El spam se introduce en la organización mediante el dispositivo de seguridad Cisco Email Security Appliance (ESA)

Contenido

Introducción

Este documento describe cinco métodos para que los correos electrónicos de spam puedan entrar en su organización.

Métodos

1. Mensaje legítimo/Correo de marketing

El usuario ha optado por el mensaje legítimo o su nombre se ha vendido a otra organización. En el primer caso, el usuario deberá tomar medidas para anular la suscripción a la lista. Si es la última, envíe el mensaje de nuevo a spam@access.ironport.com para que las definiciones de antispam puedan actualizarse globalmente, mejorando así el índice general de captura de spam de su ESA. La habilitación del correo de marketing en la política de correo entrante puede ayudar a cambiar la percepción de que este mensaje es "marketing" sobre "spam".

2. El Anti-Spam No Se Está Actualizando Correctamente

Anti-Spam está desactivado o la clave de característica ha caducado. Para comprobar y ver si Anti-Spam se está actualizando, vaya a **GUI > Servicios de seguridad > IronPort Anti-Spam**. En este panel, debería ver las actualizaciones de los conjuntos de reglas o del motor en las últimas 6 horas. También desde esta pestaña en la parte superior puede asegurarse de que el servicio Anti-Spam esté habilitado. Para revisar el estado de la clave de característica, puede ir a la ficha Administración del sistema > Clave de característica para comprobar el estado de la clave antispam.

3. Política de correo o filtro de mensajes

El spam puede entrar en su organización si el motor de seguridad Anti-Spam está desactivado para un remitente o destinatario específico por una política de correo del cliente. Otra forma de omitir el filtrado de spam es a través de los filtros de mensajes (CLI: **filtros**).

4. Política de flujo de correo

Un mensaje se clasifica utilizando el ICID del mensaje. En esta situación, es probable que la función Anti-Spam Security esté desactivada, lo que invalida la política de correo. Para determinar esto, consulte los registros de correo, en los registros primero tendrá que revisar el ICID para comprender en qué SenderGroup se clasificó el mensaje. A partir de ahí, revise la política de flujo de correo asociada. Si tiene una gran cantidad de entradas en AllowList, es posible que deba revisar algunos de los mensajes que se reciben para ver si fueron escaneados por el motor AntiSpam. Abra los encabezados de un mensaje y busque el encabezado X-IronPort-Spam, la presencia de este encabezado significa que el mensaje pasó a través del motor.

5. El mensaje es spam

El mensaje es spam real. Ha confirmado que el motor antispam ha analizado el mensaje mediante la función Rastreo de mensajes (en el seguimiento de mensajes, busque "CASE"). Si el veredicto del caso es negativo y considera que el mensaje es spam, envíe el mensaje original a spam@access.ironport.com. Este podría ser el caso de una nueva amenaza de spam que acaba de ser liberada o una amenaza antigua que fue rediseñada.

El procesamiento de los envíos de spam es un proceso automático y manual, y no hay comentarios para el envío específico. En cualquier momento, puede ponerse en contacto con el TAC de Cisco y solicitar una evaluación y una respuesta.