Probleemoplossing voor de fout "Niet-scanbare categorie = Berichtfout, niet-scanbare reden = Archieffout:Overschrijd de totale grootte van de niet-gearchiveerde bestanden" in een ESA

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen bij de fout "Niet-scanbare categorie = Berichtfout, Niet-scanbare reden = Archieffout:Overschrijd de totale grootte van de niet-gearchiveerde bestanden" in een E-mail security applicatie (ESA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ESA
- Cisco Advanced Malware Protection

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

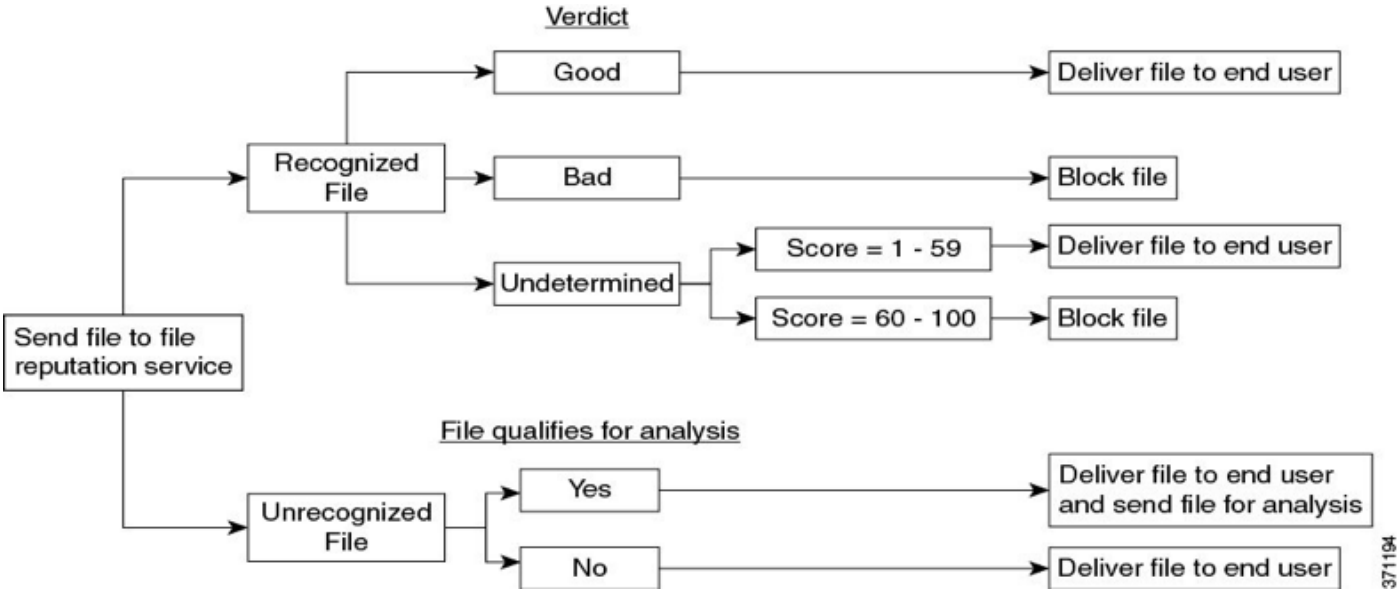
Achtergrondinformatie

Wanneer een bericht met een bijlage AMP in de pijpleiding bereikt, probeert ESA de bijlage uit het bericht te parsen en controleert het de berichtkopregels (controle op naleving van RFC 2045). Zelfs indien het bericht niet volledig conform is, doet de ESA nog steeds haar best om de bijlage te ontleden.

De volgende stap is te controleren of een bijlage een archiefbestand is en als dat zo is, ESA probeert het uit te pakken, het overweegt meerdere factoren om gecomprimeerde bestandsgrootte te bepalen om er zeker van te zijn dat de bijlage legaal is en niet een zip-bestand.

Wanneer een bestand reputatie niet wordt gevonden en het bestand voldoet aan de criteria voor analyse wordt het in quarantaine geplaatst en geüpload naar de zandbak.

ESA opent vervolgens een verbinding met AMP-servers en uploadt het bestand en wacht op verdict-updates, zoals te zien is in de afbeelding:



Het ESR geeft een oordeel op basis van deze scenario's:

- Als een van de geëxtraheerde bestanden kwaadaardig is, retourneert de service voor bestandreputatie een oordeel van Malicious voor het gecomprimeerde of archiefbestand.
- Als het gecomprimeerde of archiefbestand kwaadaardig is en alle geëxtraheerde bestanden schoon zijn, geeft de service voor bestandsherkenning een oordeel van kwaadaardig voor het gecomprimeerde of archiefbestand.
- Als het oordeel van een van de geëxtraheerde bestanden onbekend is, worden de geëxtraheerde bestanden optioneel verzonden (indien geconfigureerd en het bestandstype wordt ondersteund voor bestandsanalyse) voor bestandsanalyse.
- Als de uitspraak van een van de geëxtraheerde bestanden of bijlagen een laag risico is, wordt het bestand niet verzonden voor bestandsanalyse.
- Als de extractie van een bestand mislukt wanneer het gedecompresseerd wordt en dan wordt het gecomprimeerd of een archiefbestand, de bestandsreputatieservice retourneert een uitspraak van Unscannable voor het gecomprimeerde of archiefbestand. Houd in gedachten dat, in dit scenario, als een van de geëxtraheerde bestanden kwaadaardig is, de service van

de bestandsnavigatie een oordeel van kwaadwillig voor het gecomprimeerde of het archiefbestand (kwaadwillig vonnis heeft voorrang op onscannbaar vonnis).

Sterk gecomprimeerde bestanden zoals csv, xml, txt kunnen de maximale bestandsgrootte overschrijden hardcoded in ESA, compressie algoritmen, zoals Lempel-Ziv, genereert een digitale kaart die het aantal en de positie van tekens binnen het volledige document telt en dit geeft zeer kleine bestandsgrootte.

Aan de andere kant, bestanden die afbeeldingen bevatten, tekstformaten zoals pdf, jpg, png, ze zijn niet op dezelfde manier gecomprimeerd, dus ze houden bijna de oorspronkelijke bestandsgrootte.

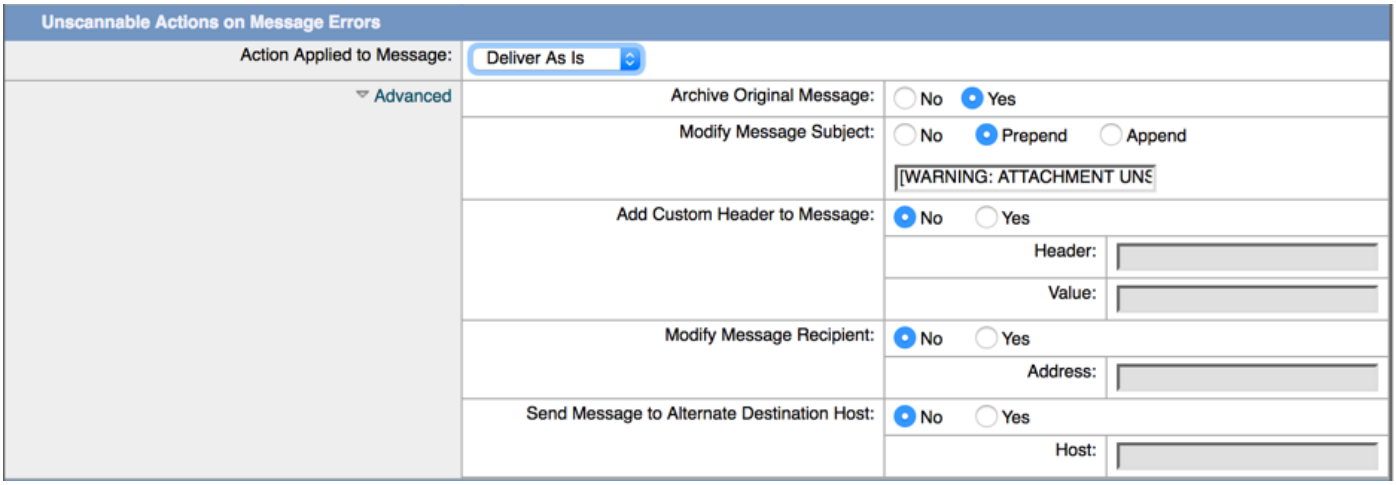
Probleem

Wanneer de ESE binnen een bijlage een e-mail ontvangt die is gecomprimeerd en de maximale compressieverhouding overschrijdt en de ESE de bestandsgrootte van de bijlage niet kan berekenen, is het gevolg dit foutenlogboek:

"Wed Feb 13 20:03:47 2019 Info: De bijlage kan niet worden gescand. Bestandsnaam = 'ACT Chopped ISO 88591 encod_NoSchema.XML.zip', MID = 226, SHA256 =7efa6154b7519872055cff10a69067dcad88562f708b284a390a9abcf5e99b8f, Niet-scanbare categorie = Berichtfout, niet-scannerbare reden = Archieffout: Overschrijdt de maximale grootte van niet-gearchiveerde bestanden"

Oplossing 1

Niet-scanbare berichten toevoegen aan Onderworpen aan gebruikers die erop attent zijn dat het bestand niet door AMP-diensten is geanalyseerd, zoals in de afbeelding wordt getoond.



Oplossing 2

Quarantaine niet te scannen in Policy Virus & Outbreak (PVO) quarantaine voor verdere analyse. zoals in de afbeelding.

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 12.0 voor Cisco e-mail security applicaties - GD (algemene implementatie)
- Advanced Malware Protection inschakelen voor Content Security Producten (ESA/WSA)
- Controleer de uploadstatus van de bestandsanalyse op ESA
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.