Notificar spam, mensajes de correo electrónico mal clasificados y virales

Contenido

Introducción

Este documento describe la notificación de correos electrónicos spam, mal clasificados, virales o adicionales a Cisco para su soporte o examen.

Tipos de envíos de mensajes de correo electrónico

Los mensajes de correo electrónico de spam, spam y marketing son:

- *Spam*: Mensajes de correo electrónico irrelevantes o inapropiados para un destinatario.
- *Jamón*: Un mensaje de correo electrónico que no es spam. O "no spam", "buen correo".
- *Comercialización*: Marketing directo de un mensaje de correo electrónico comercial.

Cisco acepta envíos para cualquier correo electrónico clasificado de forma incorrecta:

- false-negativo (spam perdido)
- falso positivo (o "Ham")
- mensajes de marketing falsos negativos
- mensajes de marketing falsos positivos
- mensajes sospechosos de phish, mensajes positivos de phish
- mensajes sospechosos de virus y virus positivos

¿Por qué informar de correos electrónicos a Cisco?

Mensajes de correo electrónico perdidos o marcados incorrectamente notificados a Cisco ayudan con la confirmación del contenido, la eficacia general y las reglas y puntuaciones asociadas. Una vez que haya notificado un mensaje de correo electrónico a Cisco, también podrá ver otros elementos observables y archivos adjuntos incrustados a través del portal de estado de correo electrónico.

Portal de estado de correo electrónico

Con una ID de CCO válida, puede iniciar sesión en https://talosintelligence.com/tickets/email_submissions. El portal de estado del correo electrónico es una herramienta para ver el estado de los envíos de correo electrónico a Cisco. Cisco fomenta los envíos de spam/phishing que han omitido el contenido de detección actual y Ham, correo electrónico deseable que se ha filtrado incorrectamente, para mejorar la eficacia general. El portal de estado de correo electrónico proporciona una forma de realizar un seguimiento del estado de estos envíos. Puede supervisar los envíos, y los administradores de dominio o los visores de dominio pueden supervisar todos los envíos de sus dominios.

> **Nota**: El portal de envío y seguimiento de mensajes de correo electrónico (ESTP) heredado se ha sustituido por el portal de estado de correo electrónico, alojado en Talosintelligence.com, a partir del 1 de septiembre de 2020.

Cómo informar mensajes de correo electrónico a Cisco

Los métodos admitidos son:

1. Complemento Cisco Secure Email Submission
   Compatible con Outlook (Windows, Mac y Web)
2. Cisco Email Security Plug-In Compatible con Outlook (sólo Windows)
3. Envío directo por correo electrónico del usuario final

Complemento Cisco Secure Email Submission

El complemento Cisco Secure Email Submission es compatible con Microsoft Outlook para Windows, Mac y Web. Consulte "Configuraciones admitidas para Cisco Secure Email Encryption Service Add-In y Cisco Secure Email Submission Add-in" en la Matriz de compatibilidad para Cisco Secure Email Encryption Service para garantizar la compatibilidad con su versión de Outlook.

Consulte Complemento Cisco Secure Email Submission para ver la documentación de descarga e instalación.

Complemento Cisco Email Security

Cisco Email Security Plug-in sólo admite Microsoft Outlook en Windows. Consulte "Configuraciones admitidas para Cisco Email Reporting Plug-in" en la Matriz de compatibilidad para Cisco Secure Email Encryption Service para garantizar la compatibilidad con su versión de Outlook.

> **Nota:** Las versiones anteriores del plug-in se denominan "IronPort Email Security Plug-in" o "Encryption Plug-in para Outlook". Esta versión del complemento contenía tanto Reporting como Encryption juntos. En 2017, Cisco separó los servicios y lanzó dos nuevas versiones del plug-in, "Email Reporting Plugin for Outlook" y "Email Encryption Plugin for Outlook". Estos estaban disponibles con una versión 1.0.0.x.

Envío de correo electrónico directo

Siga las instrucciones para el cliente de correo electrónico proporcionado para adjuntar el correo electrónico como un archivo adjunto codificado con RFC 822 Multipurpose Internet Mail Extension (MIME). Si uno de los ejemplos no refleja su cliente de correo electrónico, consulte directamente la guía del usuario del cliente de correo electrónico o la asistencia del producto, y confirme que el cliente de correo electrónico admite "Reenvío como adjunto".

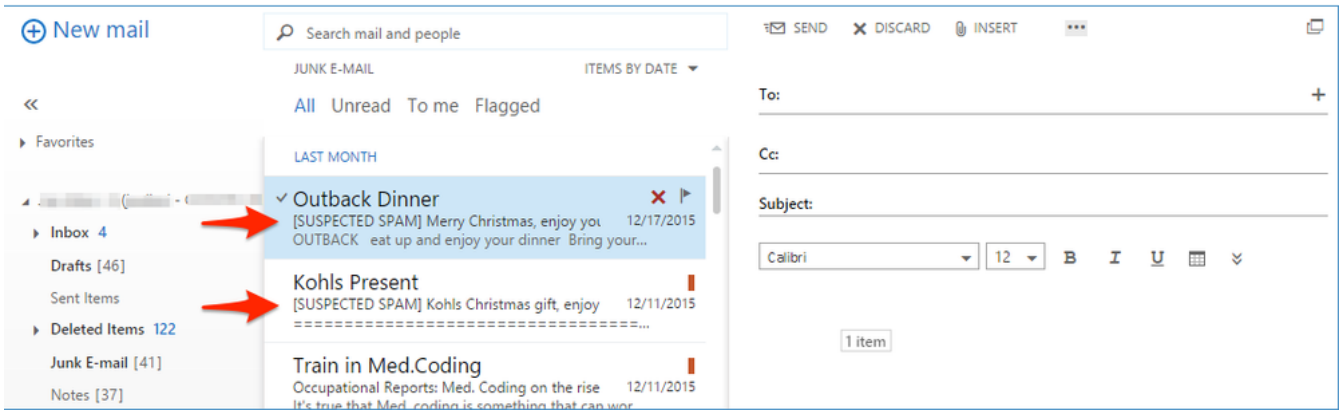
Envíe mensajes de correo electrónico a la dirección de correo electrónico adecuada:

spam@access.ironport.com	El usuario final considera que el mensaje de correo electrónico es spam o que la líne asunto contiene [SOSPECTED SPAM].
ham@access.ironport.com	El usuario final NO considera el mensaje de correo electrónico como spam. La línea asunto contiene [SOSPECTED SPAM] o el asunto incluye etiquetas adicionales.
ads@access.ironport.com	El usuario final considera que el mensaje de correo electrónico es o contiene conteni marketing o graymail, o la línea del asunto incluye [MARKETING], [SOCIAL NETWO [BULK].
not_ads@access.ironport.com	El usuario final NO considera que el mensaje de correo electrónico sea marketing o graymail, o la línea del asunto contiene [MARKETING], [SOCIAL NETWORK] o [BUL
phish@access.ironport.com	El mensaje de correo electrónico parece ser un phishing (diseñado para adquirir nom de usuario, contraseñas, información de tarjeta de crédito u otra información

	personalmente identificable), o el mensaje de correo electrónico contiene archivos adjuntos de malware (asimismo, está diseñado para adquirir nombres de usuario o contraseñas). La línea del asunto se antepone como [SOSPECTED SPAM], [Posible $threat_category Fraud] o similar.
virus@access.ironport.com	El usuario final considera que el mensaje de correo electrónico o un archivo adjunto viral, o que la línea del asunto contiene [ADVERTENCIA: VIRUS DETECTADO].

No todas las líneas de asunto contienen texto y etiquetas adicionales. Para conocer los parámetros, consulte la configuración de Cisco Secure Email Gateway o Cloud Gateway para antispam, antivirus, graymail y filtros de brote de virus, o póngase en contacto con el administrador de correo electrónico si tiene alguna duda.

Ejemplo de líneas de asunto etiquetadas:



Advertencia: No 'Reenviar' el mensaje de correo electrónico como envío. Esta acción no conserva el orden de los encabezados de enrutamiento de correo y elimina los encabezados de enrutamiento de correo necesarios para atribuir la originación del correo electrónico. En su lugar, asegúrese siempre de enviar el mensaje de correo electrónico en cuestión mediante la opción de envío como adjunto.

Puede enviar un correo electrónico directamente desde:

- Microsoft Outlook
- Microsoft Outlook Web App, Microsoft Office 365
- Microsoft Outlook 2011 y Microsoft Outlook 2016 para Mac (OS X, MacOS)
- Correo (OS X, macOS)
- Mozilla Thunderbird
- Plataformas móviles (iPhone, Android u otras)

Microsoft Outlook

- El método de envío preferido de Microsoft Outlook es utilizar el complemento Cisco Secure Email Submission.
- Envíe mensajes a Cisco para correos electrónicos no solicitados y no deseados, como spam, virus y phishing.
- El botón No es spam puede reclasificar rápidamente los mensajes de correo electrónico legítimos marcados como Spam.

Nota: Siga las instrucciones siguientes si no puede instalar Cisco Email Security Plug-In o si no lo prefiere.

Microsoft Outlook Web App, Microsoft Office 365

1. Abra el buzón en Microsoft Outlook Web App.
2. Seleccione el mensaje que desea enviar.
3. Haga clic en "Correo nuevo" en la parte superior izquierda.
4. Arrastre el mensaje y suéltelo como un adjunto al nuevo mensaje.
5. Envíe el mensaje de correo electrónico a la dirección correspondiente proporcionada en este documento.

Microsoft Outlook 2011 y Microsoft Outlook 2016 para Mac (OS X, MacOS)

1. Seleccione el mensaje en el panel de mensajes.
2. Haga clic en el botón Adjunto.
3. Reenvíe el mensaje a la dirección correspondiente proporcionada en este documento.

Correo (OS X, macOS)

1. Haga clic con el botón derecho del ratón en el mensaje de correo electrónico y elija **Reenviar como adjunto**.
2. Reenvíe el mensaje de correo electrónico a la dirección correspondiente proporcionada en este documento.

Mozilla Thunderbird

1. Haga clic con el botón derecho del ratón en el mensaje de correo electrónico y elija **Forward As > Attachment**.
2. Reenvíe el mensaje de correo electrónico a la dirección correspondiente proporcionada en este documento.

Nota: MailSentry IronPort Spam Reporter es un complemento de terceros para Mozilla Thunderbird que realiza la misma acción que se describe pero proporciona un botón "Spam/Ham". **MailSentry IronPort Spam Reporter no es un complemento compatible de Cisco.**

Plataformas móviles (iPhone, Android u otras)

- Si su plataforma móvil no dispone de un método para reenviar el correo electrónico original como adjunto, envíelo una vez que tenga acceso a uno de los otros métodos proporcionados.

Cómo verificar los envíos a Cisco

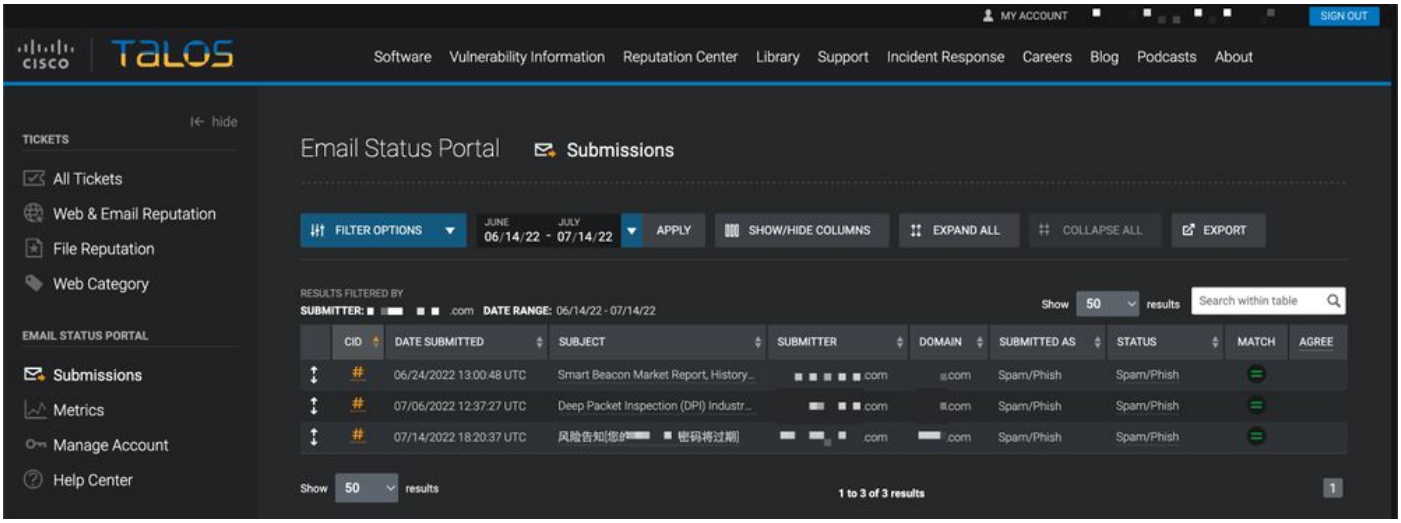
Envío de correo electrónico directo

Cisco no proporciona un correo electrónico de confirmación ni un aviso de recibo para envíos de correo electrónico. En su lugar, consulte los envíos a través del portal de estado de correo electrónico alojado en Talosintelligence.com.

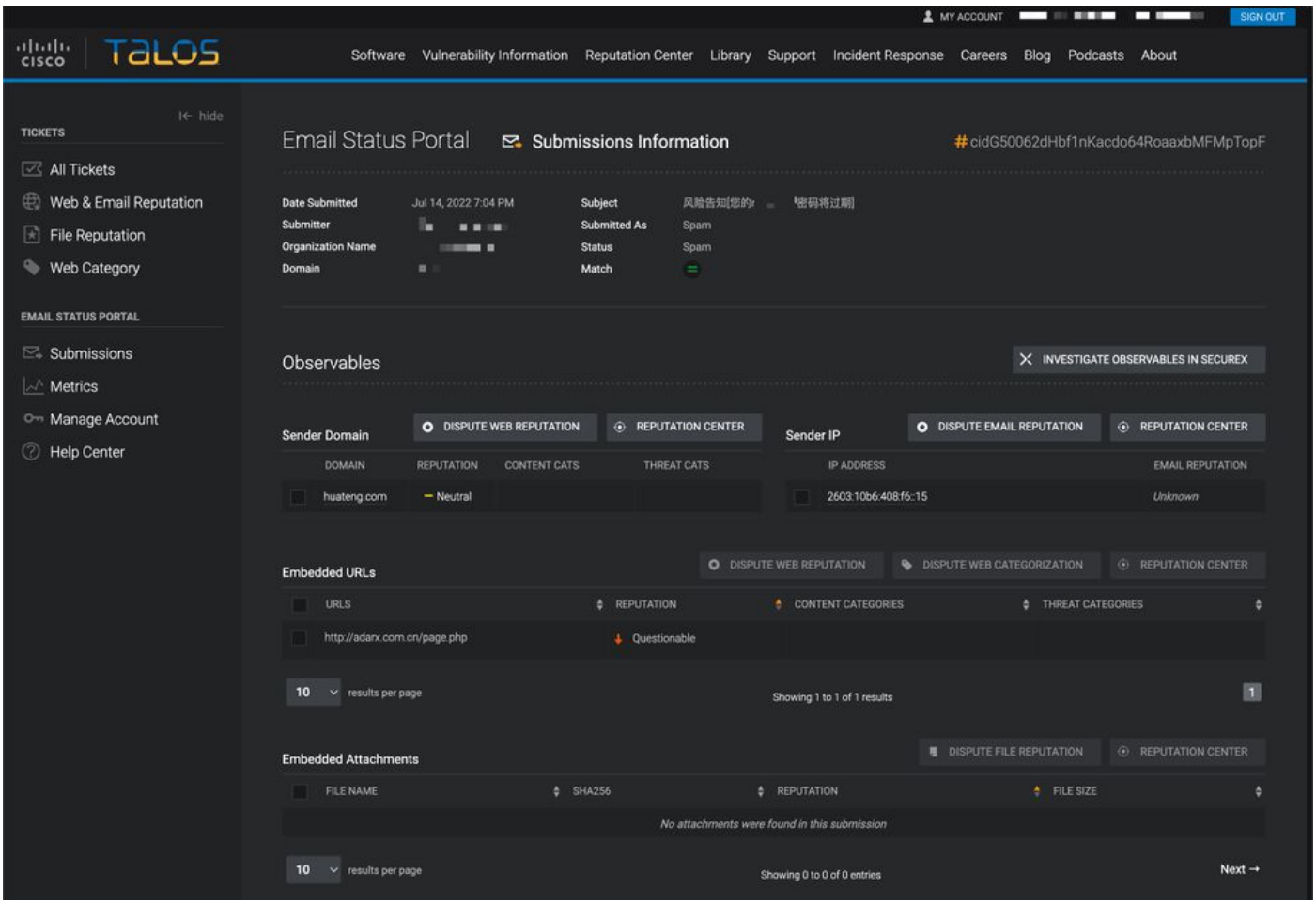
Portal de estado de correo electrónico

Valide los envíos desde el portal de estado de correo electrónico. Después de iniciar sesión, se le proporcionará una lista de todos los envíos dentro del intervalo de fecha y hora especificado.

Ejemplo:



Si hace clic en el CID exclusivo "#", podrá ver más detalles asociados con el correo electrónico notificado.



Se le presenta con Dominio de remitente, IP de remitente, URL incrustadas y adjuntos incrustados asociados al correo electrónico informado. Puede tomar más medidas con **Reputación en la Web**, **Reputación por Correo Electrónico de Disputas** y **Reputación de Archivos de Disputas**.

Cada fila de información anidada muestra un máximo de 5 observables de URL incrustadas y adjuntos incrustados. Si un envío de correo electrónico tiene más elementos observables, un usuario puede hacer clic en 'Ir a la página de detalles de envío de correo electrónico' para ver la lista completa de los elementos observables extraídos.

Puede buscar más detalles de reputación de un único observable con el observable deseado y, a continuación, hacer clic en el botón 'Centro de reputación'.

También puede investigar varios observables a través de SecureX. Este panel combina los datos

de reputación del conjunto completo de productos Cisco Secure basados en su cartera de productos de Cisco. Puede seleccionar hasta 20 observables de un único envío para investigar en SecureX a la vez con el botón 'Investigar observables en SecureX'.

Los usuarios pueden presentar una única disputa de reputación (web, correo electrónico o archivo) o aplicar disputas de forma masiva para uno o varios de los casos observables en un envío. Las URL y los dominios también pueden tener disputas de categorización web archivadas en su contra.

Para obtener más información sobre el portal de estado del correo electrónico: https://talosintelligence.com/tickets/email_submissions/help

Additional Information

Documentación de Cisco Secure Email Gateway

- Release Notes
- Guía del usuario
- Guía de referencia de CLI
- Guías de programación de API para Cisco Secure Email Gateway
- Código abierto utilizado en Cisco Secure Email Gateway
- Guía de Instalación de Cisco Content Security Virtual Appliance (incluye Virtual Cloud Gateway)

Documentación de Secure Email Cloud Gateway

- Release Notes
- Guía del usuario

Documentación de Cisco Secure Email y Web Manager

- Notas de la versión y matriz de compatibilidad
- Guía del usuario
- Guías de programación de API para Cisco Secure Email and Web Manager
- Guía de Instalación de Cisco Content Security Virtual Appliance (incluye Virtual Email and Web Manager)

Documentación de productos Cisco Secure

- Arquitectura de denominación de la cartera de Cisco Secure