Risoluzione dei problemi relativi all'errore "Unscannable Category = Message Error, Unscannable Reason = Archive Error:Exceeded the total size limit of the unarchived files" in un ESA

Sommario

Introduzione

In questo documento viene descritto come risolvere il problema relativo all'errore "Unscannable Category = Message Error, Unscannable Reason = Archive Error:Exceeded the total size limit of the unarchived files" in un Email Security Appliance (ESA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ESA
- Cisco Advanced Malware Protection

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

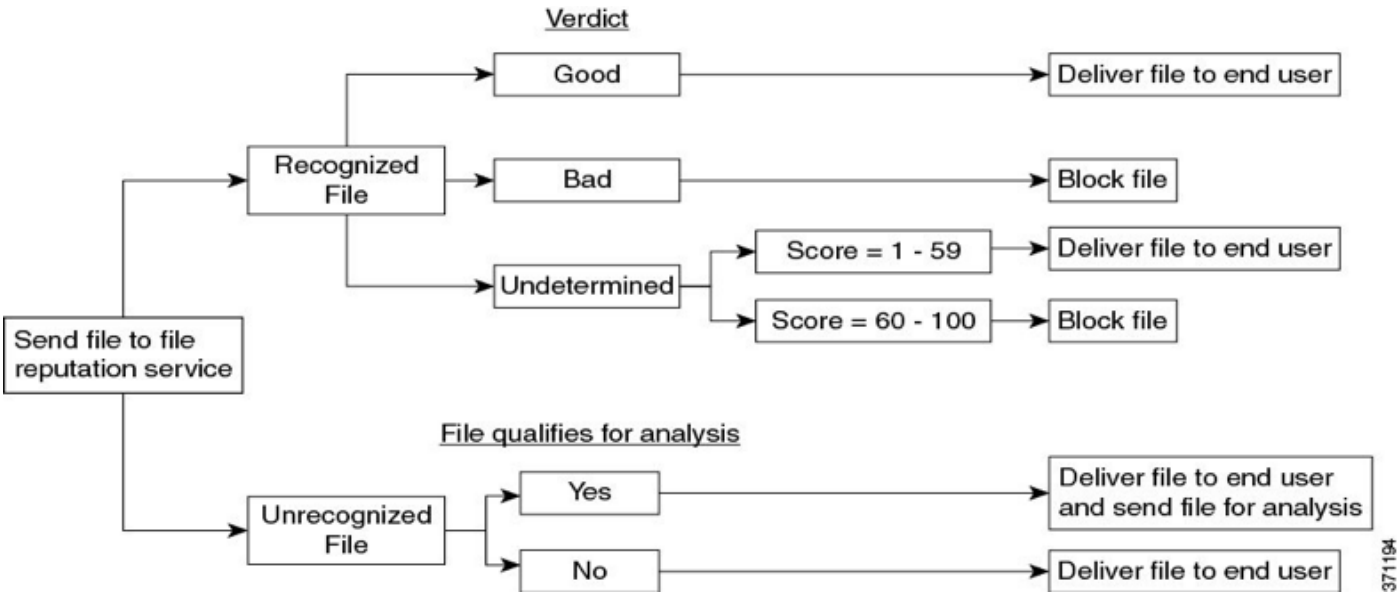
Premesse

Quando un messaggio con un allegato raggiunge AMP nella pipeline, ESA tenta di analizzare l'allegato dal messaggio e controlla le intestazioni del messaggio (verificare la conformità con RFC 2045). Anche se il messaggio non è pienamente conforme, l'ESA fa comunque del suo meglio per analizzare l'allegato.

Il passaggio successivo consiste nel verificare se un allegato è un file di archivio e, in caso affermativo, ESA tenta di decomprimerlo, prende in considerazione più fattori per determinare le dimensioni del file compresso in modo da garantire che l'allegato sia legittimo e non un file zip.

Quando non viene trovata la reputazione di un file e il file soddisfa i criteri per l'analisi, viene messo in quarantena e caricato nella sandbox.

L'ESA apre quindi una connessione ai server AMP e carica il file in attesa di aggiornamenti del verdetto, come mostrato nell'immagine:



L'ESA emette un verdetto basato su questi scenari:

- Se uno dei file estratti è dannoso, il servizio di reputazione dei file restituisce un verdetto di dannoso per il file compresso o l'archivio.
- Se il file compresso o di archivio è dannoso e tutti i file estratti sono puliti, il servizio di reputazione dei file restituisce un verdetto di dannoso per il file compresso o di archivio.
- Se il verdetto di uno dei file estratti è sconosciuto, i file estratti vengono facoltativamente inviati per l'analisi dei file (se configurati e il tipo di file è supportato per l'analisi dei file).
- Se il verdetto di uno qualsiasi dei file o degli allegati estratti è a basso rischio, il file non viene inviato per l'analisi del file.
- Se l'estrazione di un file ha esito negativo quando viene decompresso e quindi compresso o un file di archivio, il servizio di reputazione dei file restituisce un verdetto di Non scansionabile per il file compresso o di archivio. Tenere presente che, in questo scenario, se uno dei file

estratti è dannoso, il servizio di reputazione dei file restituisce un verdetto di Dannoso per il file compresso o archiviato (il verdetto dannoso ha la precedenza sul verdetto non scansionabile).

File altamente compressi come csv, xml, txt possono superare le dimensioni massime dei file hardcoded in ESA, algoritmi di compressione, come Lempel-Ziv, generano una mappa digitale che conta il numero e la posizione dei caratteri all'interno del documento completo e questo produce dimensioni di file molto piccole.

D'altra parte, i file che contengono grafica, formato testo come pdf, jpg, png, non vengono compressi allo stesso modo, quindi mantengono quasi le dimensioni originali del file.

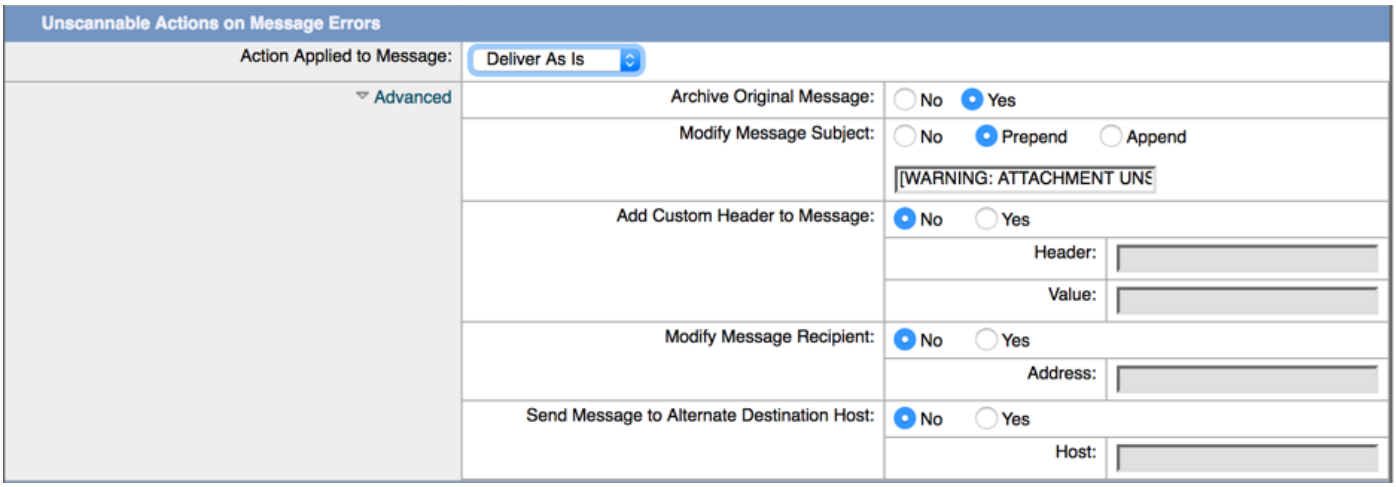
Problema

Quando l'ESA riceve un messaggio e-mail all'interno di un allegato compresso che supera il rapporto di compressione massimo e non riesce a calcolare le dimensioni del file dell'allegato, la conseguenza è il seguente log degli errori:

"Mer Feb 13 20:03:47 2019 Info: Impossibile analizzare l'allegato. Nome file = 'ACTS Chopped ISO 88591 encod_NoSchema.XML.zip', MID = 226, SHA256 =7efa6154b7519872055cff10a69067dcad88562f708b284a390a9abcf5e99b8f, Unscannable Errore messaggio, motivo non analizzabile = Errore archivio: Superate le dimensioni totali dei file non archiviati"

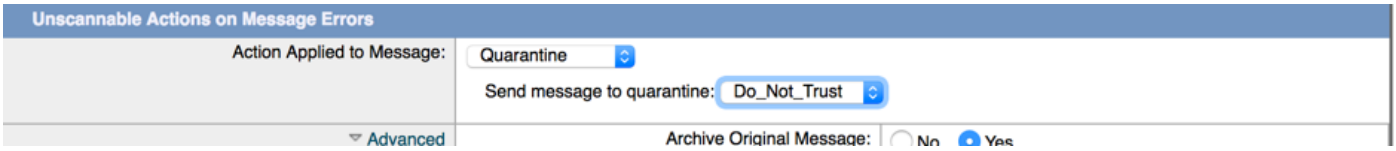
Soluzione 1

Anteporre messaggi non scansionabili in Oggetto per avvisare gli utenti che il file non è stato analizzato dai servizi AMP, come mostrato nell'immagine.



Soluzione 2

Quarantena non scansionabile nelle quarantene per virus ed epidemie di policy (PVO) per ulteriori analisi. come mostrato nell'immagine.



Informazioni correlate

- Guida per l'utente di AsyncOS 12.0 per Cisco Email Security Appliance - GD (General Deployment)
- Abilitazione di AMP sui prodotti per la sicurezza dei contenuti (ESA/WSA)
- Verifica del caricamento dell'analisi dei file sull'ESA
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).