IANA para el ccTLD
Asunto: Solicitud de suscripción a la lista de correo electrónico de TLD-OPS

Estimado Secretario de la ccNSO,

Desearía suscribir a las personas indicadas a continuación a la lista de TLD-OPS. Por la presente confirmo que dichas personas son responsables de la seguridad general y la estabilidad de mi ccTLD, y que yo soy el Contacto administrativo de la IANA o estoy autorizado para actuar en su nombre.

Cordialmente,

Contacto administrativo de la IANA para <ccTLD>

== INFORMACIÓN DE CONTACTO PARA RESPUESTA A INCIDENTES ==

Persona de contacto # 1 (primario):

Nombre: <Nombre1> <Apellido1>
Dirección de correo electrónico:
<Dirección1decorreoelectrónicoprimario>,
<Dirección1decorreoelectrónicosecundario>
Número de teléfono móvil: +<códigodepaís> <número>

Persona de contacto #2 (secundario):

Dirección de correo electrónico:
<Dirección2decorreoelectrónicoprimario>,
<Dirección2decorreoelectrónicosecundario>
Dirección de correo electrónico: <Direccióndecorreoelectrónico2>
Número de teléfono móvil: +<códigodepaís> <número>
<- - ->

Persona de contacto #6:

Nombre: <Nombre6> <Apellido6>
Dirección de correo electrónico:
<Dirección6decorreoelectrónicoprimario>,
<Dirección6decorreoelectrónicosecundario>
Número de teléfono móvil: +<códigodepaís> <número>
-- Fin del mensaje --

Toda la información intercambiada en la lista para obtener la información del contacto para respuesta a incidentes de un ccTLD es confidencial y no debe ser compartida fuera de la comunidad de TLD-OPS.

La información sobre incidentes de seguridad concretos debe estar marcada con los colores del Protocolo de Semáforo (TLP) [2]: rojo (información únicamente para destinatarios designados), ámbar/amarillo (distribución limitada), verde (distribución para toda la comunidad) o blanco (distribución sin limitaciones). TLD-OPS sigue las definiciones de TLP de US-CERT [3] y el color predeterminado es TLP-AMBAR.

Los miembros de la lista no deben compartir en la lista información que haya sido generada en forma automática. La lista de TLD-OPS no está encriptada para permitir la participación de todos los ccTLD. ■

Referencias

- [1] Informe Final del SECIR WG, <http://ccnso.icann.org/working-groups/secir.htm>
- [2] Base de datos de la raíz de la IANA, <https://www.iana.org/domains/root/db>
- [3] Protocolo de Semáforo (o TLP por sus siglas en inglés), http://en.wikipedia.org/wiki/Traffic_Light_Protocol
- [4] Definición del Centro de Conocimiento en Seguridad de Internet de los EE. UU. (US-CERT) para el TLP, <https://www.us-cert.gov/tlp>

Acerca de TLD-OPS

Folleto del Comité Permanente de TLD-OPS. Versión 2.6, 27 de noviembre de 2017