

Fehlerbehebung bei Fehlalarmen Dateianalyse in AMP für Endgeräte

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Fehlerbehebung bei Fehlalarmen Dateianalyse in AMP für Endgeräte](#)

[Datei SHA 256 Hash](#)

[Beispieldatei](#)

[Erfassung von Warnereignissen von der AMP-Konsole](#)

[Erfassung von Ereignisdetails von der AMP-Konsole](#)

[Informationen zur Datei](#)

[Erläuterung](#)

[Bereitstellung von Informationen](#)

[Schlussfolgerung](#)

Einführung

In diesem Dokument wird beschrieben, wie eine Datei-Analyse mit Fehlalarmen in AMP (Advanced Malware Protection) für Endgeräte erfasst wird.

Mitwirkend von Jesus Javier Martinez, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- AMP Console-Dashboard
- Ein Konto mit Administratorrechten

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco AMP für Endgeräte Version 6.X.X und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

AMP für Endgeräte kann übermäßige Warnungen für eine bestimmte Datei/einen bestimmten Prozess und einen sicheren Hash-Algorithmus (SHA) 256 generieren. Wenn Sie vermuten, dass in Ihrem Netzwerk Fehlalarme auftreten, können Sie sich an das Cisco Technical Assistance Center (TAC) wenden. Das Diagnoseteam führt dann eine eingehendere Dateianalyse durch. Wenn Sie sich an das Cisco TAC wenden, müssen Sie folgende Informationen angeben:

- Datei-SHA 256-Hash
- Datei-Beispielkopie
- Erfassung von Warnungs-Ereignissen von der AMP-Konsole
- Erfassung von Ereignisdetails über die AMP-Konsole
- Informationen über die Datei (woher sie stammt und warum sie in der Umgebung sein muss)
- Erläutern, warum die Datei/der Prozess Ihrer Meinung nach falsch positiv sein kann

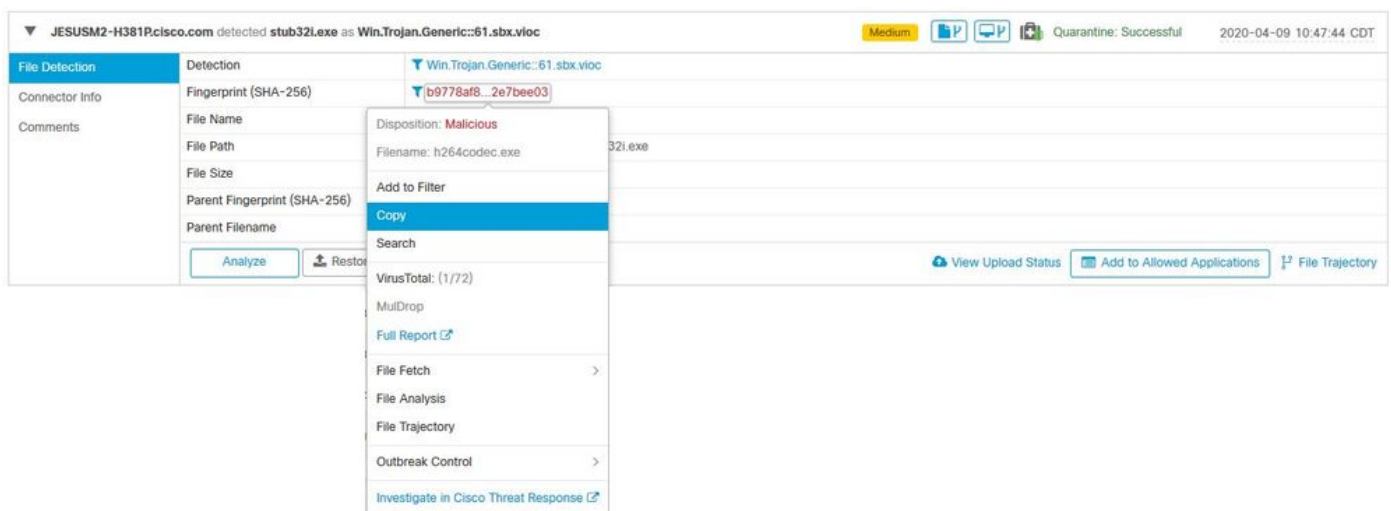
Fehlerbehebung bei Fehlalarmen Dateianalyse in AMP für Endgeräte

Dieser Abschnitt enthält Informationen, mit denen Sie alle erforderlichen Details zum Öffnen eines Fehlalarmen-Tickets beim Cisco TAC erhalten.

Datei SHA 256 Hash

Schritt 1: Um den SHA 256-Hash abzurufen, navigieren Sie zu **AMP Console > Dashboard > Events**.

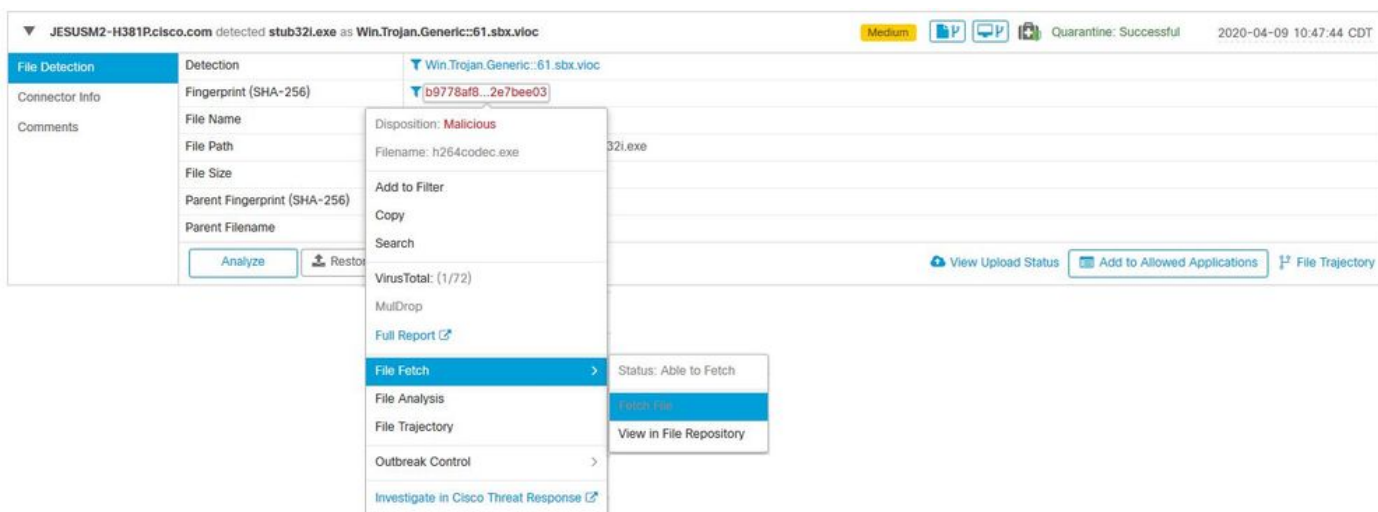
Schritt 2: Wählen Sie den **Alert Event** aus, klicken Sie auf **SHA256** und wählen Sie **Copy** aus, wie im Bild gezeigt.



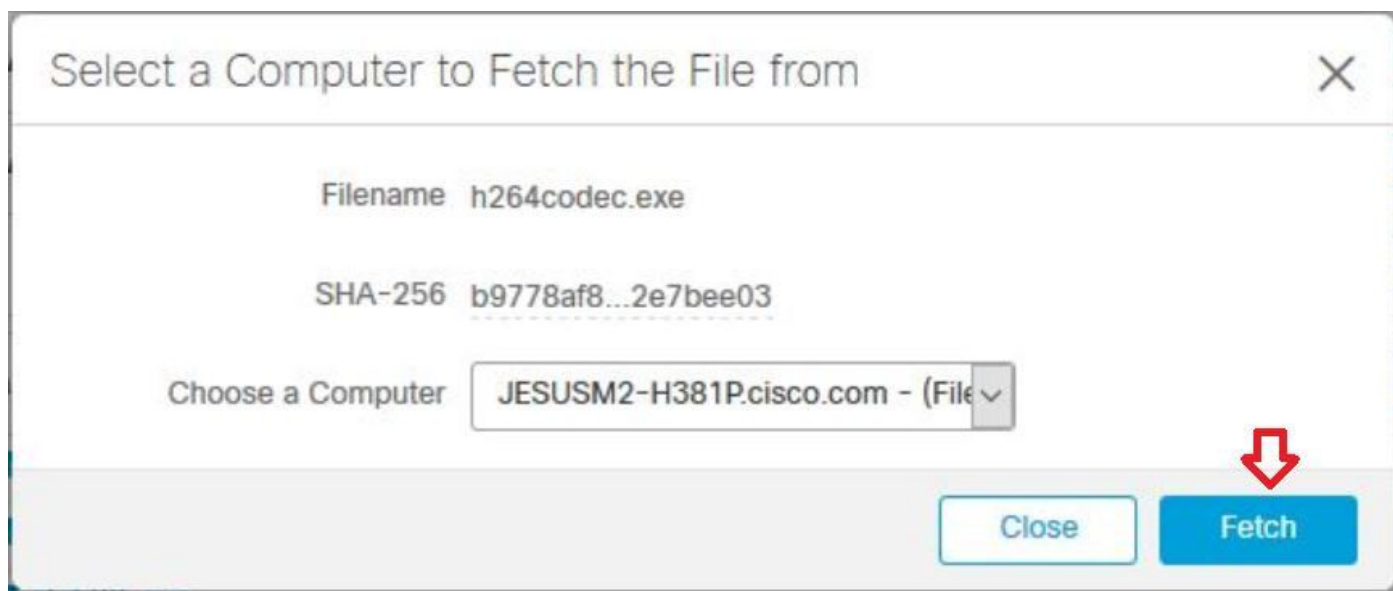
Beispieldatei

Schritt 1: Sie können das Dateibeispiel von der AMP Console abrufen und zu **AMP Console > Dashboard > Events** navigieren.

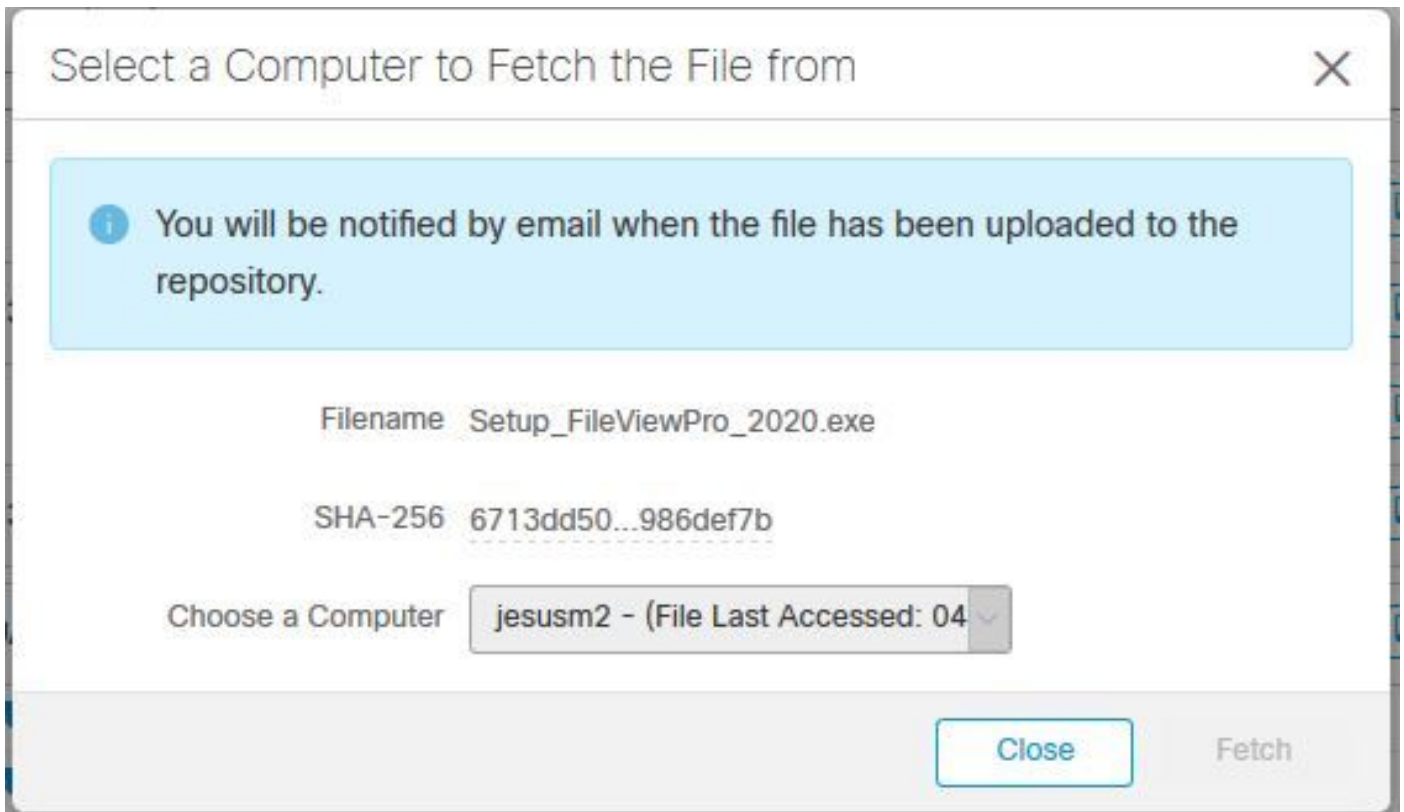
Schritt 2: Wählen Sie das **Alert Event** aus, klicken Sie auf den **SHA256** und navigieren Sie zu **File Fetch**> **File Fetch** wie im Bild gezeigt.



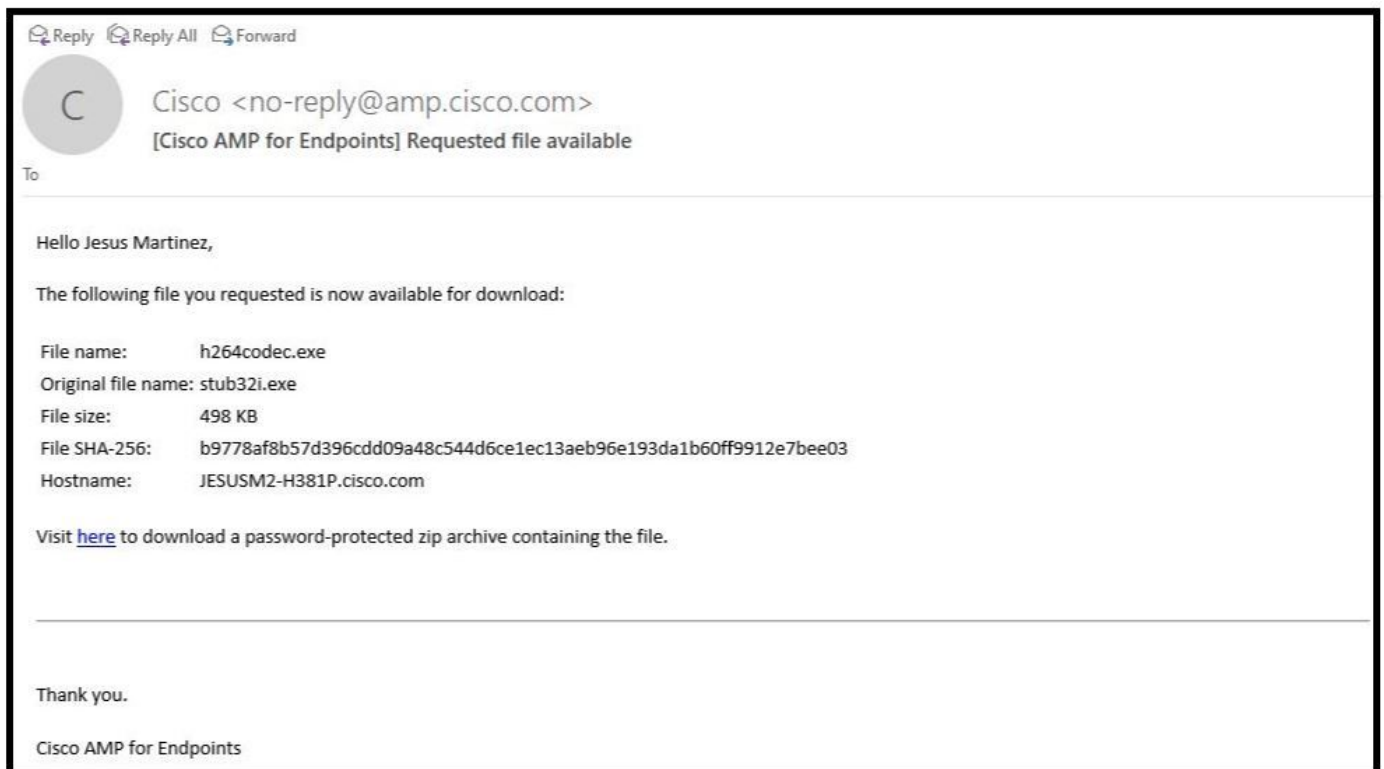
Schritt 3: Wählen Sie das Gerät aus, auf dem die Datei erkannt wurde, und klicken Sie auf **Abrufen** wie im Bild gezeigt (das Gerät muss **EIN** aktiviert sein), wie im Bild gezeigt.



Schritt 4: Sie erhalten die Nachricht wie im Bild gezeigt.



Nach einigen Minuten erhalten Sie eine E-Mail-Benachrichtigung, wenn die Datei wie im Bild gezeigt heruntergeladen werden kann.



Schritt 5: Navigieren Sie zu **AMP Console > Analysis > File Repository** und wählen Sie die Datei aus, und klicken Sie auf **Download** wie im Bild gezeigt.

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

Schritt 6: Das Benachrichtigungsfeld wird angezeigt. Klicken Sie auf **Download (Herunterladen)**, wie im Bild gezeigt, und die Datei wird auf eine ZIP-Datei heruntergeladen.

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**

Erfassung von Warnereignissen von der AMP-Konsole

Schritt 1: Navigieren Sie zu **AMP Console > Dashboard > Events**.

Schritt 2: Wählen Sie das **Alert Event** aus, und übernehmen Sie die Erfassung wie im Bild gezeigt.

▼ JESUSM2-H381P.cisco.com detected stub32i.exe as Win.Trojan.Generic::61.sbx.vloc Medium Quarantine: Successful 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

Erfassung von Ereignisdetails von der AMP-Konsole

Schritt 1: Navigieren Sie zu **AMP Console > Dashboard > Events**.

Schritt 2: Wählen Sie das Alert Event aus, und klicken Sie auf die Option **Device Trajectory** (Device Trajectory), wie im Bild gezeigt.



File Detection	Detection	Win.Trojan.Generic:61.sbx.vioc
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	

[Analyze](#) [Restore File](#) [All Computers](#) [View Upload Status](#) [Add to Allowed Applications](#) [File Trajectory](#)

Es wird zu **Device Trajectory-Details** umgeleitet, wie im Bild gezeigt.

Device Trajectory

JESUSM2-H381P:cisco.com in group jesu201 - Oscar Group

2 compromise events (spanning less than a ...)

Filters Search Device Trajectory

Event Details

2020-04-09 10:47:43 CDT

Detected **stub32i.exe**, n264codic 4.1.0.0 (b9778af8...2e7bee03) [PE_Executable] as Win.Trojan.Generic:61.sbx.vioc.

Created by 7zG.exe, 7-Zip 19.00.0.0 (2fb898ba...7bf74fef) [Unknown] executing as.

The file was quarantined.

Process disposition benign.

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

File SHA-1: 6e05e270e4136e44871b39ac3e15e2137225

File MD5: ff4325a7400bae68e37887e0d11102

File size: 510450 bytes

Parent file SHA-1: af22812647d804e015683eae490349882505a

Parent file MD5: 6ab3e795e6bc333125972e907298

Parent file size: 581632 bytes

Parent file age: 0 seconds

Parent process id: 24084

Detected by the SHA engines.

Schritt 3: Erfassen Sie das Feld **Ereignisdetails**, wie im Bild gezeigt.

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.

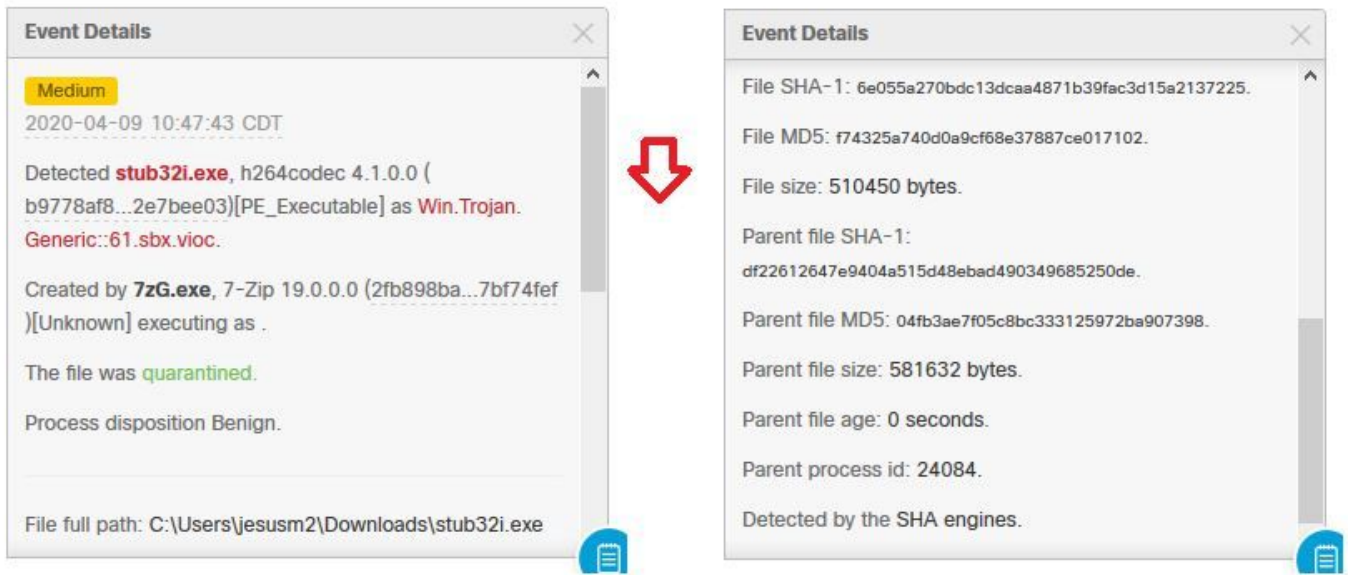
Parent file age: 0 seconds.

Parent process id: 24084.

Detected by the SHA engines.



Schritt 4: Scrollen Sie bei Bedarf nach unten, und nehmen Sie einige Aufnahmen vor, um alle im Bild angezeigten **Veranstaltungsdetails** abzurufen.



Informationen zur Datei

- Informationen darüber, woher die Datei stammt.
- Wenn die Datei von einer Website kommt, teilen Sie die Web-URL.
- Teilen Sie eine kleine Dateibeschreibung und erläutern Sie die Dateifunktion.

Erläuterung

- Warum glauben Sie, dass der Dateiprozess falsch positiv sein kann?
- Geben Sie die Gründe an, aus denen Sie der Datei vertrauen.

Bereitstellung von Informationen

- Wenn Sie alle Daten erfasst haben, laden Sie alle angeforderten Informationen auf <https://cway.cisco.com/csc/ hoch>.
- Stellen Sie sicher, dass Sie die Service Request-Nummer angeben.

Schlussfolgerung

Cisco ist stets bemüht, die Bedrohungsinformationen für die AMP für Endgeräte-Technologie zu verbessern und zu erweitern. Wenn Ihre AMP für Endgeräte-Lösung jedoch eine falsche Warnmeldung auslöst, können Sie einige Maßnahmen ergreifen, um weitere Auswirkungen auf Ihre Umgebung zu verhindern. Dieses Dokument enthält eine Richtlinie, die alle erforderlichen Details zum Erstellen eines Falls beim Cisco TAC bezüglich eines Fehlalarmen enthält. Basierend auf der Dateianalyse des Diagnostic Team kann sich die Einstufung der Datei ändern, um die auf der AMP-Konsole ausgelösten Warnungsereignisse zu stoppen, oder das Cisco TAC kann die richtige Lösung bereitstellen, damit die Datei/der Prozess ohne Probleme in Ihrer Umgebung ausgeführt werden kann.