

# エンドポイント用AMPの誤検出ファイル分析のトラブルシューティング

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[エンドポイント用AMPの誤検出ファイル分析のトラブルシューティング](#)

[ファイルSHA 256ハッシュ](#)

[ファイルサンプルコピー](#)

[AMPコンソールからのアラートイベントキャプチャ](#)

[AMPコンソールからのイベント詳細キャプチャ](#)

[ファイルに関する情報](#)

[説明](#)

[情報の提供](#)

[結論](#)

## 概要

このドキュメントでは、Advanced Malware Protection(AMP)for EndpointsでFalse Positiveファイル分析を収集する方法について説明します。

著者：Cisco TACエンジニア、Jez Javier Martinez

## 前提条件

### 要件

次の項目に関する知識があることを推奨しています。

- AMPコンソールダッシュボード
- 管理者権限を持つアカウント

### 使用するコンポーネント

このドキュメントの情報は、Cisco AMP for Endpointsバージョン6.X.X以降に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 背景説明

AMP for Endpointsは、特定のファイル/プロセス/セキュアハッシュアルゴリズム(SHA)に過剰なアラートを生成する可能性があります。ネットワーク内の誤検出が疑われる場合は、Cisco Technical Assistance Center(TAC)に連絡し、診断チームが詳細なファイル分析を行います。

- ・ ファイルSHA 256ハッシュ
- ・ ファイルサンプルコピー
- ・ AMPコンソールからのアラート・ イベントのキャプチャ
- ・ AMPコンソールからのイベント詳細のキャプチャ
- ・ ファイルに関する情報 ( ファイルの送信元および環境内にファイルが必要な理由 )
- ・ ファイル/プロセスがfalse positiveであると考えられる理由を説明する

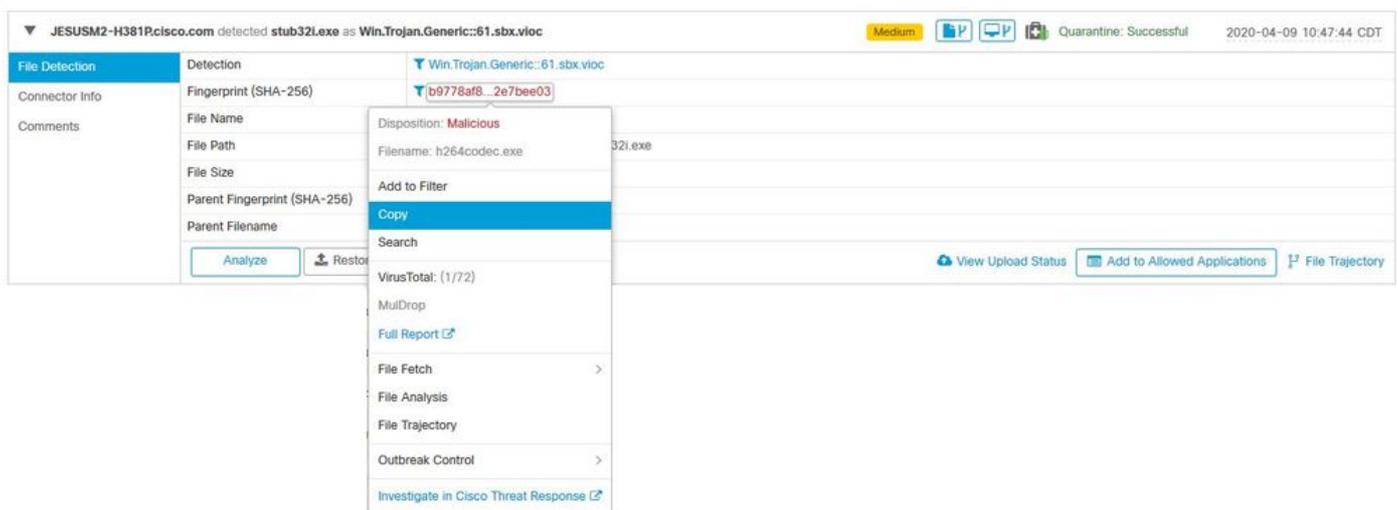
## エンドポイント用AMPの誤検出ファイル分析のトラブルシューティング

このセクションでは、Cisco TACでFalse Positiveチケットをオープンするために必要なすべての詳細を取得するために使用できる情報を提供します。

### ファイルSHA 256ハッシュ

ステップ1:SHA 256ハッシュを取得するには、[AMP Console] > [Dashboard] > [Events]に移動します。

ステップ2:[Alert Event]を選択し、SHA256をクリックし、図に示すように[Copy]を選択します。

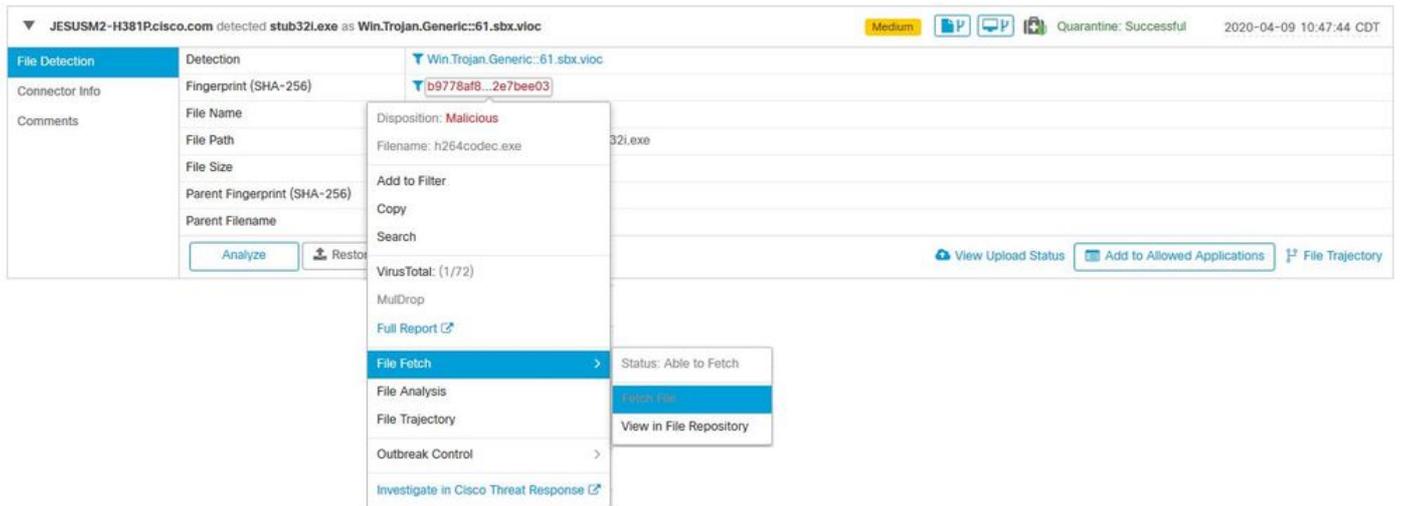


### ファイルサンプルコピー

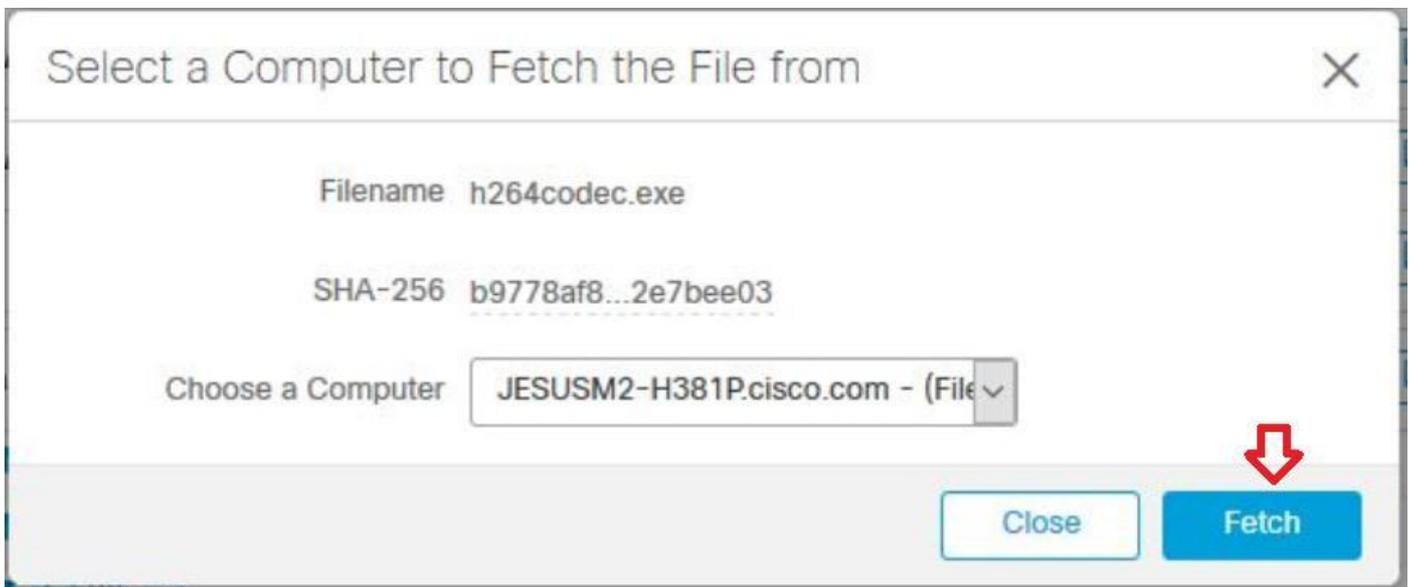
ステップ1:AMPコンソールからファイルサンプルを取得し、[AMP Console] > [Dashboard] > [Events]に移動します。

ステップ2:[Alert Event]を選択し、SHA256をクリックし、[File Fetch] > [File Fetch] に移動します

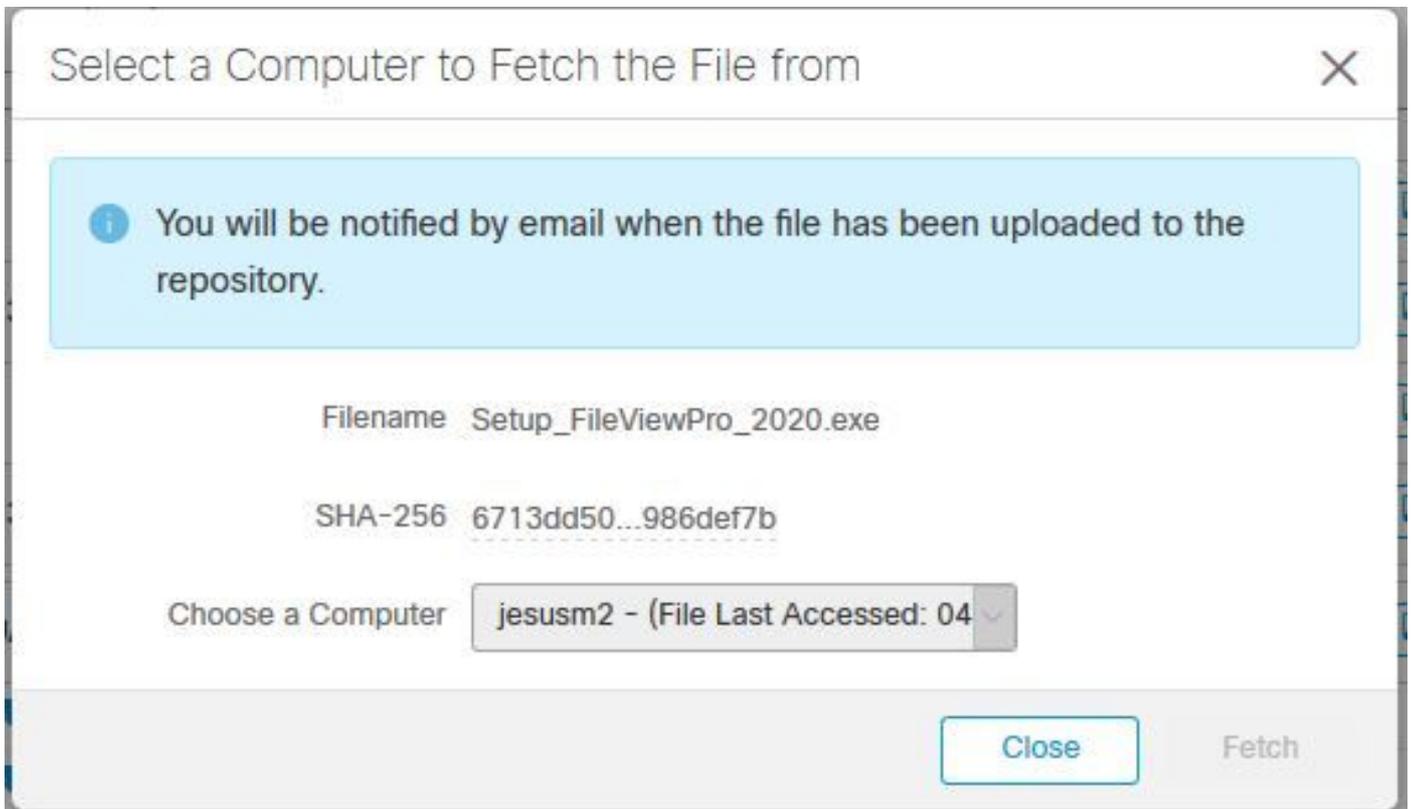
( 図を参照 )。



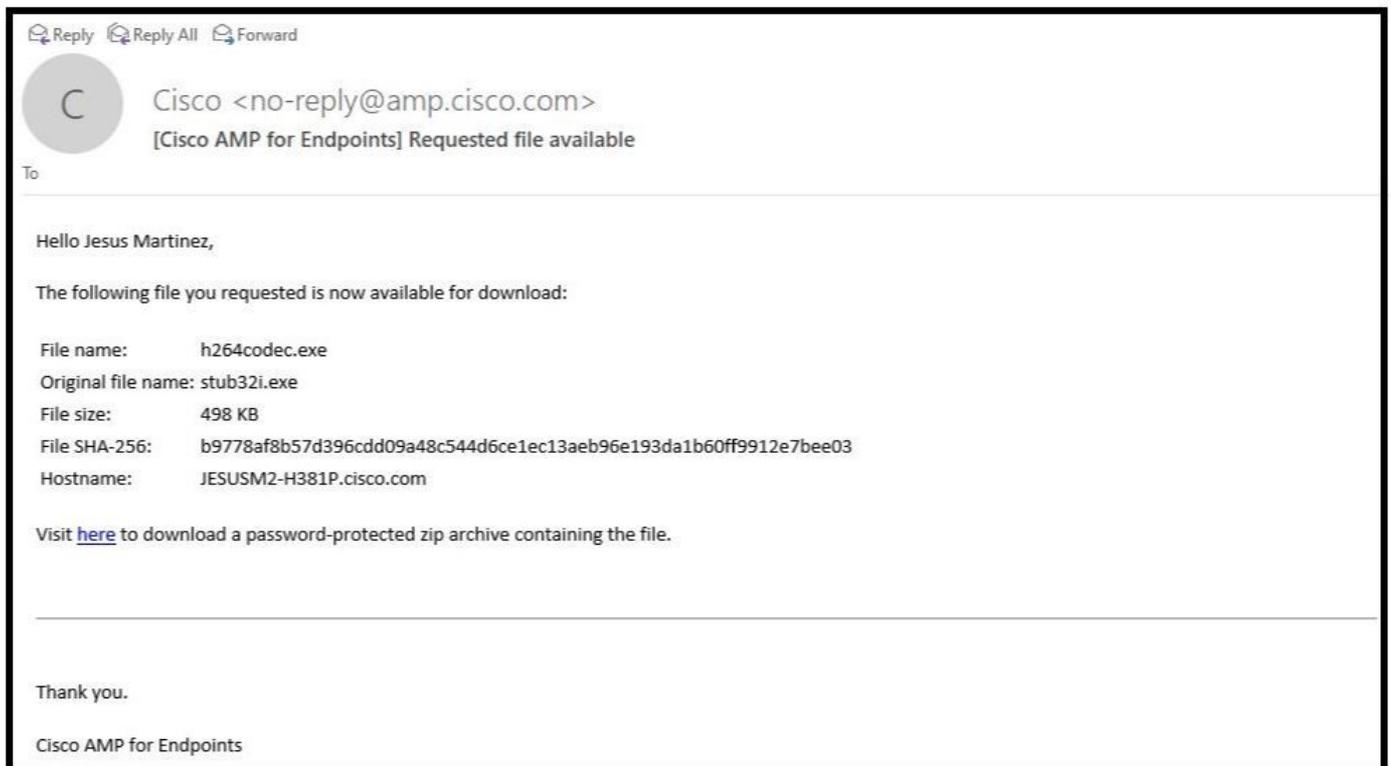
ステップ3 : ファイルが検出されたデバイスを選択し、図に示すようにFetchをクリックします(デバイスをオンにする必要がある)。



ステップ4 : 図に示すように、メッセージが表示されます。



数分後に、ファイルをダウンロードできるときに、図に示すように電子メール通知が送信されます。



ステップ5:[AMP Console] > [Analysis] > [File Repository]に移動し、ファイルを選択し、図に示すように[Download]をクリックします。

[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)	<b>b9778af8...2e7bee03</b>
File Size	498 KB
Computer	JESUSM2-H381P.cisco.com

ステップ6:[Notification]ボックスが表示されたら、図に示すように[Download]をクリックし、ファイルをZIPファイルにダウンロードします。

**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**

## AMPコンソールからのアラートイベントキャプチャ

ステップ1:[AMP Console] > [Dashboard] > [Events]に移動します。

ステップ2 : アラートイベントを選択し、図に示すようにキャプチャを取得します。

▼ 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

## AMPコンソールからのイベント詳細キャプチャ

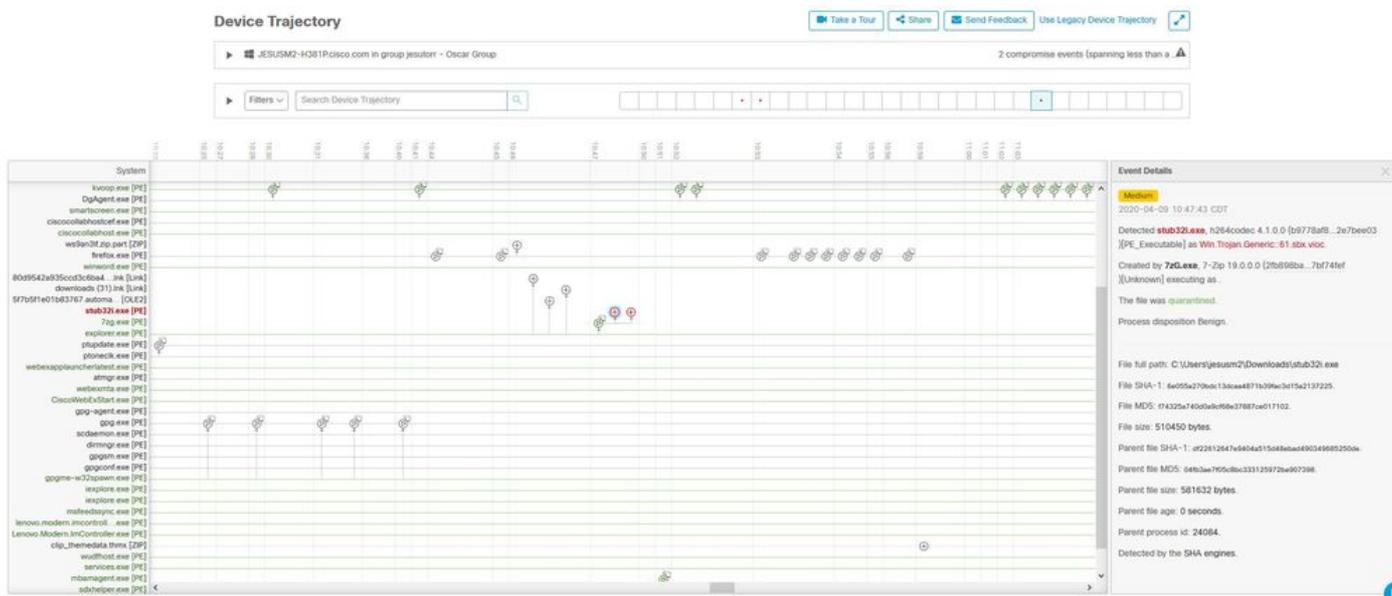
ステップ1:[AMP Console] > [Dashboard] > [Events]に移動します。

ステップ2:[Alert Event]を選択し、図に示すように[Device Trajectory]オプションをクリックします。



The screenshot shows the event details for a detected file named stub32i.exe. The detection is categorized as Win.Trojan.Generic:61.sbx.vioc with a medium severity. The file path is C:\Users\jesusm2\Downloads\stub32i.exe. The parent file is 7zG.exe. At the top right, there are buttons for 'View Upload Status', 'Add to Allowed Applications', and 'File Trajectory'. A red arrow points to the 'File Trajectory' button.

図に示すように、Device Trajectoryの詳細にリダイレクトされます。



The screenshot displays the 'Device Trajectory' interface, which shows a timeline of system events. The 'Event Details' panel on the right is open, providing information about the detected file stub32i.exe. The details include the file path, SHA-1 and SHA-256 hashes, file size, parent file information, and the detection method (SHA engines). The file was quarantined and its process disposition is benign.

ステップ3 : 図に示すように、[Event Details]ボックスをキャプチャします。

**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.

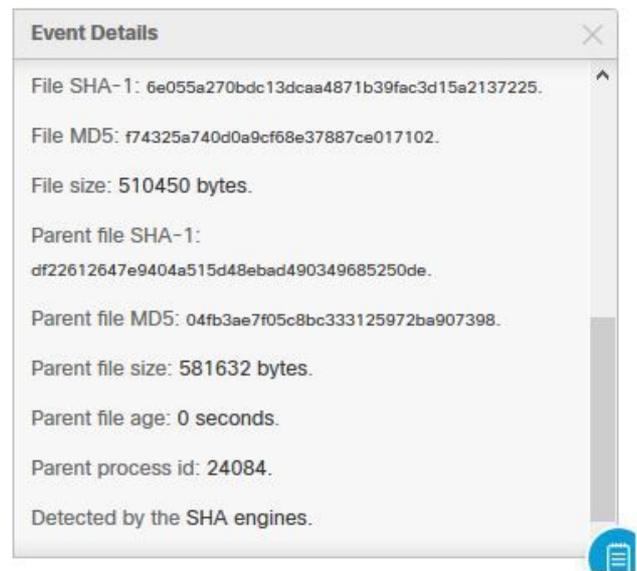
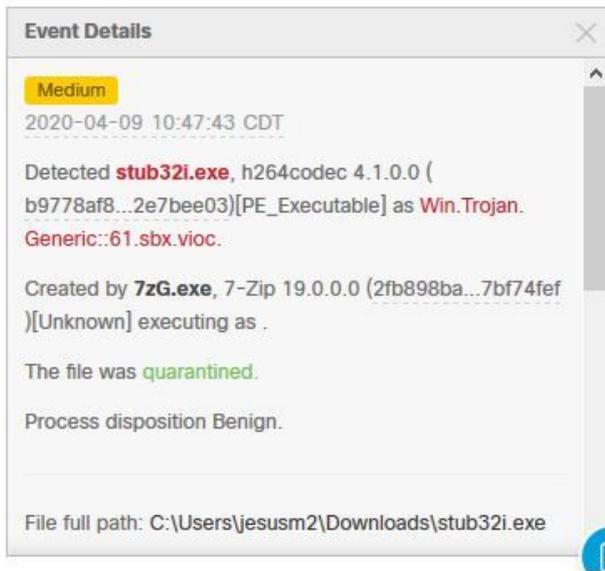
Parent file age: 0 seconds.

Parent process id: 24084.

Detected by the SHA engines.



ステップ4：必要に応じて下にスクロールし、キャプチャを取得して、図に示すすべてのイベント詳細情報を取得します。



## ファイルに関する情報

- ファイルの入手元に関する情報。
- ファイルがWebサイトから取得されている場合は、Web URLを共有します。
- ファイルの説明を少し共有し、ファイルの機能を説明します。

## 説明

- ファイルプロセスがfalse positiveであると考えられる理由は何ですか。
- ファイルに信頼する理由を共有します。

## 情報の提供

- すべての詳細を収集したら、<https://cway.cisco.com/csc/>に要求されたすべての情報をアップロードします。
- サービスリクエスト番号を参照してください。

## 結論

シスコは常にAMP for Endpointテクノロジーの脅威インテリジェンスの改善と拡張に努めていますが、AMP for Endpointソリューションが誤ってアラートをトリガーした場合は、環境への影響を防ぐために何らかの措置を講じることができます。このドキュメントでは、False Positiveの問題に関してCisco TACでケースをオープンするために必要なすべての詳細を入手するためのガイドラインを提供します。診断チームのファイル分析に基づいて、AMPコンソールでトリガーされるアラートイベントを停止するようにファイルの性質を変更するか、またはCisco TACが適切な修正を提供し、環境内で問題なくファイル/プロセスを実行できます。