

Solucione problemas de análise de arquivo falso positivo na AMP para endpoints

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Solucione problemas de análise de arquivo falso positivo na AMP para endpoints](#)

[Hash SHA 256 do arquivo](#)

[Cópia de exemplo de arquivo](#)

[Captura de evento de alerta do console AMP](#)

[Captura de detalhes do evento do console AMP](#)

[Informações sobre o arquivo](#)

[Explicação](#)

[Fornecer informações](#)

[Conclusão](#)

Introduction

Este documento descreve como coletar uma análise de arquivo Falso Positivo no Advanced Malware Protection (AMP) for Endpoints.

Contribuído por Jesus Javier Martinez, engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você conheça estes tópicos:

- Painel do console AMP
- Uma conta com privilégios de administrador

Componentes Utilizados

As informações neste documento são baseadas no Cisco AMP para endpoints versão 6.X.X e superiores.

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.

Informações de Apoio

O AMP para endpoints pode gerar alertas excessivos sobre um determinado arquivo/processo/Algoritmo de hash seguro (SHA) 256. Se você suspeitar de detecções Falso positivo em sua rede, você pode entrar em contato com o Cisco Technical Assistance Center (TAC), a equipe de diagnóstico continua fazendo uma análise mais profunda do arquivo. Ao entrar em contato com o Cisco TAC, você precisa fornecer estas informações:

Arquivo SHA 256 hash

Cópia do exemplo do arquivo

Captura de evento de alerta do console AMP

Captura de Detalhes do evento do console AMP

Informações sobre o arquivo (de onde ele veio e por que ele precisa estar no ambiente)

Explique por que você acredita que o arquivo/processo pode ser um falso positivo

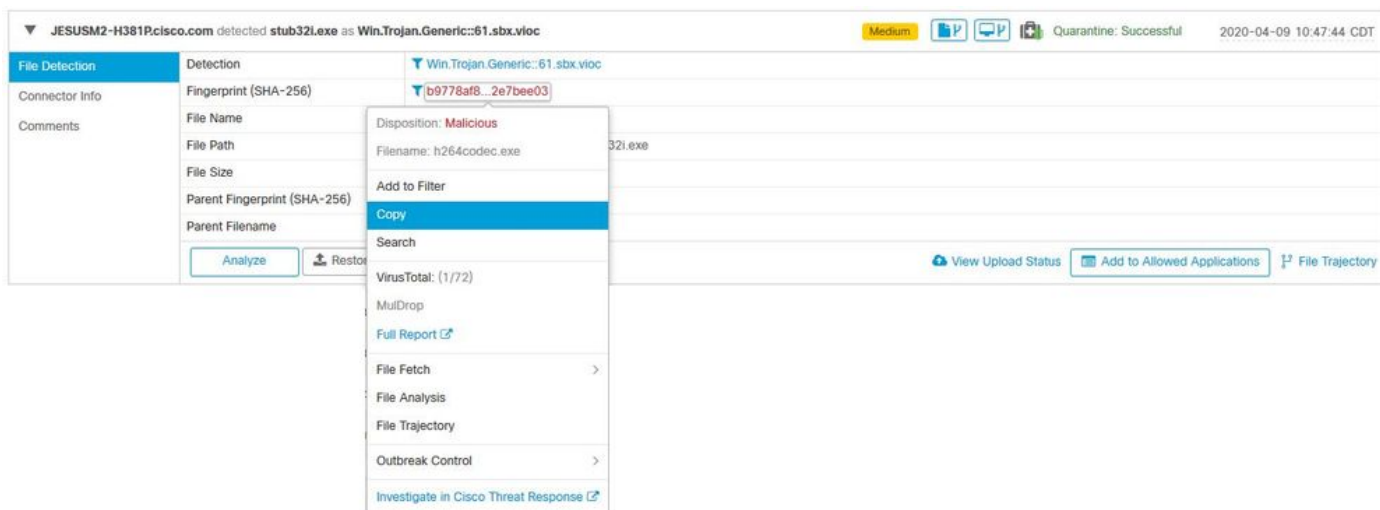
Solucione problemas de análise de arquivo falso positivo na AMP para endpoints

Esta seção fornece informações que você pode usar para obter todos os detalhes necessários para abrir um tíquete falso positivo com o Cisco TAC.

Hash SHA 256 do arquivo

Etapa 1. Para obter o hash SHA 256, navegue para **Console do AMP > Painel > Eventos**.

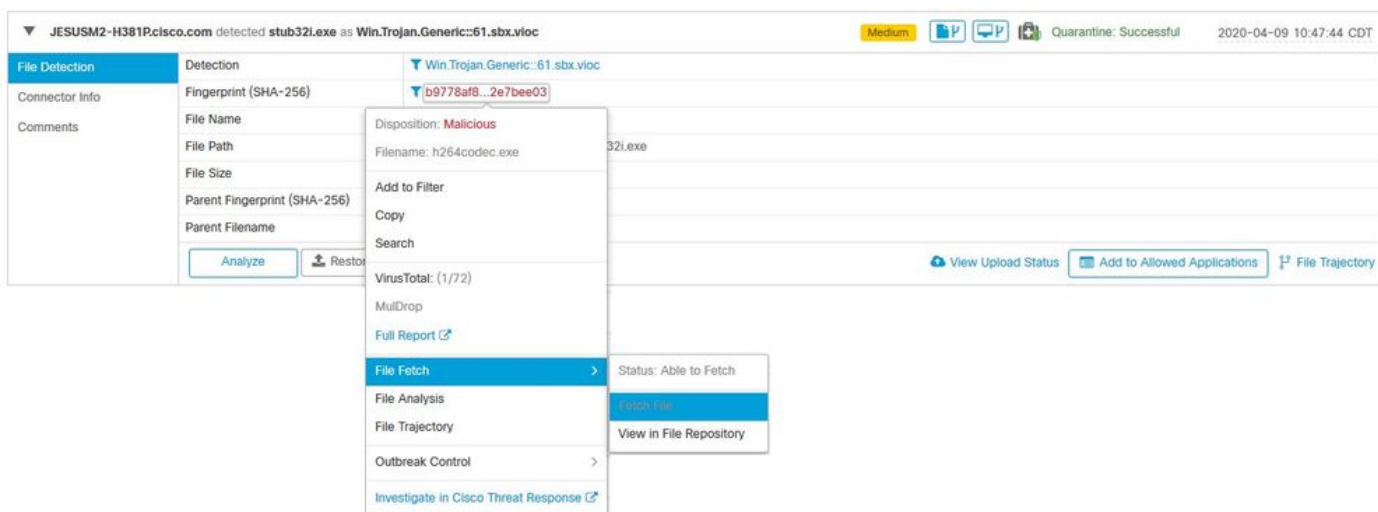
Etapa 2. Selecione o **Evento de alerta**, clique no **SHA256** e selecione **Copiar** como mostrado na imagem.



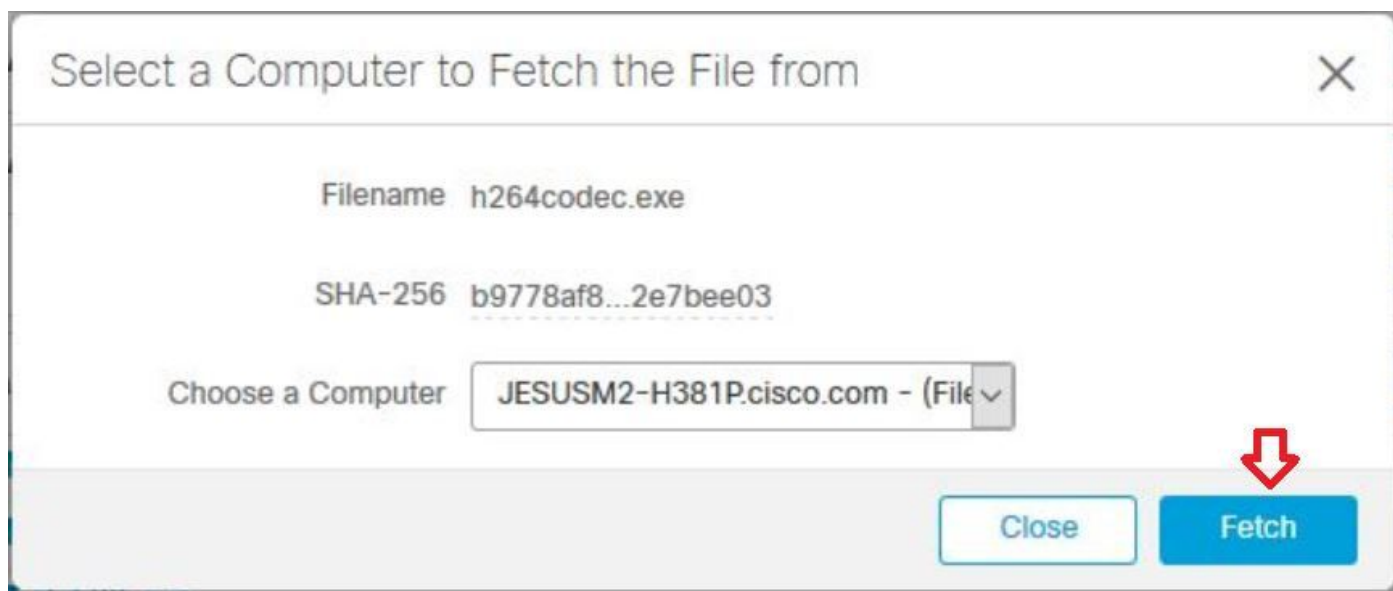
Cópia de exemplo de arquivo

Etapa 1. Você pode obter o exemplo do arquivo do console AMP, navegar para **Console AMP > Painel > Eventos**.

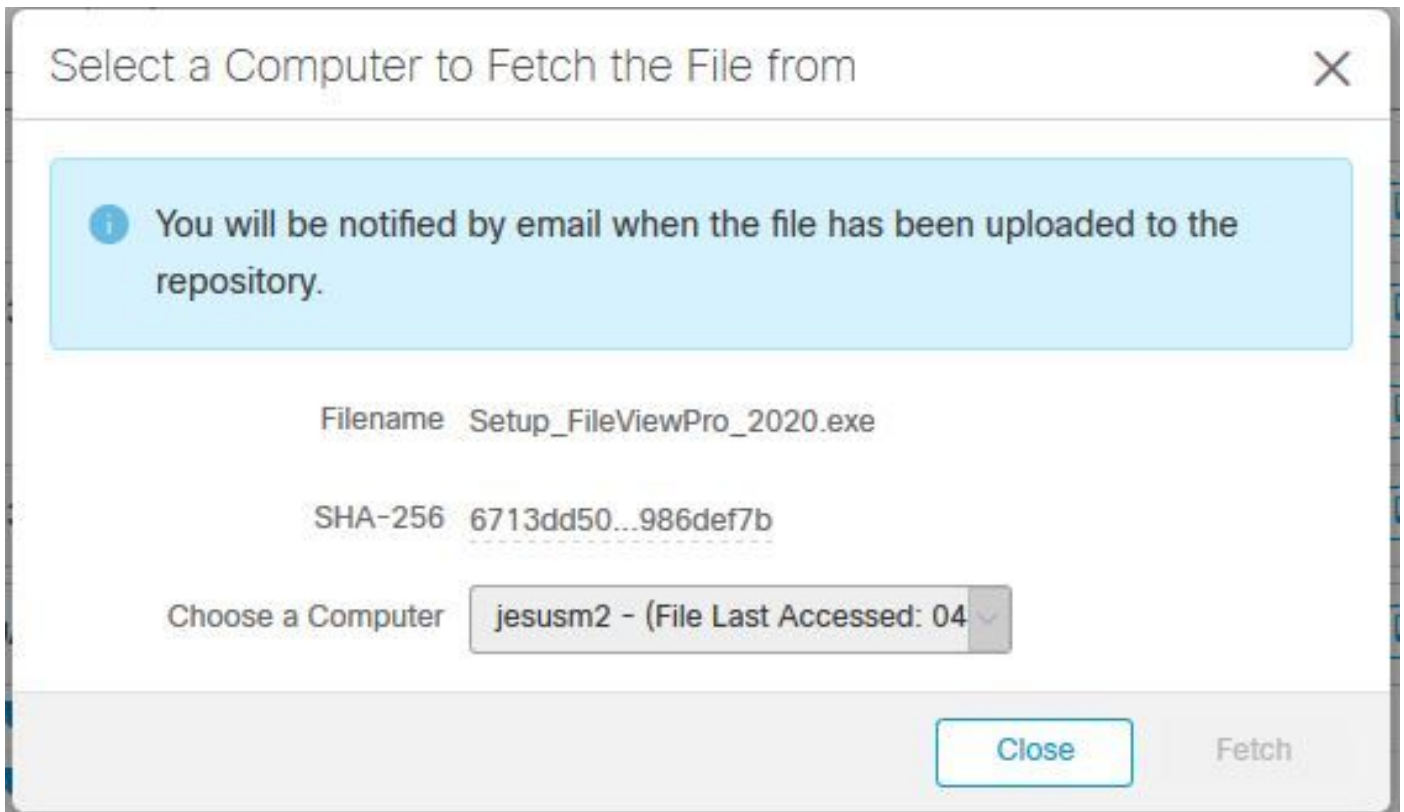
Etapa 2. Selecione o **Evento de alerta**, clique no **SHA256** e navegue para **Busca de arquivo**> **Busca de arquivo** como mostrado na imagem.



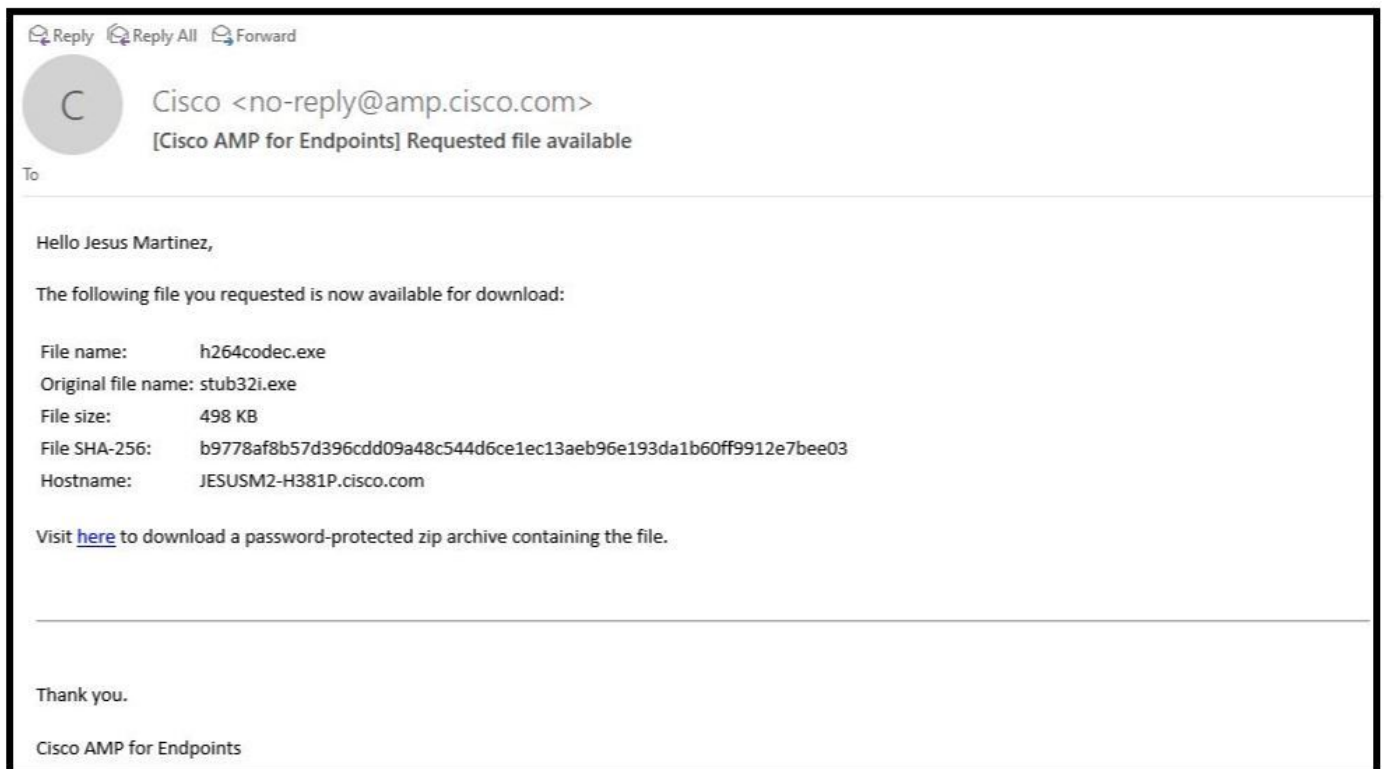
Etapa 3. Selecione o dispositivo onde o arquivo foi detectado e clique em **Buscar** como mostrado na imagem (o dispositivo deve estar **LIGADO**) como mostrado na imagem.



Etapa 4. Você recebe a mensagem como mostrado na imagem.



Após alguns minutos, você recebe uma notificação por e-mail quando o arquivo está disponível para download, como mostrado na imagem.



Etapa 5. Navegue até **Console do AMP > Análise > Repositório de arquivos** e selecione o arquivo e clique em **Download** conforme mostrado na imagem.

[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

Etapa 6. A caixa Notificação é exibida, clique em **Download**, conforme mostrado na imagem, e o arquivo é baixado em um arquivo ZIP.



Captura de evento de alerta do console AMP

Etapa 1. Navegue até **Console do AMP > Painel > Eventos**.

Etapa 2. Selecione o **evento de alerta** e faça a captura conforme mostrado na imagem.

▼ 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

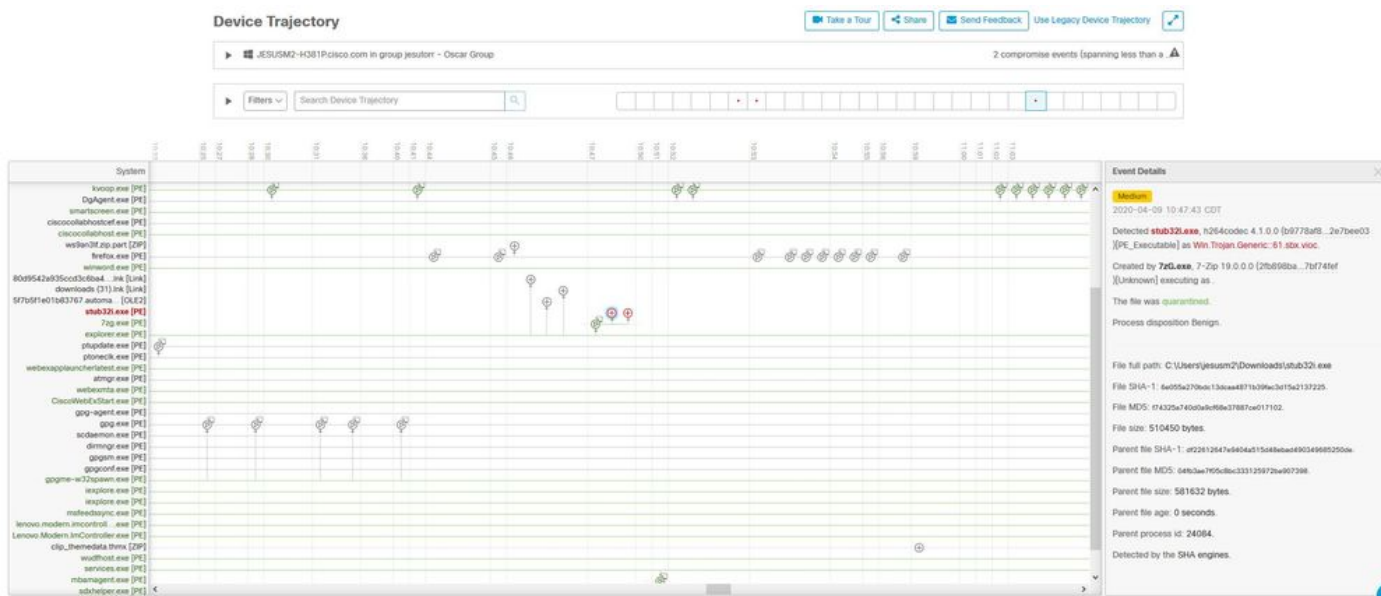
Captura de detalhes do evento do console AMP

Etapa 1. Navegue até **Console do AMP > Painel > Eventos**.

Etapa 2. Selecione o evento de alerta e clique na opção **Device Trajectory** (Trajetória do dispositivo) conforme mostrado na imagem.



Ele redireciona para os detalhes da **trajetória do dispositivo**, como mostrado na imagem.



Etapa 3. Tire uma captura da caixa **Detalhes do Evento** conforme mostrado na imagem.

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.

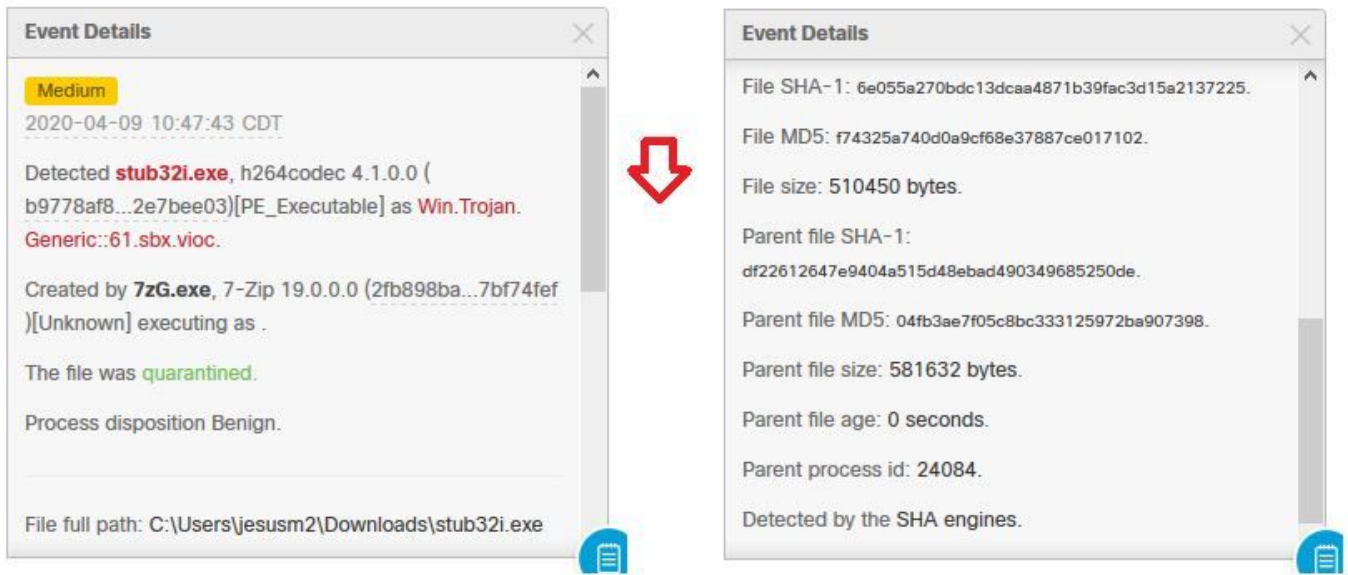
Parent file age: 0 seconds.

Parent process id: 24084.

Detected by the SHA engines.



Etapa 4. Se necessário, role para baixo e faça algumas capturas para obter todas as informações **Detalhes do evento**, como mostrado na imagem.



Informações sobre o arquivo

- Informações sobre de onde veio o arquivo.
- Se o arquivo vier de um site, compartilhe o URL da Web.
- Compartilhe uma pequena descrição do arquivo e explique a função do arquivo.

Explicação

- Por que você acredita que o processo de arquivo pode ser um falso positivo?
- Compartilhe os motivos confiáveis no arquivo.

Fornecer informações

- Depois de coletar todos os detalhes, carregue todas as informações solicitadas em <https://cway.cisco.com/csc/>.
- Certifique-se de fazer referência ao número da solicitação de serviço.

Conclusão

A Cisco sempre se esforça para melhorar e expandir a inteligência de ameaças para a tecnologia AMP para endpoints. No entanto, se a solução AMP para endpoints disparar um alerta de forma errada, você pode tomar algumas medidas para evitar qualquer impacto adicional no seu ambiente. Este documento fornece uma diretriz para obter todos os detalhes necessários para abrir um caso com o Cisco TAC em relação a um problema Falso Positivo. Com base na análise do arquivo da equipe de diagnóstico, a disposição do arquivo pode ser alterada para interromper os eventos de alerta disparados no console AMP ou o Cisco TAC pode fornecer a correção adequada para permitir a execução do arquivo/processo sem problemas no seu ambiente.