Risoluzione dei problemi relativi all'analisi dei file falsi positivi in AMP for Endpoints

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Risoluzione dei problemi relativi all'analisi dei file falsi positivi in AMP for Endpoints Hash SHA 256 file Copia di esempio file Acquisizione di eventi di avviso dalla console AMP Acquisizione di dettagli evento dalla console AMP Informazioni sul file Spiegazione Fornisci informazioni Conclusioni

Introduzione

In questo documento viene descritto come raccogliere un'analisi di file dei falsi positivi in Advanced Malware Protection (AMP) for Endpoints.

Contributo di Jesus Javier Martinez, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Dashboard della console AMP
- Account con privilegi di amministratore

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco AMP for Endpoints versione 6.X.X e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

AMP for Endpoints può generare avvisi eccessivi su un determinato file/processo/SHA (Secure Hash Algorithm) 256. Se si sospetta la presenza di falsi positivi nella rete, è possibile contattare il Cisco Technical Assistance Center (TAC), il team di diagnostica procederà a un'analisi più approfondita dei file. Quando si contatta Cisco TAC, è necessario fornire le seguenti informazioni:

·Hash file SHA 256
·Copia di esempio dei file
·Acquisizione di eventi di allarme dalla console AMP
·Acquisizione dei dettagli sugli eventi da AMP Console
·Informazioni sul file (origine e motivo della presenza nell'ambiente)
·Spiegare perché si ritiene che il file/processo possa essere un falso positivo

Risoluzione dei problemi relativi all'analisi dei file falsi positivi in AMP for Endpoints

In questa sezione vengono fornite informazioni che è possibile utilizzare per ottenere tutti i dettagli necessari per aprire un ticket Falso positivo con Cisco TAC.

Hash SHA 256 file

Passaggio 1. Per ottenere l'hash SHA 256, passare a AMP Console > Dashboard > Eventi.

Passaggio 2. Selezionare l'**evento di avviso**, fare clic su **SHA256** e selezionare **Copia** come mostrato nell'immagine.



Copia di esempio file

Passaggio 1. È possibile ottenere il file di esempio da AMP Console, passare a **AMP Console** > **Dashboard** > **Events.**

Passaggio 2. Selezionare l'evento di avviso, fare clic su SHA256 e passare a Recupero file> Recupero file come mostrato nell'immagine.

File Detection	Detection	T Win:Trojan:Generic::61.sbx.vioc						
Connector Info	Fingerprint (SHA-256)	¥ b9778af82e7bee03						
Comments	File Name	Disposition: Malicious						
	File Path	Filename: h264codec.exe	32i.exe					
	File Size Parent Fingerprint (SHA-256)	Add to Filter						
	Parent Filename	Сору						
	Analyze 🚨 Restor	Search VirusTotal: (1/72)	View Upload Status Add to Allowed Application					
		MulDrop Full Report G*	r.					
		File Fetch >	Status: Able to Fetch					
		File Analysis	Fotol: Hin					
		File Trajectory	View in File Repository					
		Outbreak Control >						
		Investigate in Cisco Threat Response 🖉						

Passaggio 3. Selezionare la periferica in cui è stato rilevato il file e fare clic su **Fetch**, come mostrato nell'immagine (la periferica deve essere accesa **)**, come mostrato nell'immagine.

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

Passaggio 4. Si riceve il messaggio come mostrato nell'immagine.

Select a Computer to	o 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 Feto	h

Dopo alcuni minuti si riceverà una notifica e-mail quando il file sarà disponibile per il download, come mostrato nell'immagine.

Q Reply Q 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 (lownload a password-protected zip archive containing the file.
Thank you.	
Cisco AMP fo	r Endpoints

Passaggio 5. Passare a **AMP Console > Analisi > Archivio file** e selezionare il file e fare clic su **Scarica** come mostrato nell'immagine.

File	Repository 🔘
------	--------------

Search by SHA-256 or file r	name Q	Status	All 🗸	Group	All Groups	~
Type All v]					
h264codec.exe is Avail	able		Requested by Jesus Martine	z 📔	P P 2020-04-16 ()3:37:42 CD1
Original File Name	stub32i.exe					
Fingerprint (SHA-256)	b9778af82e7bee03					
File Size	498 KB					

Passaggio 6. Viene visualizzata la finestra di notifica, fare clic su **Download** come mostrato nell'immagine, e il file viene scaricato in un file ZIP.

×
5
ad
6

Acquisizione di eventi di avviso dalla console AMP

Passaggio 1. Passare a AMP Console > Dashboard > Eventi.

Passaggio 2. Selezionare l'**evento di avviso** ed eseguire l'acquisizione come mostrato nell'immagine.

JESUSM2-H381	P.cisco.com detected stub32i.exe as Win.Tr	ojan.Generic::61.sbx.vioc	Medium	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	All Computers	Stew Upload Status Add to Allowed Applications	P File Trajectory					

Acquisizione di dettagli evento dalla console AMP

Passaggio 1. Passare a AMP Console > Dashboard > Eventi.

Passaggio 2. Selezionare l'evento di allarme e fare clic sull'opzione **Traiettoria periferica** come mostrato nell'immagine.

			$\mathbf{\hat{v}}$				
▼ JESUSM2-H38	P.cisco.com detected stub32i.exe as Win.1	rojan.Generic::61.sbx.vioc	Medium P P G Guarantine: 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	▼ 7zG.exe					
	Analyze & Restore F	le 🛃 All Computers	♦ View Upload Status 🔲 Add to Allowed Applications] [¹] File Trajectory				

Viene reindirizzato ai dettagli della traiettoria periferica, come mostrato nell'immagine.

		Device Trajectory										Take a Tour Share Share Send Feedback Use Legacy Device Trajectory											
	ESUSM2-H081Pcisco.com in group jesulorr - Oscar Group										2 compromise events (spanning less than a												
		► Filters ~] Search Device Trajectory						A															
		10.22		10.00	10.01		10.38	or of	10.44	70.45		ta.u	10.20	10.52	79.61		70.54	10.5m	10.58	11.00	11.02		
System																							Event Details
koop.exe (PE) DgAgent.exe (PE) imartizorees.exe (PE) ciscocolabhost.erf.exe (PE) ciscocolabhost.ere (PE) ws9an712.cip.exe (PE) trefox.exe (PE)				¢				¢	Ð	¢.				¢¢	ø	66	886	88	S		¢¢	***	A Measure 2020-04-09 10:47:43 COT Detected sh032kine, Dokkodec 4.1.0.0 (b0777882e7bee03 (I/PE_bases.tzP) as Win.Trajin.Genetic: 61.36x Vice. Caused at 9-26 mar. 2-27: 01.01.01 (2016)8982016.fef
8019542x635ccc3366ba4, with Unit downloads (31).hit (Unit 577b5f1e01b63767.automa, (OLE2) sebu32xax (PEI 7ag.ms (PEI explorer.em (PE) phpdate em (PE)	B										Ф Ф	@ [@]	₽										(Unkinown) executing as. The file was quarantimed. Process disposition Benign.
ptonecik exe (PE) webexapplauricherlatest.exe (PE) attrigr.exe (PE) webexinta.exe (PE) CiscolWebExStart.exe (PE) DiscolWebExStart.exe (PE)																							File full path: C:\UserSijesusm2\DownloadSijstub32i.exe File 394-11 6e05s270set13exex#811s09ec3e15s215725. File MDS: rk325s74ostalest8e31887ce017102.
gog exe (PE) scdaemon exe (PE) dirmogr exe (PE) gogsm exe (PE) gogorof exe (PE)		Ş		Ŷ	Ą	Ŷ		Ę															File size: 510450 bytes. Parent file SHA-1: #22812647v6604d15568kease80369683550x Parent file MDS: 6463ax78568c331339720v607398.
inspice are [Pt] inspice are [Pt] inspice are [Pt] material are [Pt] lenovo modern imcontroll are [Pt] Lenovo Modern imcontroll are [Pt]																							Parent file size: 581632 bytes. Parent file age: 0 seconds. Parent process id: 24084.
clip_therreduta.thmx [209] wudthost.exe [PE] services.exe [PE] mbarragent.exe [PE]														19.					۲			,	Detected by the SHA engines.

Passaggio 3. Acquisire la casella Dettagli evento come mostrato nell'immagine.

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.

Passaggio 4. Se necessario, scorrere verso il basso ed eseguire alcune acquisizioni per ottenere tutte le informazioni **Dettagli eventi** come mostrato nell'immagine.



Informazioni sul file

- Informazioni sulla provenienza del file.
- Se il file proviene da un sito Web, condividere l'URL Web.
- Condividere una breve descrizione del file e spiegare la funzione del file.

Spiegazione

- Perché ritieni che l'elaborazione dei file possa essere un falso positivo?
- Condividere i motivi dell'attendibilità del file.

Fornisci informazioni

- Dopo aver raccolto tutti i dettagli, caricare tutte le informazioni richieste su https://cway.cisco.com/csc/.
- Accertarsi di fare riferimento al numero della richiesta di assistenza.

Conclusioni

Cisco si impegna sempre a migliorare ed espandere le funzionalità di intelligence delle minacce della tecnologia AMP for Endpoints. Tuttavia, se la soluzione AMP for Endpoints attiva un avviso erroneamente, è possibile adottare alcune misure per evitare ulteriori impatti sull'ambiente. Questo documento offre linee guida per ottenere tutti i dettagli necessari per aprire una richiesta in Cisco TAC in relazione a un problema di falso positivo. In base all'analisi dei file del team di diagnostica, la disposizione dei file può cambiare per arrestare gli eventi di allarme attivati su AMP Console oppure Cisco TAC può fornire la correzione appropriata per consentire l'esecuzione del file/processo senza problemi nell'ambiente.