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 Cáptura 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.

File Detection	Detection	▼ Win.Trojan.Generic::61.sbx.vioc		
Connector Info	Fingerprint (SHA-256)	¥b9778af82e7bee03		
Comments	File Name	Disposition: Malicious		
	File Path	Filename: h264codec.exe Add to Filter	2i.exe	
	File Size Parent Fingerprint (SHA-256)			
	Parent Filename	Сору		
	Analyze 2 Resto	VirusTotal: (1/72)	View Uplos	ad Status 🔲 Add to Allowed Applications 🕴 🖓 File Trajectory
		MulDrop Full Report (2*		
		File Fetch >	Status: Able to Fetch	
		File Analysis	(Education)	
		Outbreak Control >	View in File Repository	
		Investigate in Cisco Threat Response I		

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.

Select a Computer to	o Fetch the File from	×
Filename	h264codec.exe	
SHA-256	b9778af82e7bee03	
Choose a Computer	JESUSM2-H381P.cisco.com - (File ~	
	Close	Fetch

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

Select a Computer to	Fetch the File from	X
You will be notified repository.	by email when the file has been uploaded to the	
Filename	Setup_FileViewPro_2020.exe	
SHA-256	6713dd50986def7b	
Choose a Computer	jesusm2 - (File Last Accessed: 04	
	Close Fetc	h

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

Q Reply Q Re	oly All 🔓 Forward
C	Cisco <no-reply@amp.cisco.com> [Cisco AMP for Endpoints] Requested file available</no-reply@amp.cisco.com>
Hello Jesus M	artinez,
The following	file you requested is now available for download:
File name:	h264codec.exe
Original file n	ame: stub32i.exe
File size:	498 KB
File SHA-256:	b9778af8b57d396cdd09a48c544d6ce1ec13aeb96e193da1b60ff9912e7bee03
Hostname:	JESUSM2-H381P.cisco.com
Visit <u>here</u> to d	ownload a password-protected zip archive containing the file.
2	
Thank you.	
Cisco AMP for	Endpoints

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

File Repository 🔘					
E Connector Diagnostics Feat	ure Overview				
Search by SHA-256 or file n Type All	ame Q	Status All	~	Group	All Groups
h264codec.exe is Available	ble	Requested b	y Jesus Martinez		भ 🗖 भ
Original File Name	stub32i.exe				

h264codec.exe is Available		Requested by Jesus Martinez	4 1	2020-04-16 03:37:42 CDT
Original File Name	stub32i.exe			
Fingerprint (SHA-256)	b9778af82e7bee03			
File Size	498 KB			
Computer	JESUSM2-H381P.cisco.com			л
P File Trajectory	ajectory ① View Changes		Analyze	Download Remove

() View All Changes

V

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

Warning	×
You are about to download h264codec.exe	
This file may be malicious and cause harm to your computer. You should on	ly 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	
Cancel	+ Download

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-H381	P.cisco.com detected stub32i.exe as Win.Tre	jan.Generic::61.sbx.vioc	Medium	DT
File Detection	Detection	▼ Win.Trojan.Generic::61.sbx.vioc		
Connector Info	Fingerprint (SHA-256)	T b9778af82e7bee03		
Comments	File Name	▼ stub32i.exe		
	File Path	C:\Users\jesusm2\Downloads\stub32i.exe		
	File Size	498.49 KB		
	Parent Fingerprint (SHA-256)	▼ 2fb898ba7bf74fef		
	Parent Filename	▼ 7zG.exe		
	Analyze 🕹 Restore File	2 All Computers	View Upload Status Add to Allowed Applications 1 ³ File Trajec	tory

Captura de detalhes do evento do console AMP

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

			$\mathbf{\hat{C}}$
▼ JESUSM2-H381	P.cisco.com detected stub32i.exe as Win.T	rojan.Generic::61.sbx.vioc	Medium
File Detection	Detection	▼ Win.Trojan.Generic::61.sbx.vioc	
Connector Info	Fingerprint (SHA-256)	T b9778af82e7bee03	
Comments	File Name	▼ stub32i.exe	
	File Path	C:\Users\jesusm2\Downloads\stub32i.exe	
	File Size	498.49 KB	
	Parent Fingerprint (SHA-256)	▼ 2fb898ba7bf74fef	
	Parent Filename	▼ 7zG.exe	
	Analyze 🕹 Restore Fi	e 🕹 All Computers	▲ View Upload Status 🛛 🕅 Add to Allowed Applications 🛛 🖓 File Trajectory

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 (b9778af82e7bee03))[PE_Executable] as Win.Trojan.Generic::61.sbx.vioc.
Created by 7zG.exe , 7-Zip 19.0.0.0 (2fb898ba7bf74fef)[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.

Event Details	K Event Details	×
Medium	 File SHA-1: 6e055a270bdc13dcaa4871b39fac 	:3d15a2137225.
2020-04-09 10:47:43 CDT	File MD5: f74325a740d0a9cf68e37887ce0171	02.
Detected stub32i.exe, h264codec 4.1.0.0 (b9778af82e7bee03)[PE Executable] as Win.Trojan.	File size: 510450 bytes.	
Generic::61.sbx.vioc.	Parent file SHA-1:	
Created by 7zG.exe, 7-Zip 19.0.0.0 (2fb898ba7bf74fef	df22612647e9404a515d48ebad490349685250d	le.
[Unknown] executing as .	Parent file MD5: 04fb3ae7f05c8bc333125972	ba907398.
The file was quarantined.	Parent file size: 581632 bytes.	
Process disposition Benign.	Parent file age: 0 seconds.	
	Parent process id: 24084.	
File full path: C:\Users\jesusm2\Downloads\stub32i.exe	Detected by the SHA engines.	

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.