Troubleshoot False Positive File Analysis Events in Cisco Secure Endpoint

Contents

Introduction

This document describes how to collect a False Positive file analysis in Cisco Secure Endpoint.

Prerequisites

Requirements

Cisco recommends that you have knowledge of the Secure Endpoint Console dashboard.

Components Used

The information in this document is based on Secure Endpoint version 7. X.X and later.

Note: An account with administrator privileges is needed.

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, ensure that you understand the potential impact of any command.

Background Information

Secure Endpoints can generate excessive alerts on a certain file/process/Secure Hash Algorithm (SHA) 256. If you suspect any False Positive detections in your network, you can contact the Cisco Technical Assistance Center (TAC), and the Diagnostic Team proceeds to do a deeper file analysis. When you contact Cisco

TAC, you need to provide this information:

- File SHA 256 hash
- File sample copy
- Alert Event capture from Secure Endpoint Console
- Event Details captured from Secure Endpoint Console
- Information about the file (where it came from and why it needs to be in the environment)
- Explain why you believe the file/process can be a false positive

Cisco always strives to improve and expand the threat intelligence for Secure Endpoint technology, however, if your Secure Endpoint solution triggers an alert erroneously, you can take some actions in order to prevent any further impact to your environment. This document provides a guideline to get all required details to open a case with Cisco TAC with regards to a False Positive issue. Based on the Diagnostic Team file analysis, the file disposition can change to stop the Alert Events triggered on Secure Endpoint Console or Cisco TAC can provide the proper fix to let run the file/process without issues in your environment.

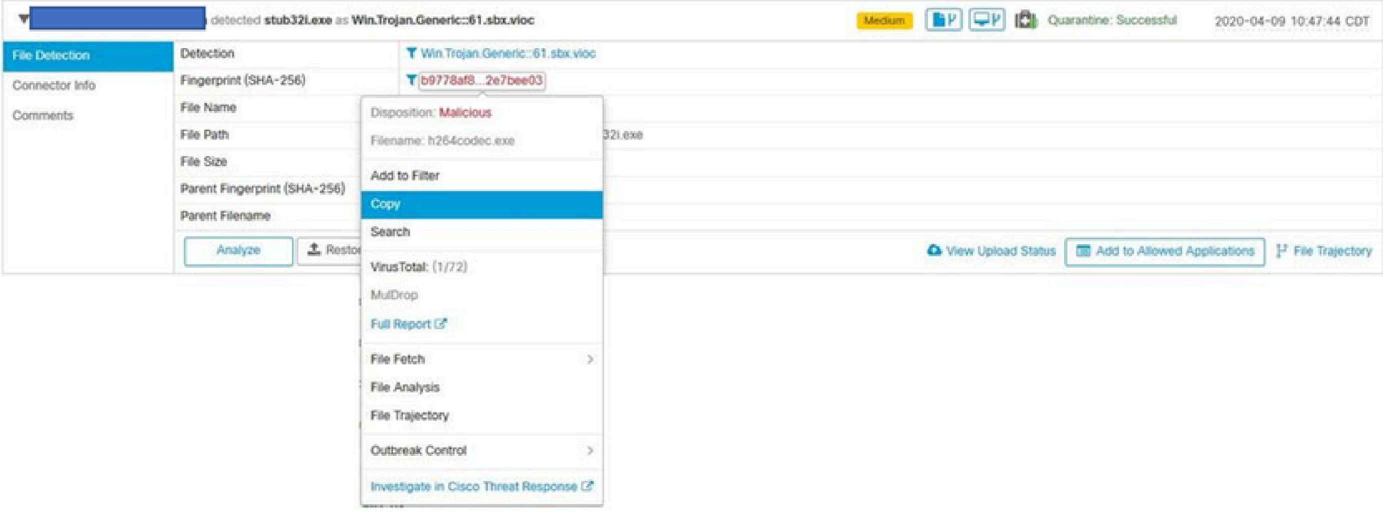
Troubleshoot False Positive File Analysis in Secure Endpoint

This section provides the information you can use to get all details needed to open a False Positive ticket with Cisco TAC.

1. File SHA 256 Hash

Step 1. In order to get the SHA 256 hash, navigate to**Secure Endpoint Console** > **Dashboard** > **Events.**

Step 2. Select the**Alert Event** andclick on the**SHA256**and select**Copy**as shown in the image.



[redacted] detected stub32i.exe as Win.Trojan.Generic::61.sbx.vioc

Medium

Quarantine: Successful

2020-04-09 10:47:44 CDT

Detection	Win.Trojan.Generic::61.sbx.vioc
Fingerprint (SHA-256)	b9778af8...2e7bee03
File Name	
File Path	32i.exe
File Size	
Parent Fingerprint (SHA-256)	
Parent Filename	

Disposition: Malicious

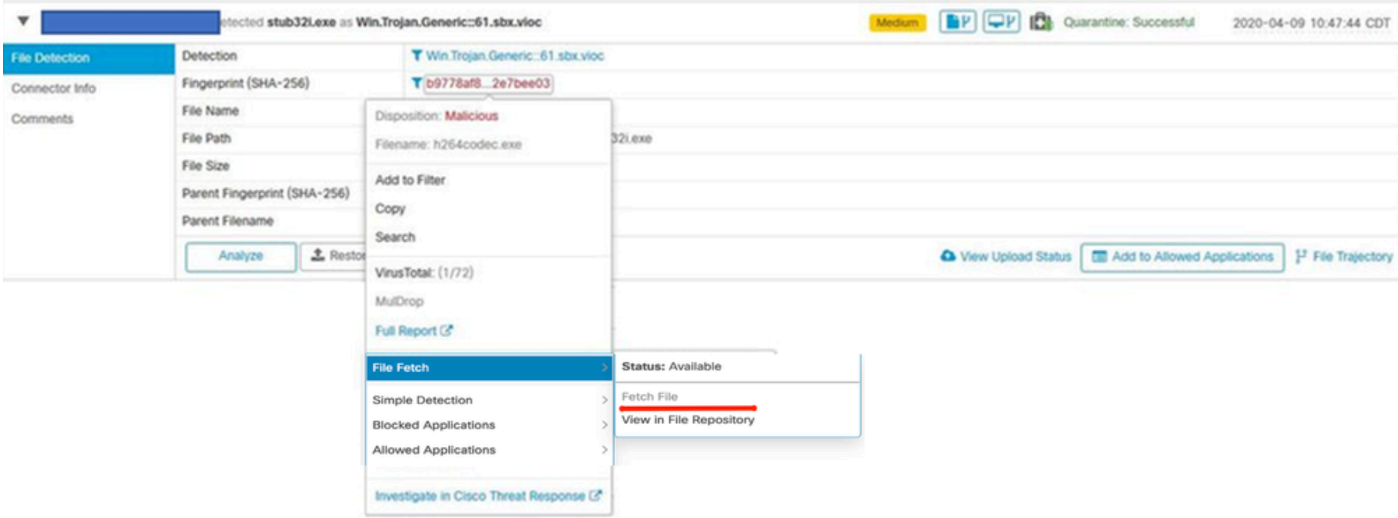
Filename: h264codec.exe

VirusTotal: (1/72)

2. File Sample Copy

Step 1. You can get the file sample from Secure Endpoint Console, navigate to**Secure Endpoint Console** > **Dashboard** > **Events.**

Step 2. Select the**Alert Event** , click on the**SHA256**and navigate to**File Fetch** > **Fetch File**as shown in the image.



[redacted] etected stub32i.exe as Win.Trojan.Generic::61.sbx.vioc

Medium · Quarantine: Successful · 2020-04-09 10:47:44 CDT

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

Fingerprint (SHA-256): b9778af8...2e7bee03

File Name

File Path: 32i.exe

File Size

Parent Fingerprint (SHA-256)

Parent Filename

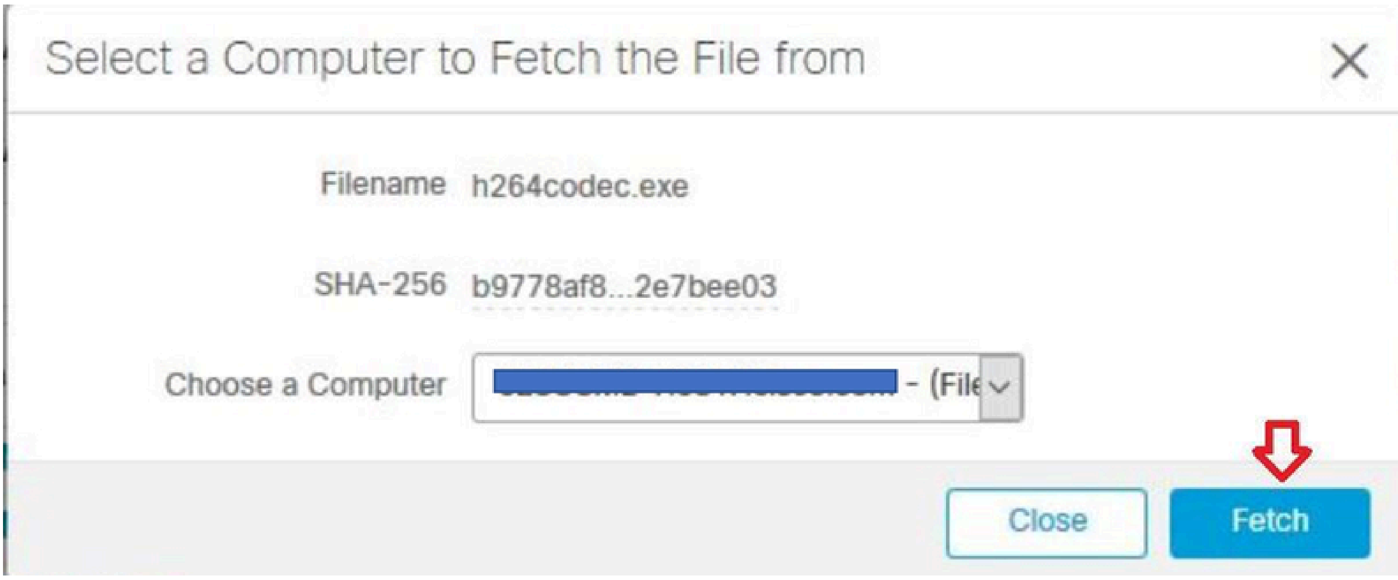
Disposition: Malicious

Filename: h264codec.exe

VirusTotal: (1/72)

Status: Available

Step 3. Select the device where the file was detected and click on**Fetch**as shown in the image.



Select a Computer to Fetch the File from

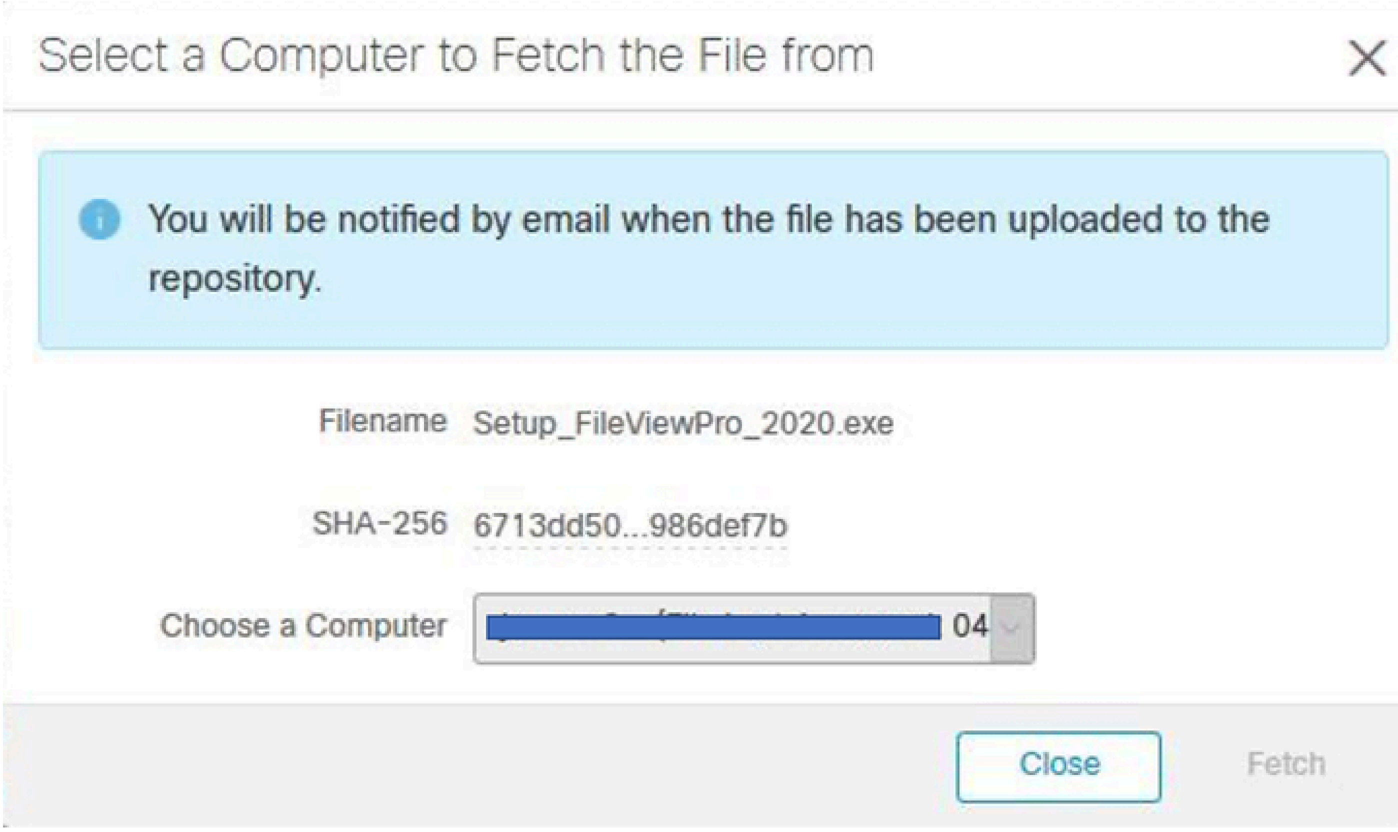
Filename h264codec.exe

SHA-256 b9778af8...2e7bee03

Choose a Computer [redacted] - (File

Note: Device must be ON, in order to get the sample file successfully.

Step 4. You receive the messageas shown in the image.



Select a Computer to Fetch the File from

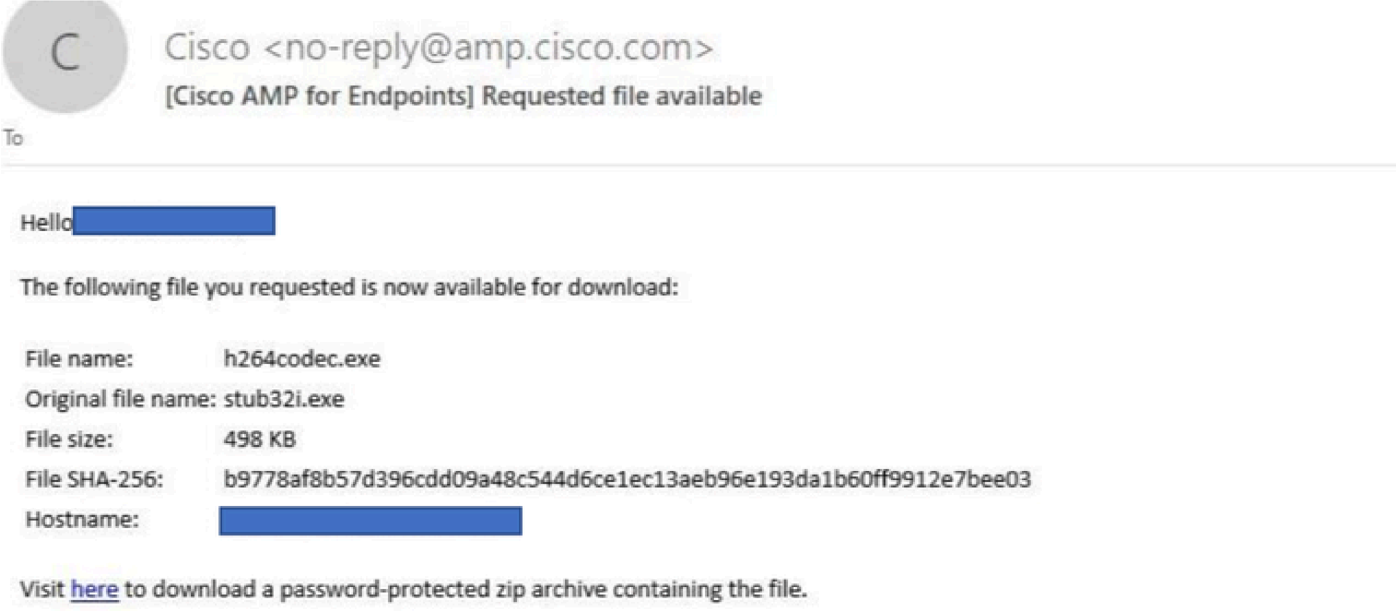
You will be notified by email when the file has been uploaded to the repository.

Filename Setup_FileViewPro_2020.exe

SHA-256 6713dd50...986def7b

Choose a Computer [redacted] 04

After a few minutes, you receive an email notification when the file is available to download as shown in the image.



Cisco <no-reply@amp.cisco.com>

[Cisco AMP for Endpoints] Requested file available

To

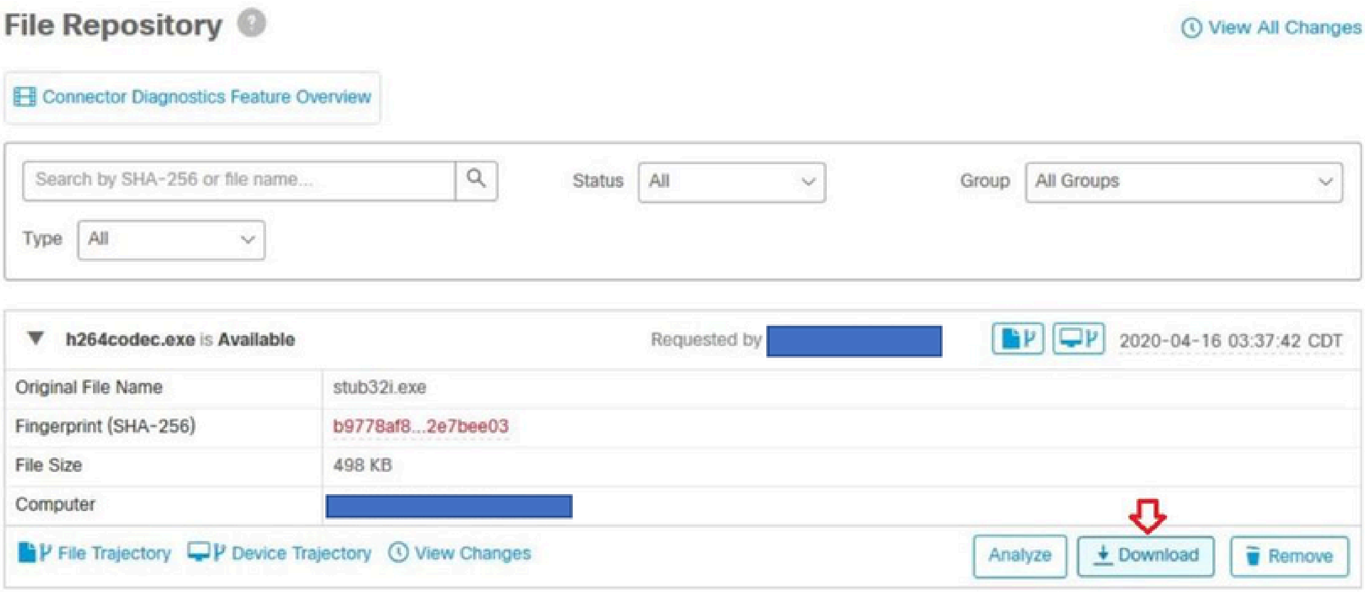
Hello [redacted]

The following file you requested is now available for download:

File name:	h264codec.exe
Original file name:	stub32i.exe
File size:	498 KB
File SHA-256:	b9778af8b57d396cdd09a48c544d6ce1ec13aeb96e193da1b60ff9912e7bee03
Hostname:	[redacted]

Visit here to download a password-protected zip archive containing the file.

Step 5. Navigate to **Secure Endpoint Console** > **Analysis** > **File Repository**and select**Download**as shown in the image.



File Repository

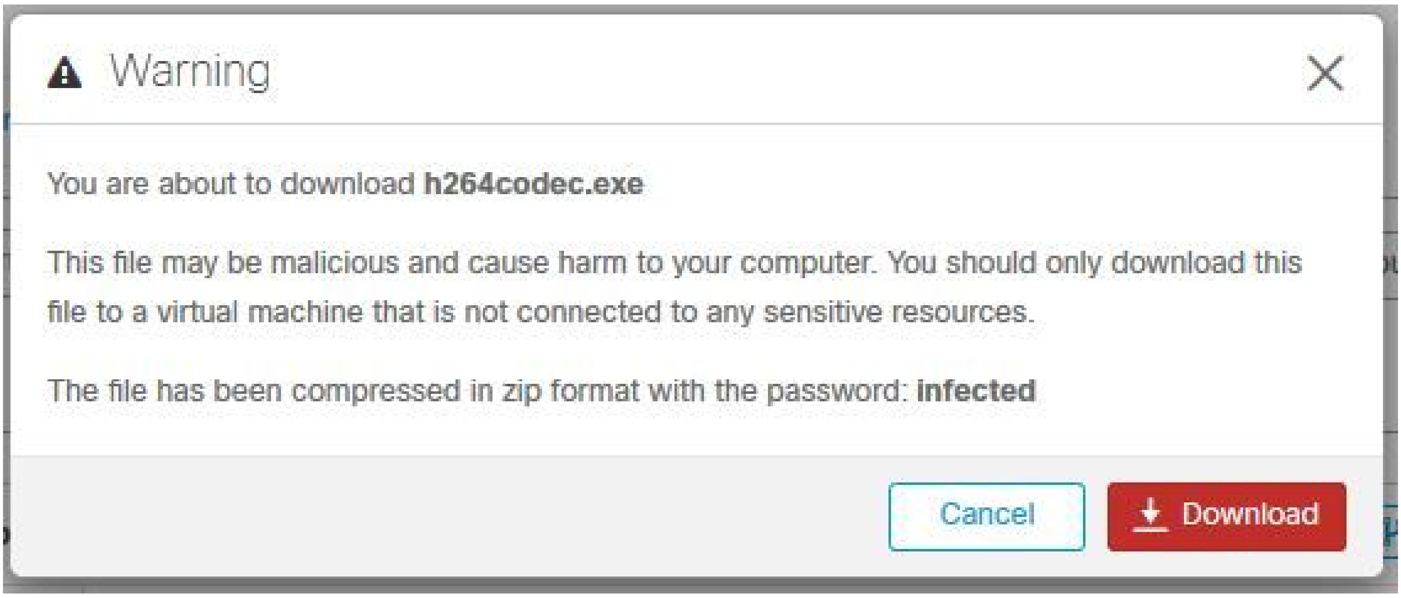
Connector Diagnostics Feature Overview

Search by SHA-256 or file name... | Status: All | Group: All Groups | Type: All

h264codec.exe is **Available** — Requested by [redacted] — 2020-04-16 03:37:42 CDT

Original File Name	stub32i.exe
Fingerprint (SHA-256)	b9778af8...2e7bee03
File Size	498 KB
Computer	[redacted]

Step 6. A notification box appears, click on **Download**, as shown in the image, and the file is downloaded as a ZIP file.



Warning

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

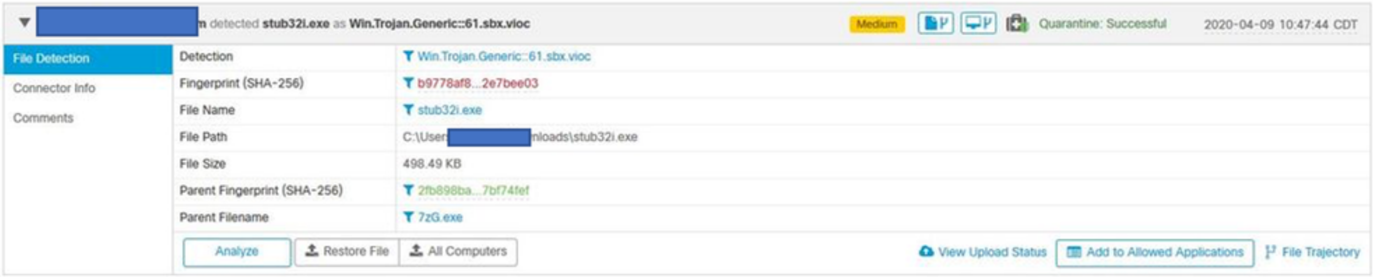
This file may be malicious and cause harm to your computer. You should only download this file to a virtual machine that is not connected to any sensitive resources.

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

3. Alert Event Capture from Secure Endpoint Console

Step 1. Navigate to**Secure Endpoint Console** > **Dashboard** > **Events.**

Step 2. Select the**Alert Event**and take the capture as shown in the image.



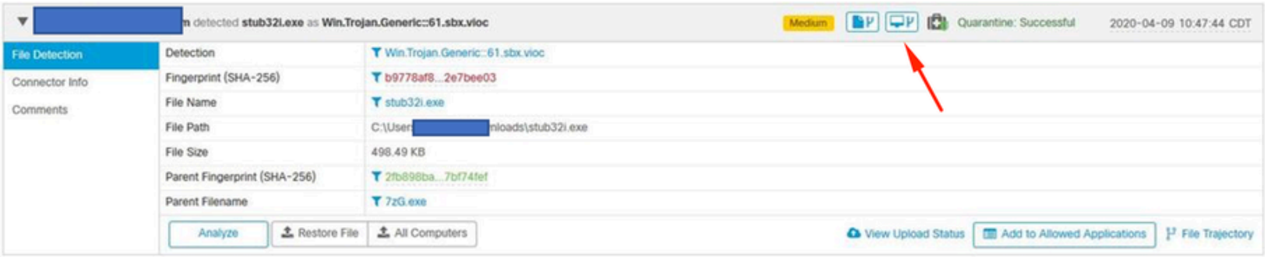
[redacted]n detected **stub32i.exe** as **Win.Trojan.Generic::61.sbx.vioc** — Medium — Quarantine: Successful — 2020-04-09 10:47:44 CDT

Detection	Win.Trojan.Generic::61.sbx.vioc
Fingerprint (SHA-256)	b9778af8...2e7bee03
File Name	stub32i.exe
File Path	C:\User[redacted]nloads\stub32i.exe
File Size	498.49 KB
Parent Fingerprint (SHA-256)	2fb898ba...7bf74fef
Parent Filename	7zG.exe

4. Event Details Capture from Secure Endpoint Console

Step 1. Navigate to**Secure Endpoint Console** > **Dashboard** > **Events.**

Step 2. Select the Alert Event and click on**Device Trajectorythe** option as shown in the image.



[redacted] detected **stub32i.exe** as **Win.Trojan.Generic::61.sbx.vioc**

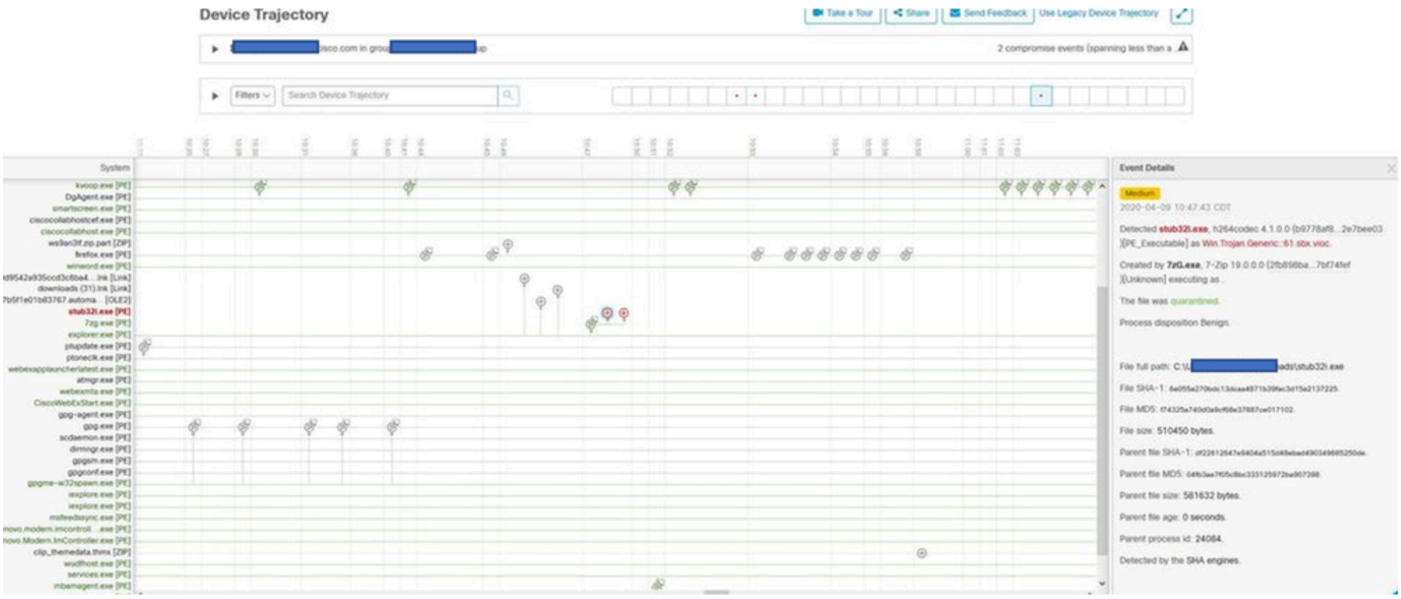
Medium

Quarantine: Successful

2020-04-09 10:47:44 CDT

Detection	Win.Trojan.Generic::61.sbx.vioc
Fingerprint (SHA-256)	b9778af8...2e7bee03
File Name	stub32i.exe
File Path	C:\User[redacted]nloads\stub32i.exe
File Size	498.49 KB
Parent Fingerprint (SHA-256)	2fb898ba...7bf74fef
Parent Filename	7zG.exe

It redirects to**Device Trajectory**details as shown in the image.



Device Trajectory

[redacted]isco.com in grou[redacted]up

2 compromise events (spanning less than a ...

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:\U[redacted]ads\stub32i.exe

File SHA-1: 6e055a270bdc13dcaa4871b39fec3d15e2137225.

File MD5: f74325a740d0a9cf68e37887ce017102.

File size: 510450 bytes.

Parent file SHA-1: df22612647e9404a515d48ebad4903496685250de.

Parent file MD5: 04fb3ae7f05c8bc333125972be907398.

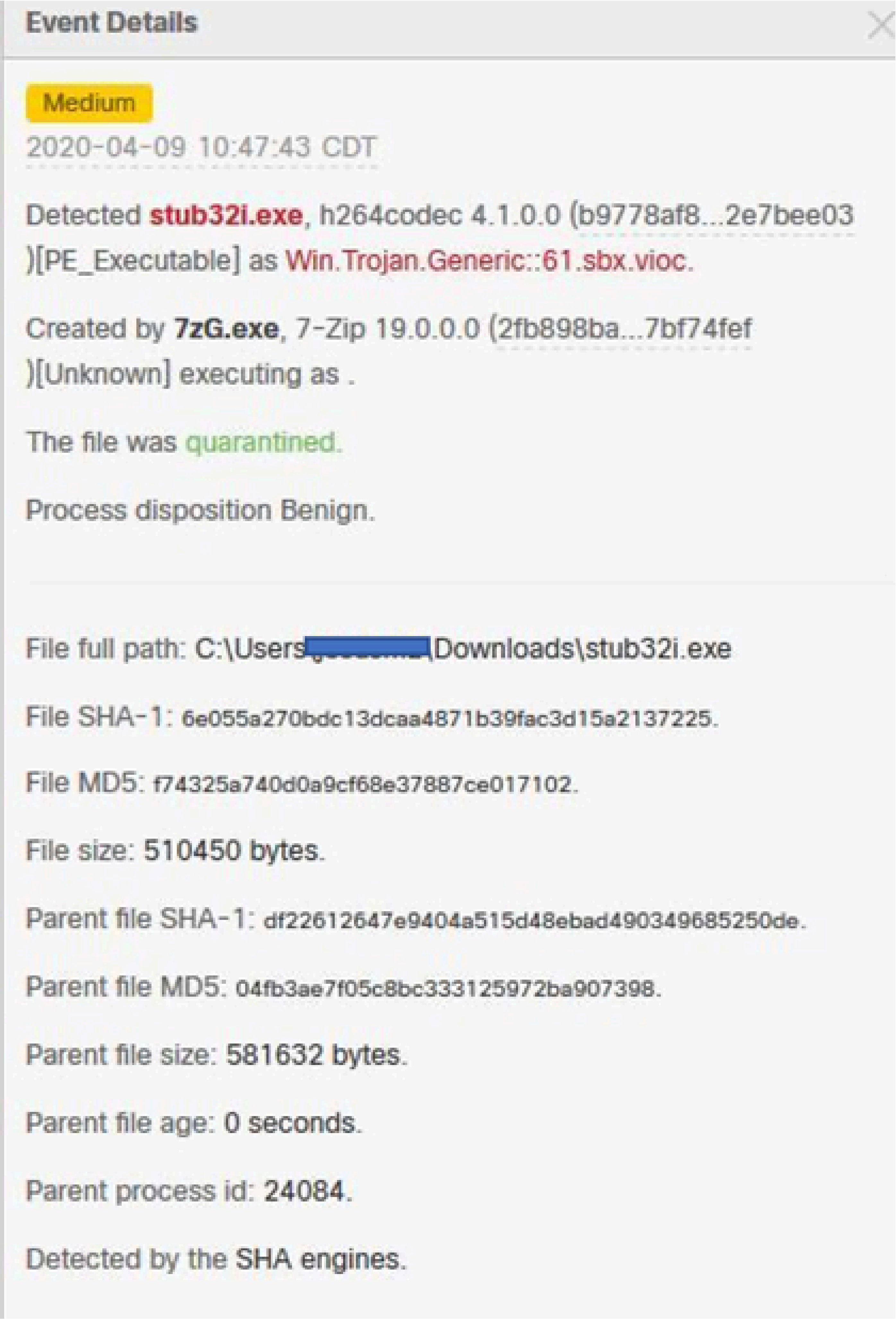
Parent file size: 581632 bytes.

Parent file age: 0 seconds.

Parent process id: 24084.

Detected by the SHA engines.

Step 3. Take a capture of**Event Details**box as shown in the image.



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[redacted]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.

Step 4. If it is necessary, scroll down and take some captures to get all **Event Details**.