Probleemoplossing bij fout-positieve bestandsanalyse in Advanced Malware Protection voor endpoints

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Probleemoplossing bij fout-positieve bestandsanalyse in Advanced Malware Protection voor endpoints Bestand SHA 256 Hash Kopie bestand voorbeeld Alert Event Capture van AMP-console Event Details Capture of AMP-console Informatie over het bestand verklaring Informatie verstrekken Conclusie

Inleiding

Dit document beschrijft hoe u een foute positieve bestandsanalyse kunt verzamelen in Advanced Malware Protection (AMP) voor endpoints.

Bijgedragen door Jezus Javier Martinez, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze onderwerpen:

- AMP-console dashboard
- Een account met administratorrechten

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Advanced Malware Protection voor endpoints, versie 6.X.X en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

AMP voor endpoints kan buitensporige waarschuwingen genereren op een bepaald bestand/proces/Secure Hash Algorithm (SHA) 256. Als u foutieve positieve detecties in uw netwerk vermoedt, kunt u contact opnemen met het Cisco Technical Assistance Center (TAC) en gaat het diagnostische team verder om een diepere bestandsanalyse uit te voeren. Wanneer u contact opneemt met Cisco TAC, moet u deze informatie verstrekken:

- · File SHA 256 shash
- Kopie voor bestandstaal
- · Waarschuwingsgebeurtenissen bij opname in AMP-console
- · Event Details van AMP-console
- Informatie over het bestand (waar het vandaan komt en waarom het in de omgeving moet zijn)
- · Leg uit waarom u gelooft dat het bestand/proces verkeerd-positief kan zijn

Probleemoplossing fout positieve bestandsanalyse in Advanced Malware Protection voor endpoints

Deze sectie verschaft informatie die u kunt gebruiken om alle informatie te verkrijgen die nodig is om een vals positief ticket met Cisco TAC te openen.

Bestand SHA 256 Hash

Stap 1. Ga voor de SHA 256-hash naar **AMP-console > Dashboard > Events.**

Stap 2. Selecteer de **gebeurtenis** in het **alarmsignaal**, klik op **SHA256** en selecteer **Kopie** zoals in de afbeelding.

File Detection	Detection	T Win.Trojan.Generic::61.sbx.vio	50 S
Connector Info	Fingerprint (SHA-256)	T b9778af82e7bee03	
Comments	File Name	Disposition: Malicious	
	File Path	Filename: h264codec.exe	321.exe
	File Size	Add to Filter	
	Parent Fingerprint (SHA-256)	Add to Filter	
	Parent Filename	Сору	
	Analyze 🕹 Restor	VirusTotal: (1/72)	▲ View Upload Status Add to Allowed Applications 1 ² File Trajectory
		MulDrop Full Report 🕫	
		File Fetch File Analysis File Trajectory	2
		Outbreak Control	5

Kopie bestand voorbeeld

Stap 1. U kunt de bestandssteekproef van AMP-console ophalen, navigeer naar **AMP-console > Dashboard > Events.**

Stap 2. Selecteer de **gebeurtenis** in het **alarmsignaal**, klik op **SHA256** en navigeer naar **bestandsgrootte > bestandsgrootte** zoals in de afbeelding.

File Detection	Detection	T Win.Trojan.Generic::61.sbx.vioc						
Connector Info	Fingerprint (SHA-256)	T b9778af82e7bee03						
Comments	File Name	Disposition: Malicious						
	File Path	Filename: h264codec.exe	32i.exe					
	File Size	Add to Filter						
	Parent Fingerprint (SHA-256)	Add to Filter						
	Parent Filename	Сору						
	Analyze 🚨 Resto	VirusTotal: (1/72)	▲ View Upload Status 🛛 🔤 Add to Allowed Applications 👌 🖓 File Tr					
		MulDrop						
		Full Report 2*						
		File Fetch >	Status: Able to Fetch					
		File Analysis	Exteth fair					
		File Trajectory	View in File Repository					
		Outbreak Control						
		Investigate in Cisco Threat Response	s					

Stap 3. Selecteer het apparaat waar het bestand is gedetecteerd en klik op **Fetch** zoals in de afbeelding (het apparaat moet **ingeschakeld** zijn) zoals in de afbeelding.

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

Stap 4. U ontvangt het bericht zoals in de afbeelding.

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

Na een paar minuten ontvangt u een e-mailbericht wanneer het bestand kan worden gedownload zoals in de afbeelding wordt weergegeven.

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

Stap 5. Navigeer naar **AMP-console > Analysis > File Repository** en selecteer het bestand en klik op **Download** zoals in de afbeelding.

File Repository					
Connector Diagnostics Feature Overview					
Search by SHA-256 or file name	Q	Status	All	~	Group
Type All V					
h264codec.exe is Available			Requested by	Jesus Martinez	<u>ч</u>
Original File Name	ovo				

Search by SHA-256 or file n	ame Q	Status	All	~	Group	All Groups	~
Type All ~]						
h264codec.exe is Available	able		Requested b	by Jesus Martinez		P P 2020-04-10	5 03:37:42 CD1
Original File Name	stub32i.exe						
Fingerprint (SHA-256)	b9778af82e7bee03						
File Size	498 KB						
Computer	JESUSM2-H381P.cisco	o.com					

Stap 6. Het vakje voor melding verschijnt, klik op Downloaden, zoals in de afbeelding, en het bestand wordt gedownload in een ZIP-bestand.

A Warning	×
You are about to download h264codec.exe	
This file may be malicious and cause harm to your computer. You should onl	y 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
Cancel	🛨 Download

Alert Event Capture van AMP-console

Stap 1. Navigeer naar AMP-console > Dashboard > gebeurtenissen.

Stap 2. Selecteer de gebeurtenis in de waarschuwing en neem de opname zoals in de afbeelding.

JESUSM2-H381	P.cisco.com detected stub32i.exe as Win.Tro	jan.Generic::61.sbx.vioc	Medium P P Quarantine: Successful 2020-04-09 10:47:44 CDT
File Detection	Detection	Y 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 Trajectory

Event Details Capture of AMP-console

Stap 2. Selecteer de gewenste gebeurtenis en klik op de optie **Apparaattraject** zoals in de afbeelding.

			$\mathbf{\hat{C}}$
▼ JESUSM2-H381	P.cisco.com detected stub32i.exe as Win.	frojan.Generic::61.sbx.vioc	Medium P P Quarantine: Successful 2020-04-09 10:47:44 CDT
File Detection	Detection	T 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)	T 2fb898ba7bf74fef	
	Parent Filename	T 7zG.exe	
	Analyze 📩 Restore F	ile 🛃 All Computers	▲ View Upload Status ▲ Add to Allowed Applications ↓ File Trajectory

Het is gericht op de details van het apparaattraject zoals in de afbeelding.

		D	evic	e Traj	ector	1											0	M Take a	Tour	< Share	Ser	nd Fee	dback Use Legacy (levice Trajectory
		KE JESUSM2-H381Pclaso com in group jesulorr - Oscar Group										2 compromise events (spanning less than a .												
			•	iters ~	Search (evice Tr	njectory									• •								
1		10.27		ş.	10.01	1		10.43	10.44	10.45	1	10	10.50	10.91	10.52	1040		10.54	10.00	10.58	18	1001	11.00	
System																								Event Details
kvoop me (Pt) DgAgent.exe (Pt) smartscreen.exe (Pt) ciscocollabhostcef.exe (Pt)				¢				¢							\$\$ \$							(*****	Medant 2020-04-09 10:47:43 CDT
ciscocolabhost.exe (PE) ws9an3if.zip.part (ZP) firefox.exe (PE) w/nword.exe (PE)									ø	ø	₽					ð	đđ	88	88	ø				Detected stub32Laxe, h2t4codec 4.1.0.0 [bit778at8_2e7bee03 (PE_Executable] as Win.Trojan.Genenc::61.stox.vioc. Created by 7zG.exe, 7-Zip 19.0.0.0 (2tb698ba_7bt74fef
R0d9542a635ccd546ba4xmk [Link] 547b5f1e01b63367_automa_[CkL2] stub328.exe [PE] 7ag.exe [PE] explores.exe [PE]											¢ ¢	¢.	φ											(Uetrown) executing as. The file was quarantized. Process disposition Benign.
ptupdate exe [PE] ptonecik.exe [PE] webexapplauricherlatest.exe [PE] atrugr.exe [PE] webexonta.exe [PE]	9																							File full parts: C:\Userstjjesusm2\Downloads\stub32i.exe File 5H4-1: 6e055e219boct3scawEP1b09bc3e15e2137225
gog-agent.exe [PE] gog.exe [PE] scdaemon.exe [PE]		Ş		8	Ŷ	Ŷ		P																File MDS: tr4325x7403046x80x37887cx017102. File size: 510450 bytes.
dirmegr exer (PE) gogstm exer (PE) gogsonf exer (PE) gogsone-w32xpawn exer (PE)																								Parent file SHA-1: #22812647v6604x515568ebebe680366685250ee Parent file MDS: 6463ae7r65c8bc333125972be807398
iexplore.exe (PE) iexplore.exe (PE) maleedsaync.exe (PE)																								Parent file size: 581632 bytes. Parent file age: 0 seconds.
enovo modern imcontroli – exe (PE) enovo Modern imController exe (PE) clip_themedata thmx (ZIP) widthost.exe (PE)																				۲				Parent process ki: 24084. Detected by the SHA engines.
services.exe (PE) mbarnagent.exe (PE) sdxheiper.exe (PE) <														di?									,	*

Stap 3. Neem een opnamen van Event Details zoals in de afbeelding.

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.

Stap 4. Als dit nodig is, scrollen en neem dan een aantal opnamen om alle informatie over **gebeurtenissen** in de afbeelding te verkrijgen.



Informatie over het bestand

- Informatie over waar het bestand vandaan kwam.
- Als het bestand van een website komt, deelt u de URL van het web.
- Geef een kleine bestandsindeling en leg de bestandfunctie uit.

verklaring

- Waarom denk je dat het bestandsproces een fout-positief kan zijn?
- Geef de redenen aan waarom u op het bestand vertrouwt.

Informatie verstrekken

- Nadat u alle gegevens hebt verzameld, uploadt u alle gevraagde informatie naar <u>https://cway.cisco.com/csc/.</u>
- Zorg ervoor dat u het nummer van de serviceaanvraag raadpleegt.

Conclusie

Cisco streeft er altijd naar de bedreigingsintelligentie voor AMP voor endpoints-technologie te verbeteren en uit te breiden, maar als uw AMP voor Endpoints-oplossing onjuist een waarschuwing oproept, kunt u bepaalde acties ondernemen om verdere impact op uw omgeving te voorkomen. Dit document biedt een richtlijn om alle vereiste details te verkrijgen om een case met Cisco TAC te openen voor een valse positieve kwestie. Gebaseerd op de diagnostische teamanalyse kan de bestandsindeling veranderen om de waarschuwingsgebeurtenissen te stoppen die zijn geactiveerd op AMP Console of Cisco TAC kan de juiste oplossing bieden om het bestand/proces te laten uitvoeren zonder problemen in uw omgeving.