Resuelva problemas el " del error; Categoría = mensaje de error de Unscannable, razón de Unscannable = error del archivo: Excedió el límite del tamaño total del files" unarchived; en un ESA

Contenido

Introducción

Este documento describe cómo resolver problemas categoría = mensaje de error de Unscannable del error “, razón de Unscannable = error del archivo: Excedió el límite del tamaño total de los archivos unarchived” en un dispositivo de seguridad del correo electrónico (ESA).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- ESA
- Cisco avanzó la protección de Malware (el AMP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ESA AsyncOS 11.1.2-023.
- ESA AsyncOS 12.0.0-419.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

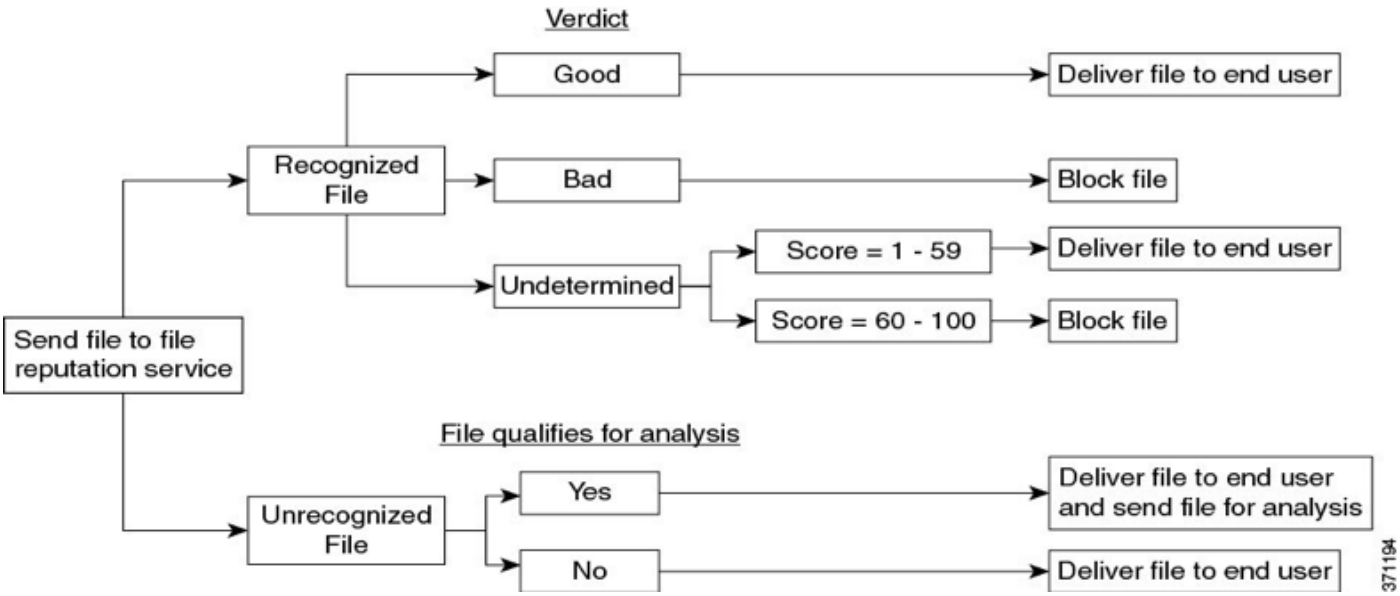
Antecedentes

Cuando un mensaje con una conexión alcanza el AMP en la tubería, el ESA intenta analizar la conexión del mensaje y marca los encabezados del mensaje (comprobación para la conformidad con el RFC 2045). Incluso si el mensaje no es completamente obediente, el ESA todavía hace mejor esfuerzo para analizar la conexión.

El siguiente paso es marcar si una conexión es un archivo y si es así ESA intenta desempaquetarlo, considera los factores múltiples para determinar los tamaños del archivo comprimido para asegurarse que la conexión es legit y no a archivo zip.

Cuando una reputación del archivo no se encuentra, y el archivo cumple los criterios para el análisis que quarantined y que está cargado a la salvadera.

Entonces, el ESA abre una conexión a los servidores AMP y carga el archivo y las esperas para las actualizaciones del veredicto, tal y como se muestra en de la imagen:



El ESA proporciona un veredicto basado en estos escenarios:

- Si uno de los archivos extraídos es malévolo, el servicio de la reputación del archivo vuelve un veredicto de malévolo para el comprimido o el archivo.
- Si el comprimido o el archivo es malévolo y todos los archivos extraídos son limpios, el servicio de la reputación del archivo vuelve un veredicto de malévolo para el comprimido o el archivo.
- Si el veredicto de los archivos extraídos uces de los es desconocido, los archivos extraídos (si está configurado y soportan al tipo de archivo para el análisis del archivo) se envían opcionalmente para el análisis del archivo.
- Si el veredicto de los archivos extraídos o de las conexiones uces de los es poco arriesgado, el archivo no se envía para el análisis del archivo.
- Si la extracción de un archivo la falla cuando consigue descomprimida y entonces es

comprimida o un archivo, el servicio de la reputación del archivo vuelve un veredicto de Unscannable para el comprimido o el archivo. Tenga en cuenta que, en este escenario, si uno de los archivos extraídos es malévolo, el servicio de la reputación del archivo vuelve un veredicto de malévolo para el comprimido o el archivo (el veredicto malévolo toma la precedencia sobre el veredicto de Unscannable).

Altamente los archivos comprimidos como el csv, xml, txt pueden exceder los tamaños del archivo máximos puestos en hard-code en el ESA, los algoritmos de compresión, como Lempel-Ziv, generan una correspondencia digital que cuente el número y la posición de los caracteres dentro del documento entero y ésta produce los tamaños del archivo muy pequeños.

Por otra parte, los archivos que contienen los gráficos, formato de texto como el pdf, jpg, png, no se comprimen la misma manera, así que casi guardan los tamaños del archivo original.

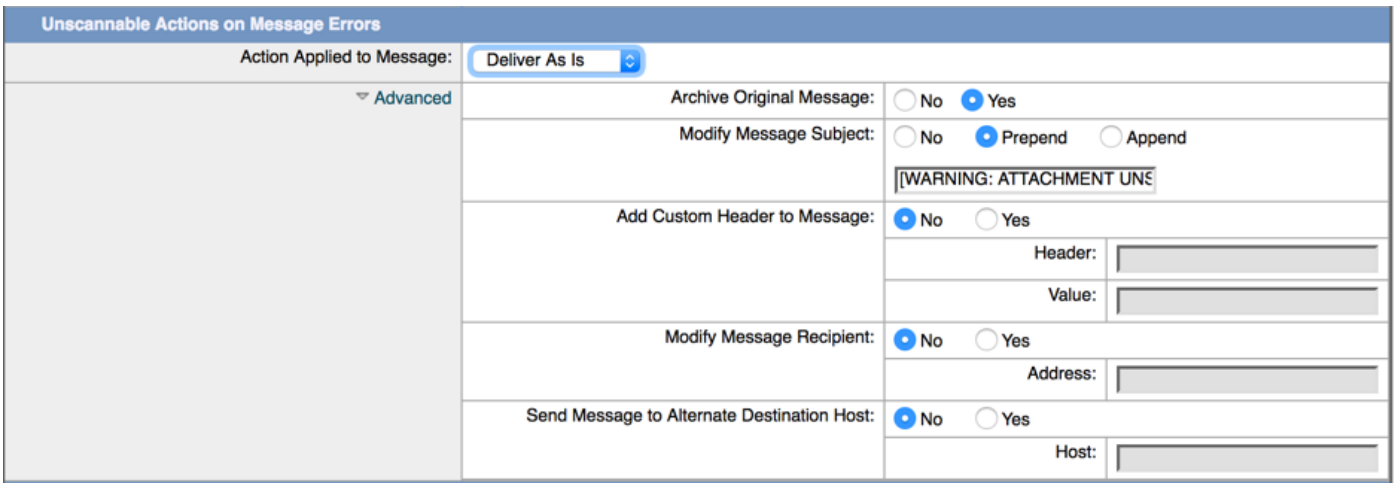
Problema

Cuando el ESA recibe un correo electrónico dentro de una conexión que sea comprimida y ésta excede la relación de transformación de compresión máxima y el ESA no puede calcular los tamaños del archivo de la conexión entonces que la consecuencia es este registro de error:

“Información 2019 del miércoles 13 de febrero 20:03:47: La conexión no podía ser analizada. El nombre del archivo = los “ACTOS tajó ISO 88591 encod_NoSchema.XML.zip”, MEDIADOS DE = 226, SHA256 =7efa6154b7519872055cff10a69067dcad88562f708b284a390a9abcf5e99b8f, categoría de Unscannable = mensaje de error, razón de Unscannable = error del archivo: Excedió el límite del tamaño total de los archivos unarchived”

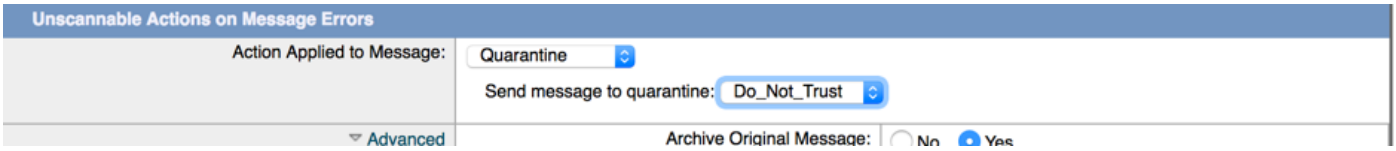
Solución 1

Prepend los mensajes unscannable en conforme a los usuarios alertas que el archivo no era analizado por los servicios AMP, tal y como se muestra en de la imagen.



Solución 2

Quarantine unscannable en las cuarentenas del virus y del brote de la directiva (PVO) para el análisis adicional. tal y como se muestra en de la imagen.



Información Relacionada

- Guía del usuario para AsyncOS 12.0 para los dispositivos de seguridad del correo electrónico de Cisco - GD (General Deployment)
- Permiso AMP en los productos de seguridad contentos (ESA/WSA)
- Verifique las cargas del análisis del archivo en el ESA
- Soporte Técnico y Documentación - Cisco Systems