

Solución de problemas de análisis de archivos falsos positivos en AMP para terminales

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Solución de problemas de análisis de archivos falsos positivos en AMP para terminales](#)

[Archivo SHA 256 Hash](#)

[Copia de ejemplo de archivo](#)

[Captura de eventos de alerta desde la consola de AMP](#)

[Captura de detalles del evento desde la consola de AMP](#)

[Información sobre el archivo](#)

[Explicación](#)

[Proporcionar información](#)

[Conclusión](#)

Introducción

Este documento describe cómo recopilar un análisis de archivos falsos positivos en protección frente a malware avanzado (AMP) para terminales.

Colaborado por Jesús Javier Martínez, Ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda tener conocimientos de estos temas:

- Panel de la consola AMP
- Una cuenta con privilegios de administrador

Componentes Utilizados

La información de este documento se basa en Cisco AMP para terminales versión 6.X.X y posterior.

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. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

AMP para terminales puede generar alertas excesivas en un determinado archivo/proceso/algorithm hash seguro (SHA) 256. Si sospecha que hay detecciones de falsos positivos en la red, puede ponerse en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC), el equipo de diagnóstico procede a realizar un análisis de archivos más profundo. Cuando se ponga en contacto con el TAC de Cisco, debe proporcionar esta información:

hash de archivo · SHA 256

Ejemplo de copia de archivo ·

Captura de evento de alerta de · desde la consola de AMP

Captura de detalles del evento de · desde la consola de AMP

·Información sobre el archivo (de dónde procede y por qué debe estar en el entorno)

·Explicar por qué cree que el archivo/proceso puede ser un falso positivo

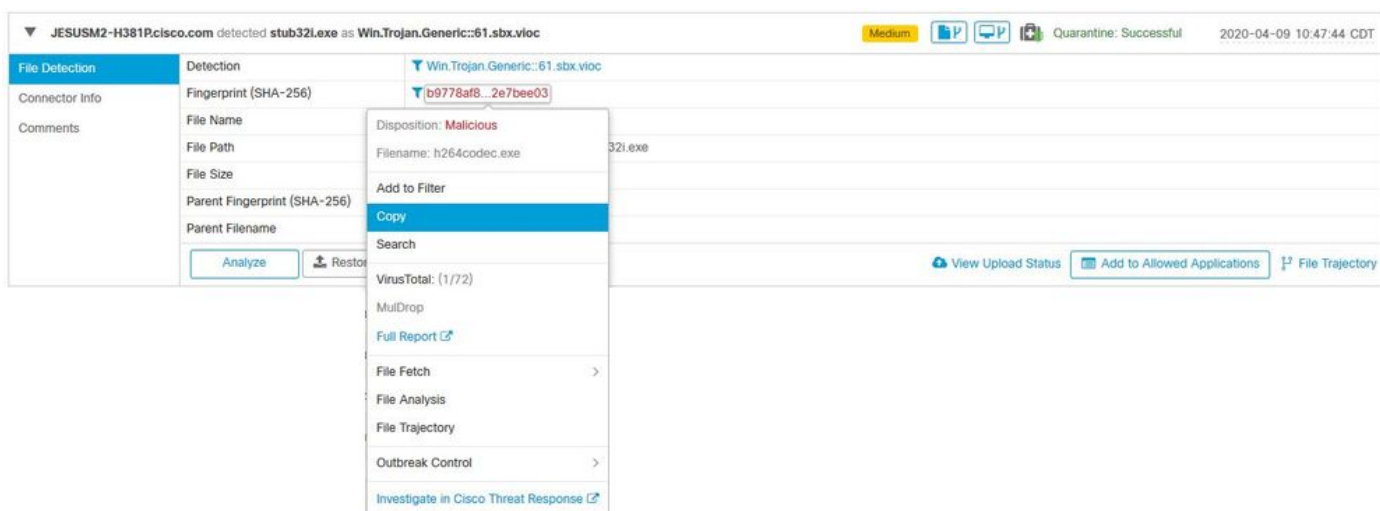
Solución de problemas de análisis de archivos falsos positivos en AMP para terminales

Esta sección proporciona información que puede utilizar para obtener todos los detalles necesarios para abrir un ticket de falso positivo con el TAC de Cisco.

Archivo SHA 256 Hash

Paso 1. Para obtener el hash SHA 256, navegue hasta **Consola AMP > Panel > Eventos**.

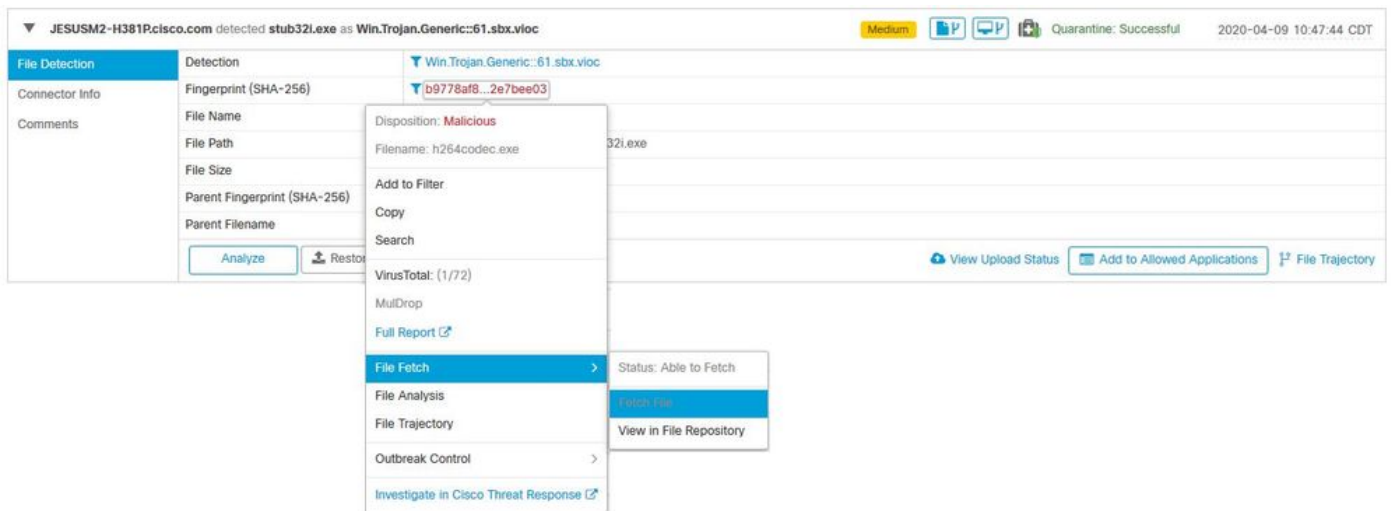
Paso 2. Seleccione el **Evento de alerta**, haga clic en el **SHA256** y seleccione **Copiar** como se muestra en la imagen.



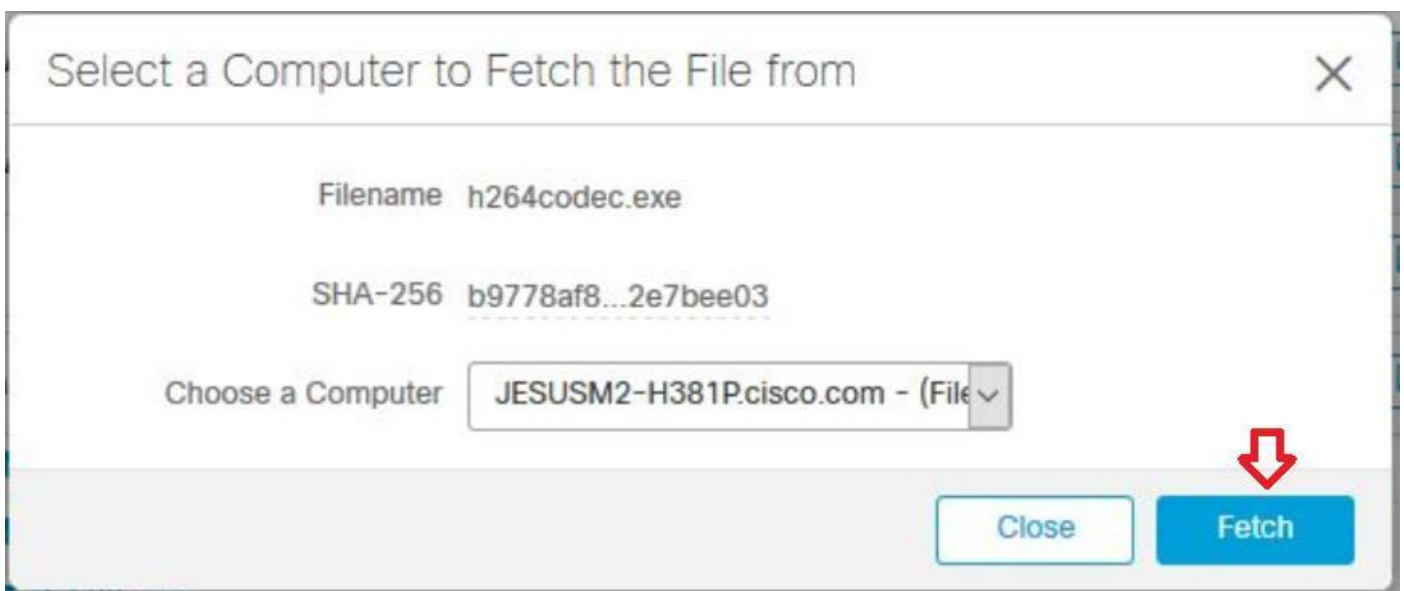
Copia de ejemplo de archivo

Paso 1. Puede obtener el ejemplo de archivo desde la consola de AMP, navegar hasta **la consola de AMP > Panel > Eventos**.

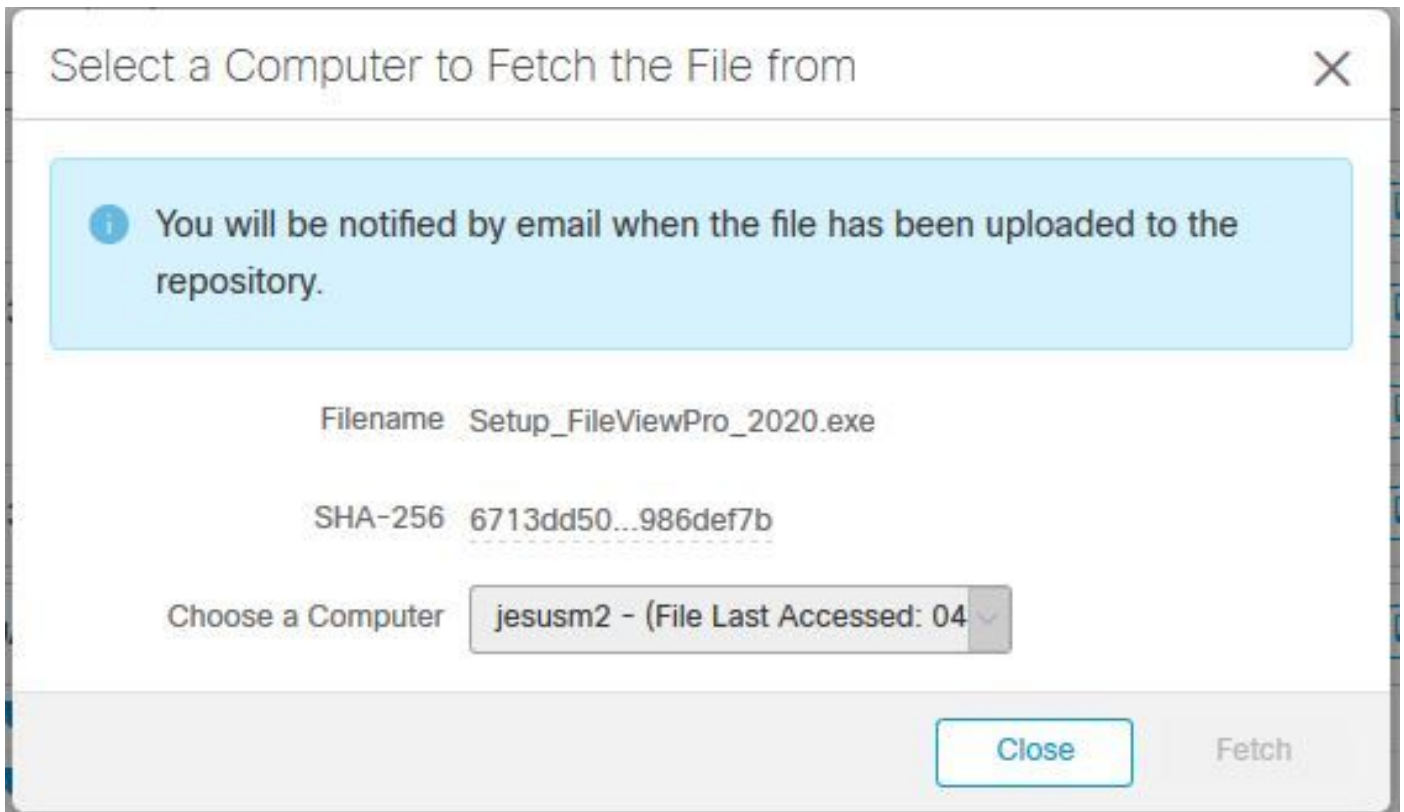
Paso 2. Seleccione el **Evento de Alerta**, haga clic en el **SHA256** y navegue hasta **Archivo Buscar** > **Archivo Buscar** como se muestra en la imagen.



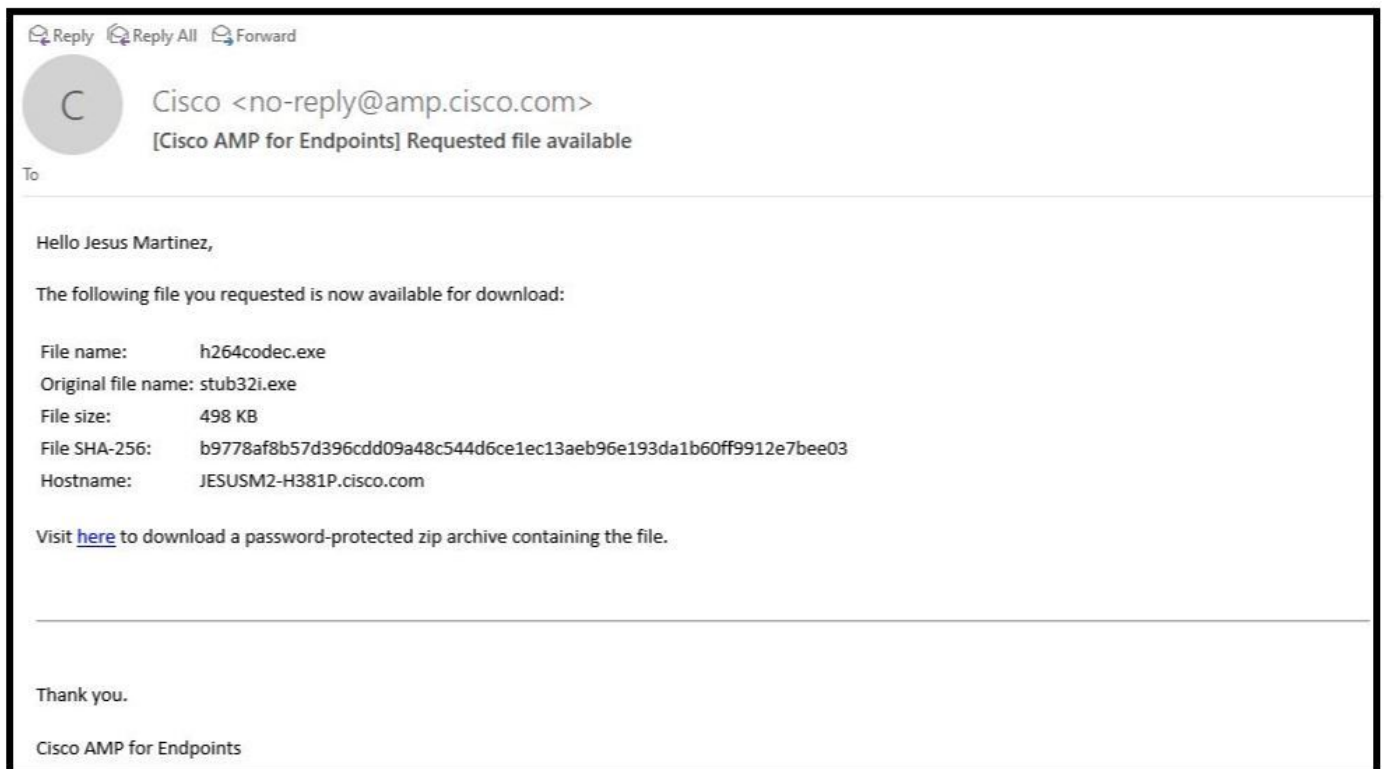
Paso 3. Seleccione el dispositivo en el que se detectó el archivo y haga clic en **Buscar** como se muestra en la imagen (el dispositivo debe estar encendido) como se muestra en la imagen.



Paso 4. Recibirá los mensajes como se muestra en la imagen.



Después de unos minutos, recibirá una notificación por correo electrónico cuando el archivo esté disponible para descargar, como se muestra en la imagen.



Paso 5. Navegue hasta **Consola de AMP > Análisis > Repositorio de archivos** y seleccione el archivo y haga clic en **Descargar** como se muestra en la imagen.

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

Paso 6. Aparece el cuadro Notificación, haga clic en **Descargar**, como se muestra en la imagen, y el archivo se descarga en un archivo ZIP.

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**

Captura de eventos de alerta desde la consola de AMP

Paso 1. Vaya a **Consola de AMP > Panel > Eventos**.

Paso 2. Seleccione el **evento Alert** y tome la captura como se muestra en la imagen.

▼ 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

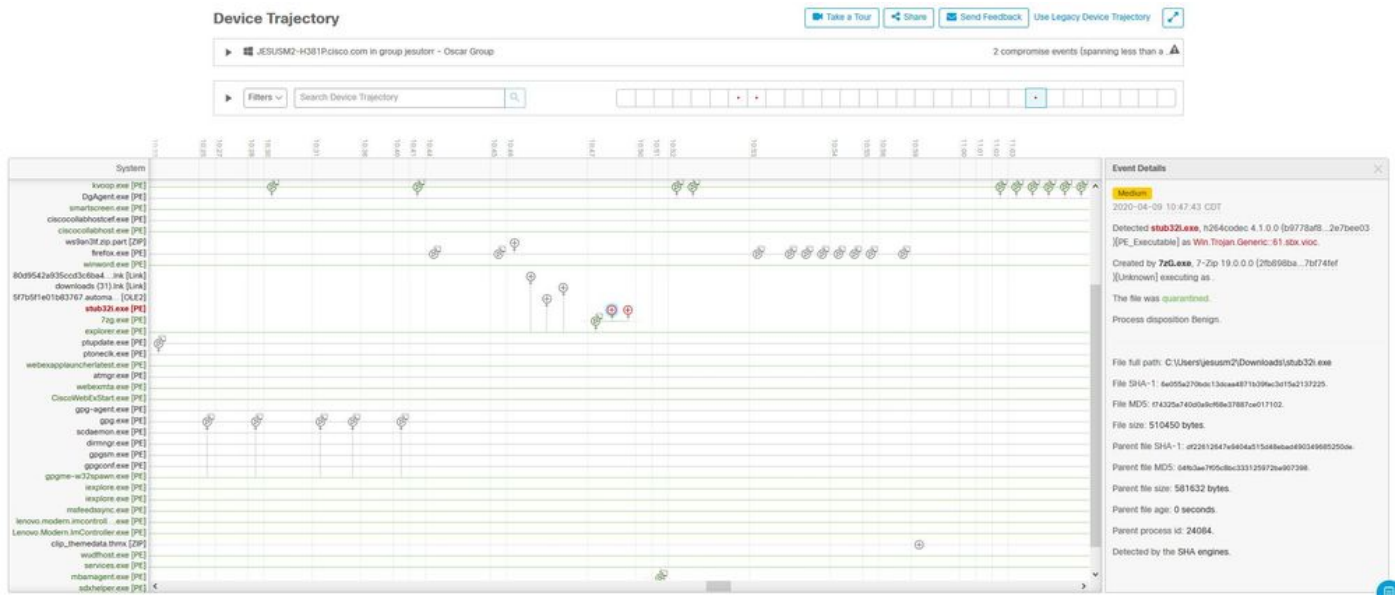
Captura de detalles del evento desde la consola de AMP

Paso 1. Vaya a **Consola de AMP > Panel > Eventos.**

Paso 2. Seleccione el evento Alert y haga clic en la opción **Device Trajectory** como se muestra en la imagen.



Se redirige a los detalles de trayectoria del dispositivo como se muestra en la imagen.



Paso 3. Realice una captura del cuadro **Detalles del evento** como se muestra en la imagen.

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.

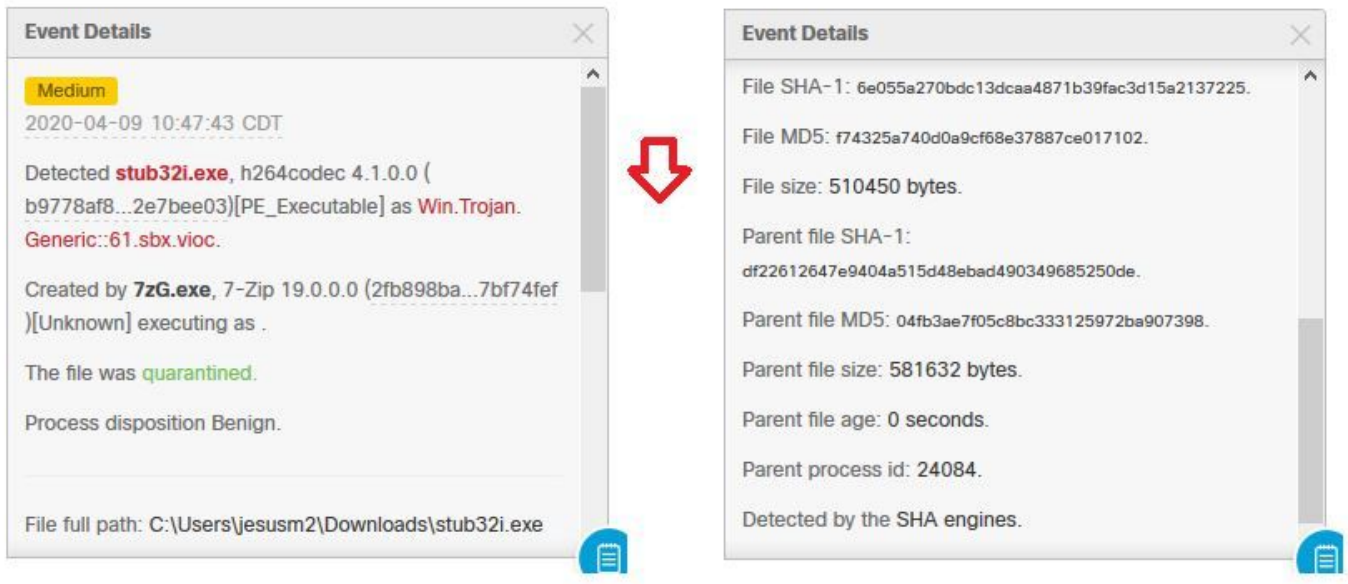
Parent file age: 0 seconds.

Parent process id: 24084.

Detected by the SHA engines.



Paso 4. Si es necesario, desplácese hacia abajo y tome algunas capturas para obtener toda la información **de detalles de eventos** como se muestra en la imagen.



Información sobre el archivo

- Información sobre de dónde vino el archivo.
- Si el archivo proviene de un sitio web, comparta la URL web.
- Comparta una pequeña descripción del archivo y explique su función.

Explicación

- ¿Por qué cree que el proceso de archivo puede ser un falso positivo?
- Comparta los motivos en los que confía en el archivo.

Proporcionar información

- Una vez que recopile todos los detalles, cargue toda la información solicitada en <https://cway.cisco.com/csc/>.
- Asegúrese de hacer referencia al número de solicitud de servicio.

Conclusión

Cisco siempre se esfuerza por mejorar y ampliar la inteligencia de amenazas para la tecnología de AMP para terminales; sin embargo, si su solución de AMP para terminales activa una alerta por error, puede tomar algunas medidas para evitar cualquier impacto adicional en su entorno. Este documento proporciona una guía para obtener todos los detalles requeridos para abrir un caso con Cisco TAC con respecto a un problema de falsos positivos. En base al análisis de archivos del equipo de diagnóstico, la disposición del archivo puede cambiar para detener los eventos de alerta activados en la consola de AMP o Cisco TAC puede proporcionar la solución adecuada para permitir ejecutar el archivo/proceso sin problemas en su entorno.