

Probleemoplossing bij fout-positieve bestandsanalyse in Advanced Malware Protection voor endpoints

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Probleemoplossing bij fout-positieve bestandsanalyse in Advanced Malware Protection voor endpoints](#)

[Bestand SHA 256 Hash](#)

[Kopie bestand voorbeeld](#)

[Alert Event Capture van AMP-console](#)

[Event Details Capture of AMP-console](#)

[Informatie over het bestand](#)

[verklaring](#)

[Informatie verstrekken](#)

[Conclusie](#)

Inleiding

Dit document beschrijft hoe u een foute positieve bestandsanalyse kunt verzamelen in Advanced Malware Protection (AMP) voor endpoints.

Bijgedragen door Jezus Javier Martinez, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze onderwerpen:

- AMP-console dashboard
- Een account met administratorrechten

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Advanced Malware Protection voor endpoints, versie 6.X.X en hoger.

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 de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

AMP voor endpoints kan buitensporige waarschuwingen genereren op een bepaald bestand/proces/Secure Hash Algorithm (SHA) 256. Als u foutieve positieve detecties in uw netwerk vermoedt, kunt u contact opnemen met het Cisco Technical Assistance Center (TAC) en gaat het diagnostische team verder om een diepere bestandsanalyse uit te voeren. Wanneer u contact opneemt met Cisco TAC, moet u deze informatie verstrekken:

- File SHA 256 shash
- Kopie voor bestandstaal
- Waarschuwingsgebeurtenissen bij opname in AMP-console
- Event Details van AMP-console
- Informatie over het bestand (waar het vandaan komt en waarom het in de omgeving moet zijn)
- Leg uit waarom u gelooft dat het bestand/proces verkeerd-positief kan zijn

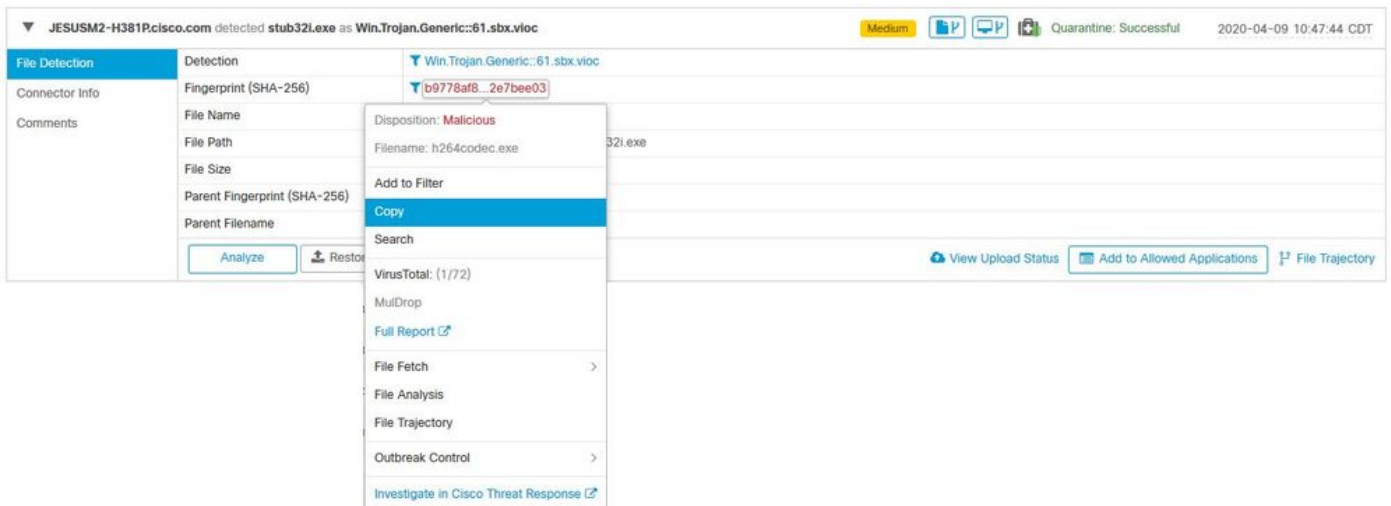
Probleemoplossing fout positieve bestandsanalyse in Advanced Malware Protection voor endpoints

Deze sectie verschaft informatie die u kunt gebruiken om alle informatie te verkrijgen die nodig is om een vals positief ticket met Cisco TAC te openen.

Bestand SHA 256 Hash

Stap 1. Ga voor de SHA 256-hash naar **AMP-console > Dashboard > Events**.

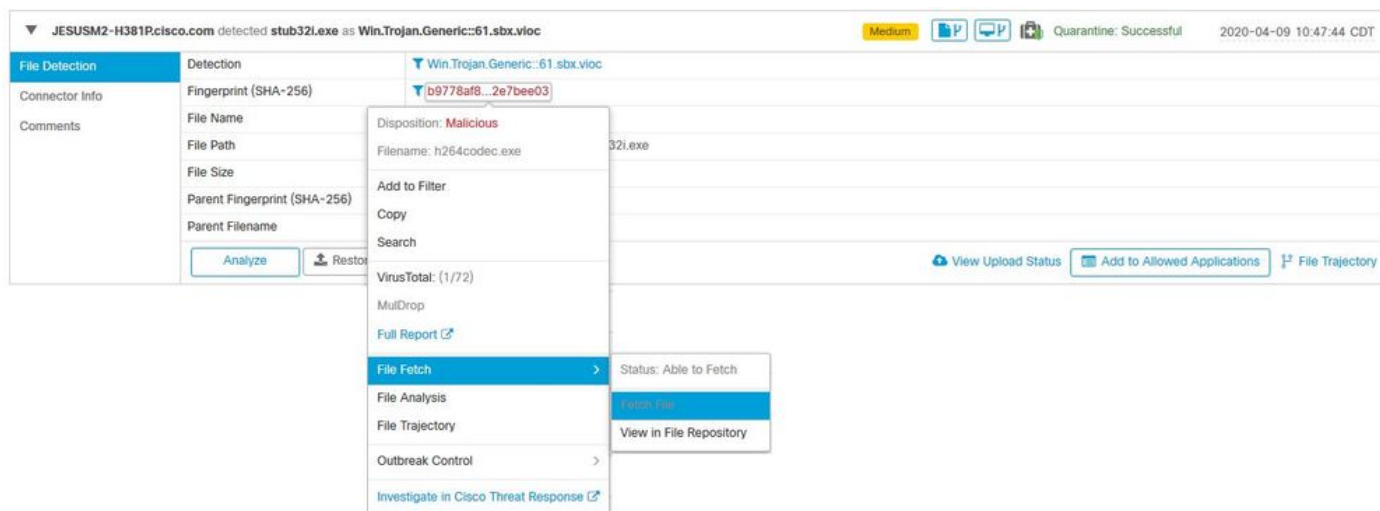
Stap 2. Selecteer de **gebeurtenis** in het **alarmsignaal**, klik op **SHA256** en selecteer **Kopie** zoals in de afbeelding.



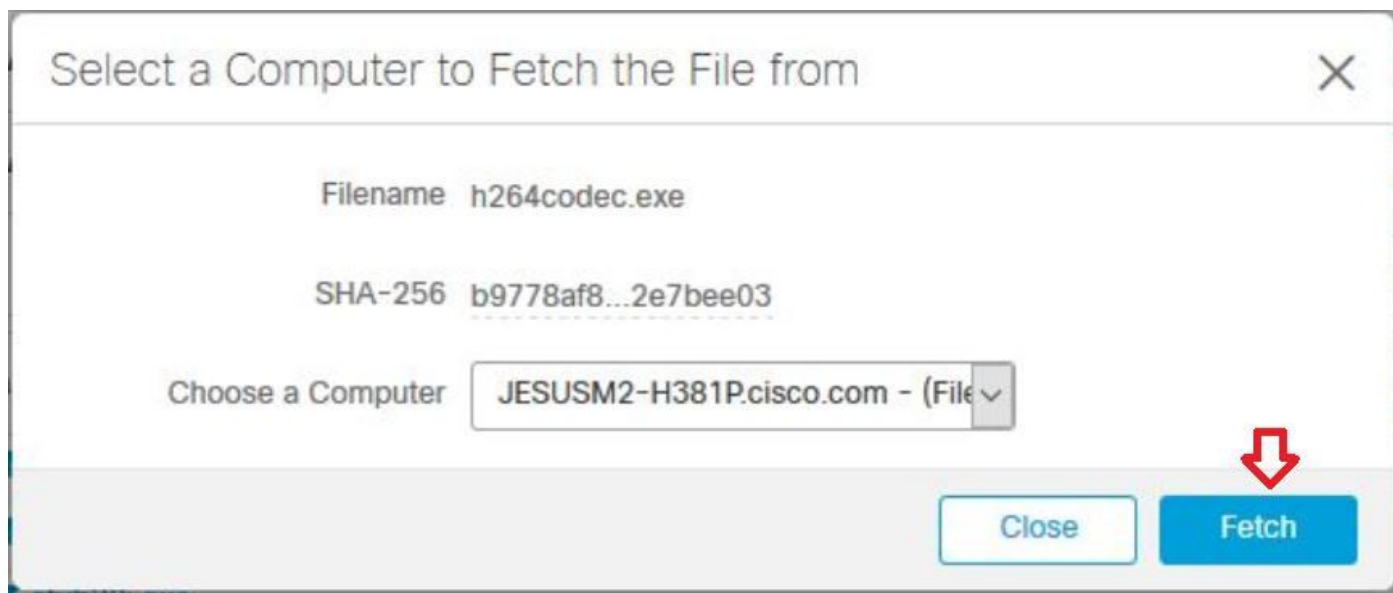
Kopie bestand voorbeeld

Stap 1. U kunt de bestandssteekproef van AMP-console ophalen, navigeer naar **AMP-console > Dashboard > Events**.

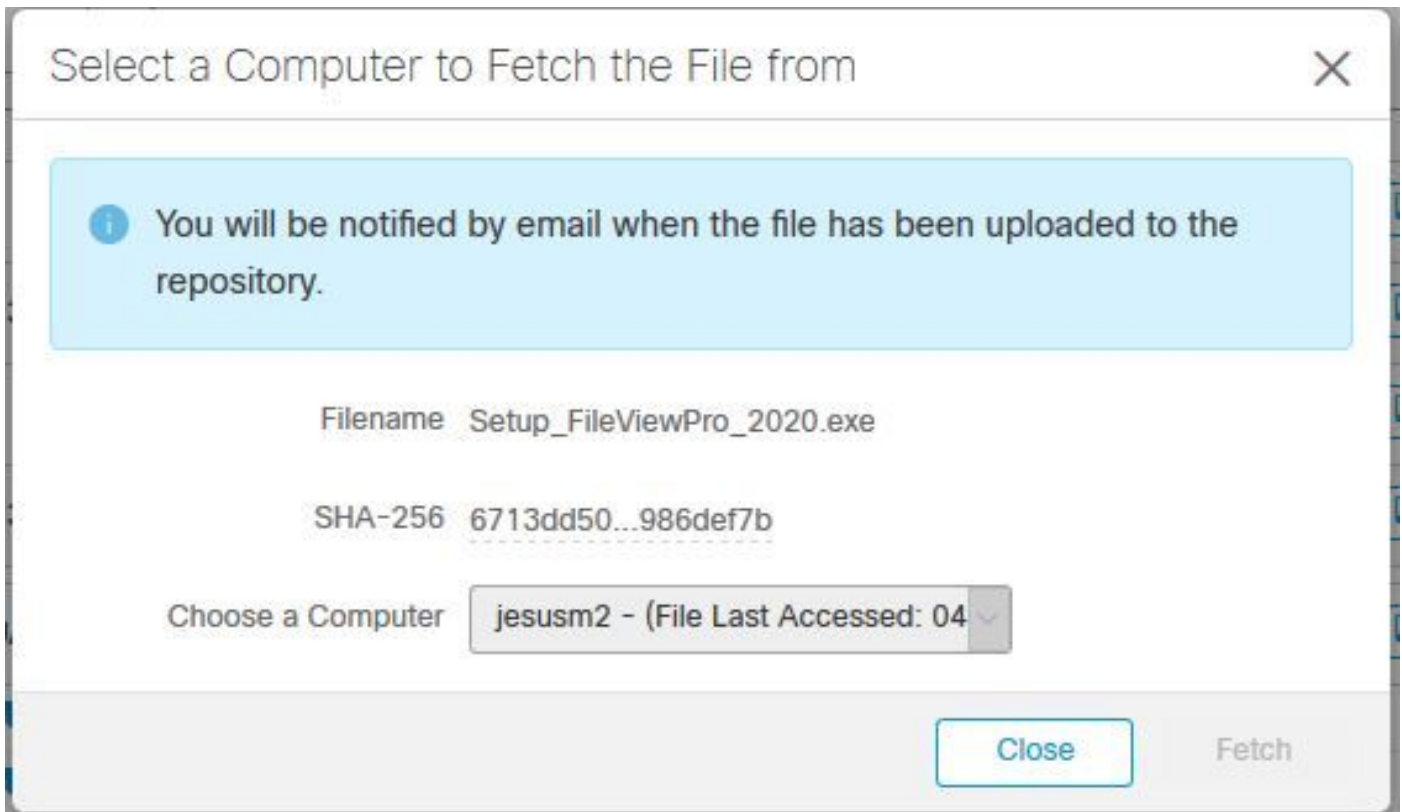
Stap 2. Selecteer de **gebeurtenis** in het **alarmsignaal**, klik op **SHA256** en navigeer naar **bestandsgrootte> bestandsgrootte** zoals in de afbeelding.



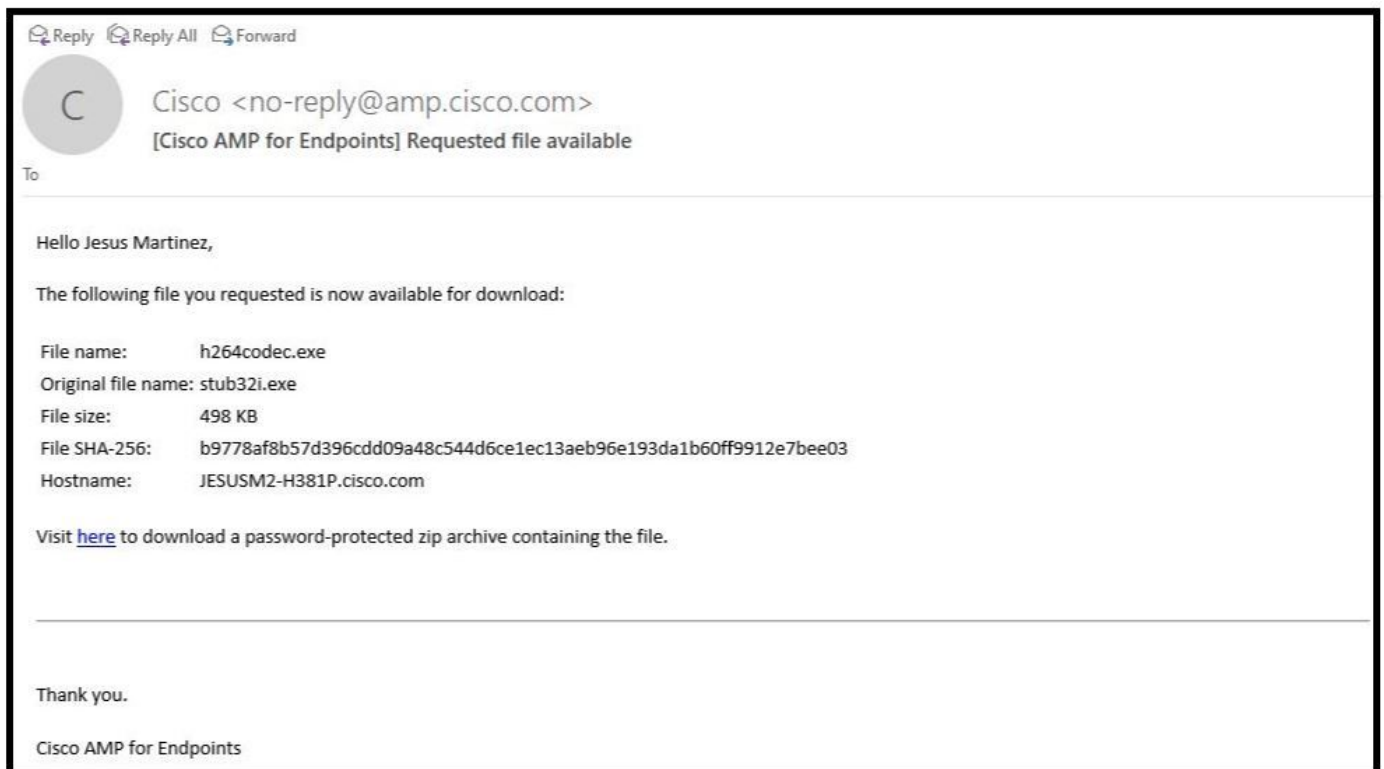
Stap 3. Selecteer het apparaat waar het bestand is gedetecteerd en klik op **Fetch** zoals in de afbeelding (het apparaat moet **ingeschakeld** zijn) zoals in de afbeelding.



Stap 4. U ontvangt het bericht zoals in de afbeelding.



Na een paar minuten ontvangt u een e-mailbericht wanneer het bestand kan worden gedownload zoals in de afbeelding wordt weergegeven.



Stap 5. Navigeer naar **AMP-console > Analysis > File Repository** en selecteer het bestand en klik op **Download** zoals in de afbeelding.

[Connector Diagnostics Feature Overview](#)

Search by SHA-256 or file name...

Status

Group

Type

▼ **h264codec.exe is Available** Requested by **Jesus Martinez** 2020-04-16 03:37:42 CDT

Original File Name	stub32i.exe
Fingerprint (SHA-256)	b9778af8...2e7bee03
File Size	498 KB
Computer	JESUSM2-H381P.cisco.com

Stap 6. Het vakje voor melding verschijnt, klik op **Downloaden**, zoals in de afbeelding, en het bestand wordt gedownload in een ZIP-bestand.

Warning

You are about to download **h264codec.exe**

This file may be malicious and cause harm to your computer. You should only download this file to a virtual machine that is not connected to any sensitive resources.

The file has been compressed in zip format with the password: **infected**

Alert Event Capture van AMP-console

Stap 1. Navigeer naar AMP-console > Dashboard > gebeurtenissen.

Stap 2. Selecteer de **gebeurtenis in de waarschuwing** en neem de opname zoals in de afbeelding.

▼ JESUSM2-H381P.cisco.com detected stub32i.exe as Win.Trojan.Generic::61.sbx.vloc Medium 2020-04-09 10:47:44 CDT

File Detection	Detection	▼ Win.Trojan.Generic::61.sbx.vloc
Connector Info	Fingerprint (SHA-256)	▼ b9778af8...2e7bee03
Comments	File Name	▼ stub32i.exe
	File Path	C:\Users\jesusm2\Downloads\stub32i.exe
	File Size	498.49 KB
	Parent Fingerprint (SHA-256)	▼ 2fb898ba...7bf74fef
	Parent Filename	▼ 7zG.exe

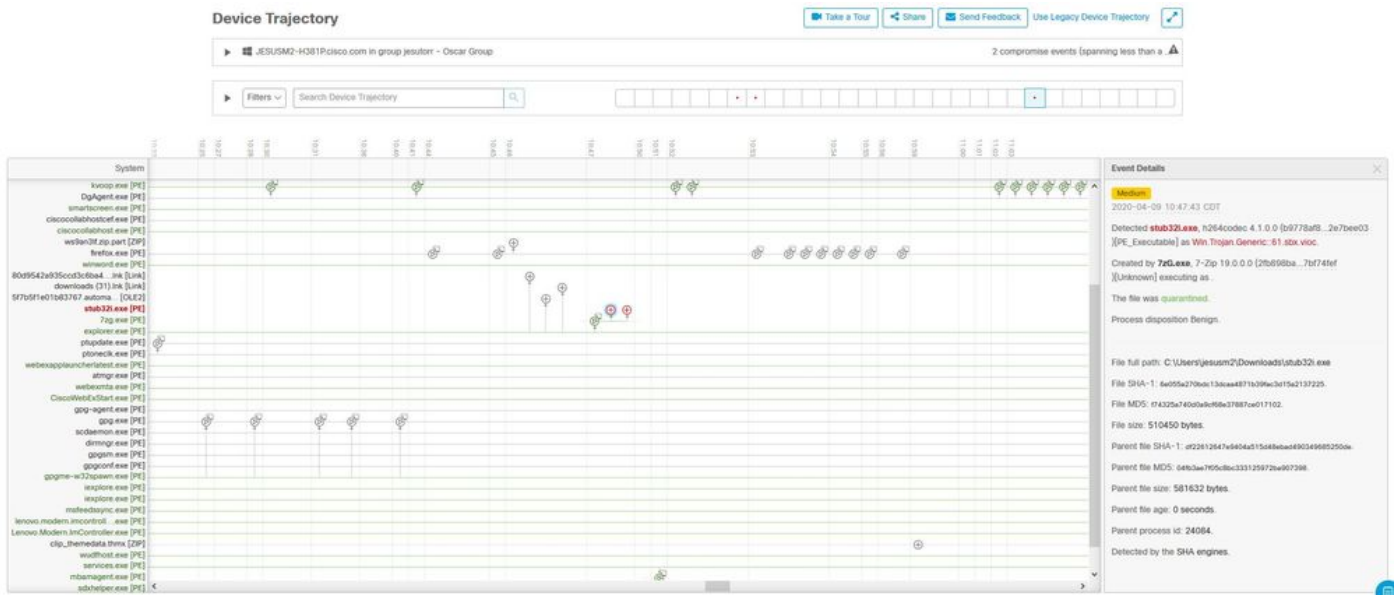
Event Details Capture of AMP-console

Stap 1. Navigeer naar **AMP-console > Dashboard > gebeurtenissen**.

Stap 2. Selecteer de gewenste gebeurtenis en klik op de optie **Apparaattraject** zoals in de afbeelding.



Het is gericht op de details van het **apparaattraject** zoals in de afbeelding.



Stap 3. Neem een opnamen van **Event Details** zoals in de afbeelding.

Event Details ✕

Medium

2020-04-09 10:47:43 CDT

Detected **stub32i.exe**, h264codec 4.1.0.0 (b9778af8...2e7bee03)
[PE_Executable] as **Win.Trojan.Generic::61.sbx.vioc**.

Created by **7zG.exe**, 7-Zip 19.0.0.0 (2fb898ba...7bf74fef)
[Unknown] executing as .

The file was **quarantined**.

Process disposition Benign.

File full path: C:\Users\jesusm2\Downloads\stub32i.exe

File SHA-1: 6e055a270bdc13dcaa4871b39fac3d15a2137225.

File MD5: f74325a740d0a9cf68e37887ce017102.

File size: 510450 bytes.

Parent file SHA-1: df22612647e9404a515d48ebad490349685250de.


Parent file MD5: 04fb3ae7f05c8bc333125972ba907398.

Parent file size: 581632 bytes.

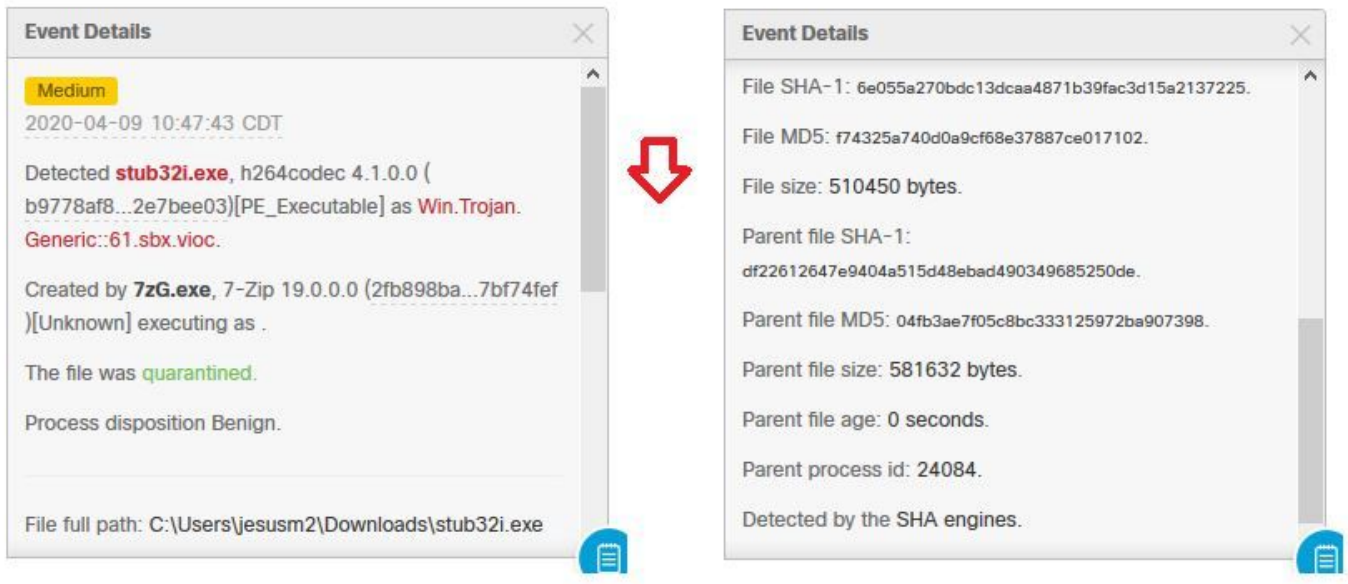
Parent file age: 0 seconds.

Parent process id: 24084.

Detected by the SHA engines.



Stap 4. Als dit nodig is, scrollen en neem dan een aantal opnamen om alle informatie over **gebeurtenissen** in de afbeelding te verkrijgen.



Informatie over het bestand

- Informatie over waar het bestand vandaan kwam.
- Als het bestand van een website komt, deelt u de URL van het web.
- Geef een kleine bestandsindeling en leg de bestandfunctie uit.

verklaring

- Waarom denk je dat het bestandsproces een fout-positief kan zijn?
- Geef de redenen aan waarom u op het bestand vertrouwt.

Informatie verstrekken

- Nadat u alle gegevens hebt verzameld, uploadt u alle gevraagde informatie naar <https://cway.cisco.com/csc/>.
- Zorg ervoor dat u het nummer van de serviceaanvraag raadpleegt.

Conclusie

Cisco streeft er altijd naar de bedreigingsintelligentie voor AMP voor endpoints-technologie te verbeteren en uit te breiden, maar als uw AMP voor Endpoints-oplossing onjuist een waarschuwing oproept, kunt u bepaalde acties ondernemen om verdere impact op uw omgeving te voorkomen. Dit document biedt een richtlijn om alle vereiste details te verkrijgen om een case met Cisco TAC te openen voor een valse positieve kwestie. Gebaseerd op de diagnostische teamanalyse kan de bestandsindeling veranderen om de waarschuwingsgebeurtenissen te stoppen die zijn geactiveerd op AMP Console of Cisco TAC kan de juiste oplossing bieden om het bestand/proces te laten uitvoeren zonder problemen in uw omgeving.