# 对面向终端的AMP中的误报文件分析进行故障排 除

## 目录

简<u>介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> <u>对面向终端的AMP中的误报文件分析进行故障排除</u> <u>文件SHA 256哈希</u> <u>文件示例副本</u> <u>从AMP控制台捕获警报事件</u> <u>从AMP控制台捕获事件详细信息</u> <u>有关文件的信息</u> <u>解释</u> <u>提供信息</u> 结论

## 简介

本文档介绍如何在面向终端的高级恶意软件防护(AMP)中收集误报文件分析。

作者:Jesus Javier Martinez,思科TAC工程师。

## 先决条件

## 要求

Cisco 建议您了解以下主题:

- AMP控制台控制面板
- 具有管理员权限的帐户

### 使用的组件

本文档中的信息基于面向终端的思科AMP 6.X.X及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

背景信息

面向终端的AMP可以针对特定文件/进程/安全哈希算法(SHA)256生成过多警报。如果怀疑网络中存 在误报检测,可以联系思科技术支持中心(TAC),诊断团队将继续进行更深入的文件分析。当您联 系思科TAC时,您需要提供以下信息:

·文件SHA 256哈希 ·文件示例副本 ·从AMP控制台捕获警报事件 ·从AMP控制台捕获事件详细信息 ·有关文件的信息(文件的来源以及文件在环境中的原因) ·解释为什么您认为文件/进程可能是误报

## 对面向终端的AMP中的误报文件分析进行故障排除

本部分提供信息,您可以使用这些信息获取通过Cisco TAC打开误报票证所需的所有详细信息。

#### 文件SHA 256哈希

步骤1.要获取SHA 256哈希,请导航至AMP Console > Dashboard > Events。

步骤2.选择Alert Event,单击SHA256,然后选择Copy,如图所示。

File Detection	Detection	▼ Win,Trojan,Generic::61,sbx.vioc	
Connector Info	Fingerprint (SHA-256)	T b9778af82e7bee03	
Comments	File Name	Disposition: Malicious	
	File Path	Filename: h264codec.exe	321.exe
	File Size Parent Fingerprint (SHA-256) Parent Filename	Add to Filter	
		Add to Filter	
		Сору	
	Analyze 🕹 Restor	Search	▲ View Upload Status G Add to Allowed Applications P File Trajecto
		MulDrop Full Report 2	
		File Fetch File Analysis File Trajectory	6 6
		Outbreak Control	e

#### 文件示例副本

步骤1.您可以从AMP控制台获取文件示例,导航至AMP控制台>控制面板>事件。

步骤2.选择Alert Event,单击SHA256,然后导航到File Fetch > File Fetch ,如图所示。

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) Parent Filename Analyze 2 Restor	Add to Filter Copy Search VirusTotal: (1/72) MulDrop Full Report C	View Upload Status Add to Allowed Applications
		File Fetch >	Status: Able to Fetch
		File Analysis	Telebh Fair
		File Trajectory	View in File Repository
		Outbreak Control	
		Investigate in Cisco Threat Response 2	

步骤3.选择检测到文件的设备,然后点击Fetch(如图所示)(设备必须打开),如图所示。

Select a Computer to	Fetch the File from	×
Filename	h264codec.exe	
SHA-256	b9778af82e7bee03	
Choose a Computer	JESUSM2-H381P.cisco.com - (File ~	_
	Close	Fetch
etub 20 ovo		

步骤4.您会收到如图所示的消息。

Select a Computer to	Fetch the File from	×
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

几分钟后,当文件可下载时,您会收到电子邮件通知,如图所示。

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

步骤5.导航至AMP Console > Analysis > File Repository,然后选择文件,然后单击Download,如 图所示。

#### File Repository

Search by SHA-256 or file n	All	~	Group	All Groups		
Type All ~	]					
h264codec.exe is Available	able		Requested by <b>Je</b>	sus Martinez		P 2020-04-16 03:37:42 CE
Original File Name	stub32i.exe					
Fingerprint (SHA-256)	b9778af82e7bee03					
File Size	498 KB					

步骤6.出现通知框,单击下载(如图所示),文件将下载到ZIP文件中。

Warning	$\times$
You are about to download h264codec.exe	
This file may be malicious and cause harm to your computer. You should only	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

## 从AMP控制台捕获警报事件

步骤1.导航至AMP Console > Dashboard > Events。

### 步骤2.选择Alert Event并捕获,如图所示。

JESUSM2-H381	P.cisco.com detected stub32i.exe as Win.Tro	jan.Generic::61.sbx.vloc	Medium			
File Detection	Detection	Y Win.Trojan.Generic::61.sbx.vioc				
Connector Info	Fingerprint (SHA-256)	₹ b9778af82e7bee03				
Comments	File Name	▼ stub32i.exe				
	File Path	C:\Users\jesusm2\Downloads\stub32i.exe				
	File Size	498.49 KB				
	Parent Fingerprint (SHA-256)	₹ 2fb898ba7bf74tet				
	Parent Filename	▼ 7zG.exe				
	Analyze 🏼 🏝 Restore File	2 All Computers	▲ View Upload Status 🛛 🖬 Add to Allowed Applications 🛛 P File Trajectory			

## 从AMP控制台捕获事件详细信息

步骤2.选择Alert Event(警报事件),然后单击Device Trajectory(设备轨迹)选项,如图所示。

			$\mathbf{\hat{c}}$			
▼ JESUSM2-H381	P.cisco.com detected stub32i.exe as Win	Trojan.Generic::61.sbx.vioc	Medium			
File Detection	Detection	T Win,Trojan,Generic::61.sbx.vioc				
Connector Info	Fingerprint (SHA-256)	▼ b9776at82e7bee03				
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	T7zG.exe				
	Analyze & Restore I	File 1 All Computers	▲ View Upload Status 🛛 🖀 Add to Allowed Applications 🛛 P File Trajectory			

#### 它重定向到**设备轨**迹详细信息,如图所示。



步骤3.捕获Event Details(事**件详细**信息)框,如图所示。

#### **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 guarantined. 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.

步骤4.如果需要,向下滚动并捕获一些信息,以获取图**像中**所示的所有事件详细信息。



## 有关文件的信息

- 有关文件来源的信息。
- 如果文件来自网站,请共享Web URL。
- 共享一些文件说明并解释文件功能。

#### 解释

- •为什么您认为文件进程可能是误报?
- 分享您信任该文件的原因。

### 提供信息

- 收集所有详细信息后,将所有请求的信息上传到<u>https://cway.cisco.com/csc/。</u>
- •确保引用服务请求编号。

## 结论

思科始终致力于改进和扩展面向终端的AMP的威胁情报技术,但是,如果面向终端的AMP解决方案 错误地触发警报,您可以采取一些措施来防止对您的环境造成任何进一步影响。本文档提供了获取 所有所需详细信息的指南,以便向思科TAC提交与误报问题有关的问题。根据诊断团队文件分析 ,文件性质可以更改以停止在AMP控制台上触发的警报事件,或者思科TAC可以提供适当的修复 ,以便在您的环境中运行文件/进程而不出现问题。