Dépanner l'erreur « Unscannable Category = Message Error, Unscannable Reason = Archive Error : Exceeded the total size limit of unarchived files » dans un ESA

Contenu

Introduction

Ce document décrit comment dépanner l'erreur "Unscannable Category = Message Error, Unscannable Reason = Archive Error:Exceeded the total size limit of the unarchived files" dans un dispositif de sécurité de la messagerie (ESA).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ESA
- Cisco Advanced Malware Protection (AMP)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

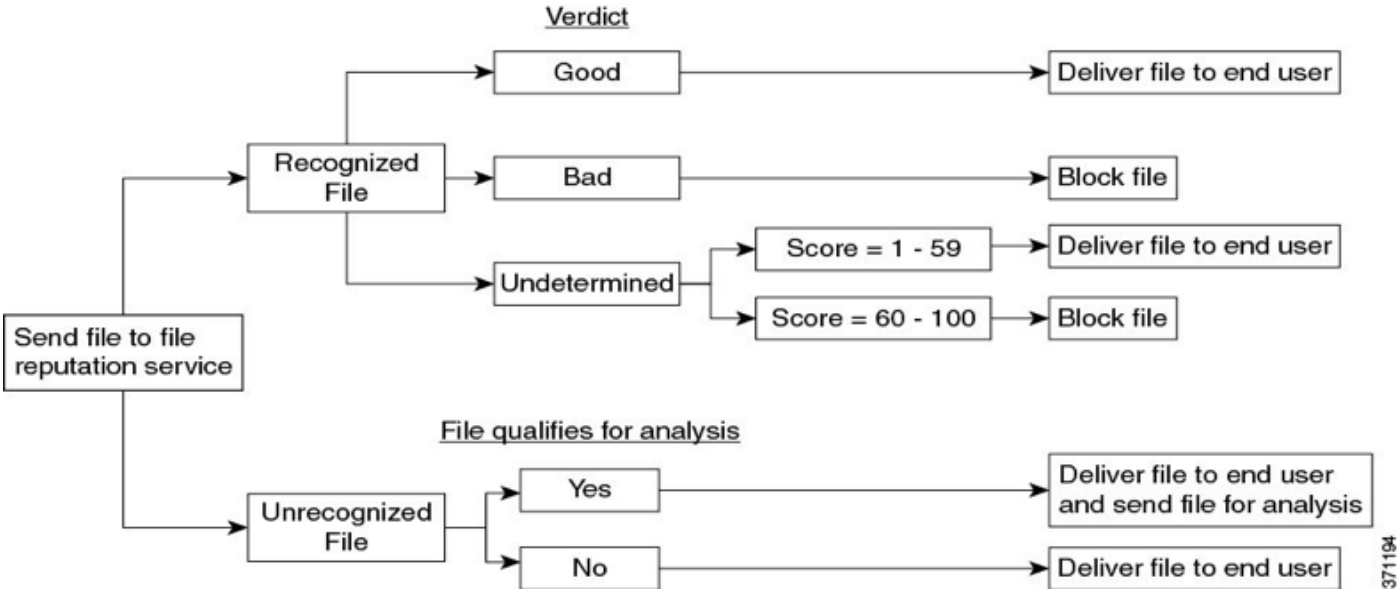
Informations générales

Lorsqu'un message avec une pièce jointe atteint AMP dans le pipeline, ESA tente d'analyser la pièce jointe à partir du message et vérifie les en-têtes de message (vérifier la conformité avec la RFC 2045). Même si le message n'est pas entièrement conforme, ESA fait de son mieux pour analyser la pièce jointe.

L'étape suivante consiste à vérifier si une pièce jointe est un fichier d'archive et, si tel est le cas, ESA tente de le décompresser. Elle prend en compte plusieurs facteurs afin de déterminer la taille du fichier compressé afin de s'assurer que la pièce jointe est légitime et non un fichier zip.

Lorsqu'une réputation de fichier est introuvable et que le fichier répond aux critères d'analyse, il est mis en quarantaine et chargé dans le sandbox.

Ensuite, ESA ouvre une connexion aux serveurs AMP et télécharge le fichier et attend les mises à jour des verdicts, comme le montre l'image :



ESA fournit un verdict basé sur ces scénarios :

- Si l'un des fichiers extraits est malveillant, le service de réputation des fichiers renvoie le verdict Malveillant pour le fichier compressé ou le fichier d'archive.
- Si le fichier compressé ou le fichier d'archive est malveillant et que tous les fichiers extraits sont sains, le service de réputation des fichiers renvoie le verdict Malveillant pour le fichier compressé ou le fichier d'archive.
- Si le verdict de l'un des fichiers extraits est inconnu, les fichiers extraits sont éventuellement (s'ils sont configurés et si le type de fichier est pris en charge pour l'analyse de fichier) envoyés pour l'analyse de fichier.
- Si le verdict de l'un des fichiers extraits ou des pièces jointes est faible, le fichier n'est pas envoyé pour analyse.
- Si l'extraction d'un fichier échoue lorsqu'il est décompressé et qu'il est compressé ou qu'il s'agit d'un fichier d'archive, le service de réputation de fichiers renvoie le verdict Unscannable pour le fichier compressé ou le fichier d'archive. Gardez à l'esprit que, dans ce scénario, si l'un des fichiers extraits est malveillant, le service de réputation des fichiers renvoie un verdict

Malveillant pour le fichier compressé ou le fichier d'archive (le verdict Malveillant a priorité sur le verdict Inanalysable).

Les fichiers fortement compressés comme csv, xml, txt peuvent dépasser la taille maximale de fichier codé en dur dans ESA, les algorithmes de compression, comme Lempel-Ziv, génère une carte numérique qui compte le nombre et la position des caractères dans le document complet et cela produit de très petites tailles de fichiers.

D'autre part, les fichiers qui contiennent des graphiques, format de texte comme pdf, jpg, png, ils ne sont pas compressés de la même manière, de sorte qu'ils conservent presque la taille du fichier d'origine.

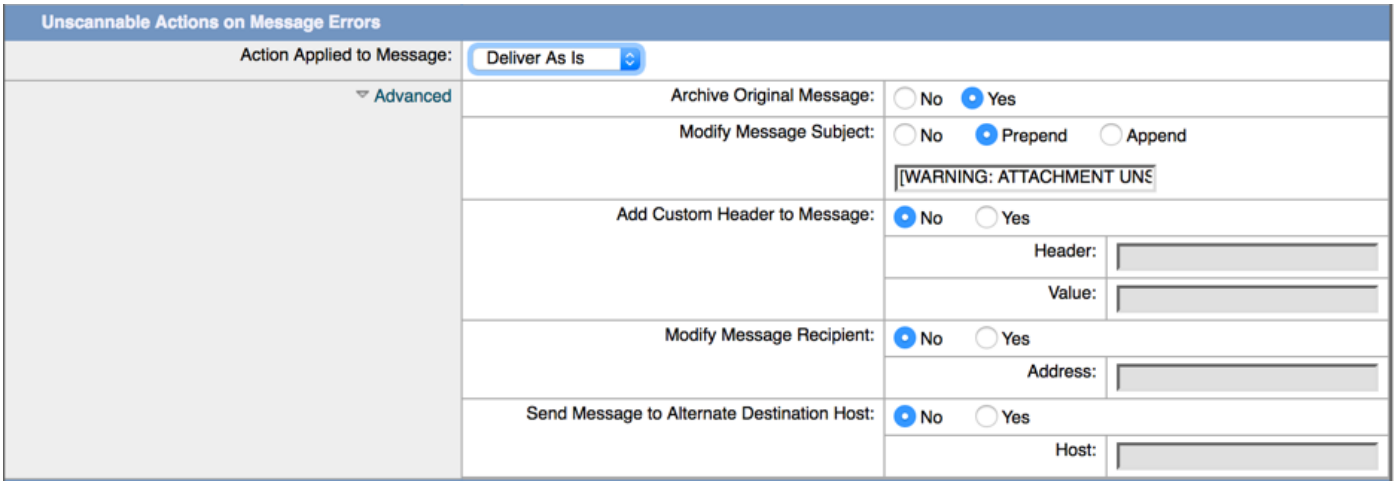
Problème

Lorsque l'ESA reçoit un e-mail dans une pièce jointe compressée, ce qui dépasse le taux de compression maximal et que l'ESA ne parvient pas à calculer la taille de fichier de la pièce jointe, la conséquence est le journal des erreurs suivant :

"Mer Feb 13 20:03:47 2019 Info : Impossible d'analyser la pièce jointe. Nom du fichier = 'ACTS Chopped ISO 88591 encod_NoSchema.XML.zip', MID = 226, SHA256 =7efa6154b7519872055cff10a69067dcad88562f708b284a390a9abcf5e99b8f, Catégorie non analysable = Erreur de message, Motif non analysable = Erreur d'archivage : Dépassement de la limite de taille totale des fichiers non archivés

Solution 1

Ajoutez les messages non analysables à l'objet pour avertir les utilisateurs que le fichier n'a pas été analysé par les services AMP, comme illustré dans l'image.



Solution 2

Quarantaine non analysable dans les quarantaines des virus et des attaques de stratégie (PVO) pour analyse ultérieure. comme illustré dans l'image.

Informations connexes

- Guide de l'utilisateur d'AsyncOS 12.0 pour les appareils de sécurité de la messagerie Cisco - GD (General Deployment)
- Activer AMP sur les produits de sécurité du contenu (ESA/WSA)
- Vérification des chargements d'analyse de fichier sur ESA
- Support et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.