分析AMP诊断套件,用于高CPU

目录

简介 先决条件 要求 使用的组件 故障排除 验证计算机上是否安装了其他防病毒软件 确定特定应用使用时是否发生高CPU 收集诊断套件以进行分析 启用调试日志级别 终端中的调试级别 策略中的调试级别 <u>重现问题并</u>收集诊断捆绑包 进行分析 Diag_Analyzer.exe Amphandlecount.ps1 调整排除项 向TAC提交捆绑包以供分析

简介

本文档介绍从面向Windows设备上的终端的高级恶意软件防护(AMP)公共云分析诊断捆绑包以排除 高CPU使用率故障的步骤。

作者:Luis Velazquez和Yeraldin Sánchez, Cisco TAC工程师编辑。

先决条件

要求

Cisco 建议您了解以下主题:

• 访问AMP控制台

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 面向终端的AMP控制台5.4.20200204
- Windows操作系统设备

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。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

故障排除

本部分提供的信息可用于对配置进行故障排除。

验证计算机上是否安装了其他防病毒软件

如果安装了另一个AV(防病毒软件),请确保在策略配置中排除AV的主进程

提示:如果列表中包含思科维护的排除项,请记住,这些排除项可以添加到应用程序的新版本 。

要查看Cisco维护的排除部分中的可用列表,请导航至**Management > Policies > Edit >** Exclusions > Cisco维护的排除。

根据计算机上当前安装的软件选择终端需要的软件,然后保存策略,如图所示。

Edit Policy Windows				
Nam	e hevelaz-W7_Policy			
1 Descriptio	n			
Model and Engines	Circo-Maintai	2	d	
ardinizan a	5 selected V	ciusions 🕑		
exclusion sets	Bearch	^	3 Exclusions 🗶	
Proxy	- All		11 Exclusions ×	
	Attris by Symantec	3 Exclusions	1 Exclusion ×	
Outbreak Control	Appsense	6 Exclusions	29 Exclusions ×	
Product Updates	AWAST	3 Exclusions	3 Exclusions 💌	
Idvanced Settings	Avita	3 Exclusions	_	
	Citrix AppONA	2 Exclusions		
	Citrix Cloud Connector	3 Exclusions		
3	Citrix EdgeSight Server	3 Exclusions	85 Exclusions	
_	Citrix ICA Client	5 Exclusions		
	Citrix Provisioning Server	18 Exclusions		
	Citrix XenApp v6.5 and 7	7 Exclusions		
	Crashplan	3 Exclusions		
	Diebold Warsaw	10 Exclusions		
	Domain Controller	19 Exclusions		Ľ
	Hyper-V	17 Exclusions		
	15	7 Exclusions		
		¥		Cancel

确定特定应用使用时是否发生高CPU

确定问题是否发生在执行一个应用程序或其中几个应用程序时,如果您能够复制该问题,则有助于 确定潜在的排除项。

收集诊断套件以进行分析

启用调试日志级别

要收集有用的诊断包,必须启用调试日志级别。

终端中的调试级别

如果可以复制问题并有权访问终端,以下是捕获诊断捆绑包的最佳步骤:

- 1. 打开AMP GUI
- 2. 导航至**设置**
- 3. 滚动到AMP GUI底部并打开Cisco AMP连接器设置
- 4. 单击"Enable Debug Logging (启用调试日志记录) "
- 5. "调试日志记录状态"必须更改为"已启动"。此过程启用调试级别,直到下一个策略心跳,默认为15分钟

WINCHU	
^[A-Za-z]:\\/Wildcard/A	d/Drive
^[A-Za-z]:\\Wildcard\ a ^[A-Za-z]:\\pagefile\.sy	I\ drives s
Scan Settings	▼
Notification Settings	▼
Proxy Settings	▼
Cisco AMP Connector Settings	5 A
Service Status:	Started
Password:	
Stop Service	
Debug Logging Status:	Stopped
Enable Debug Logging	

策略中的调试级别

如果您无权访问终端或无法一致地重现问题,则必须在策略中启用调试日志级别。

要按策略启用调试日志级别,请导航到Management > Policies > Edit > Advanced Settings > Connector Log Level 和Management > Policies > Edit > Advanced Settings > Tray Log Level,然 后选择Debug并保存策略,如图所示。

<	Edit Policy					
	Name	luivelaz-W7_Policy				
	Description			4		
	Modes and Engines		Send User Name in Events			
	Exclusions 6 exclusion sets		Send Filename and Path Info 0			
	Proxy	2 Connector Log Level	Debug v	0		
	Outbreak Control	Tray Log Level	Debug	0		
	Advanced Settings Advanced Settings Administrative Features	Connector Protection Password	Enable Connector Protection 0	0		
	Client User Inherlane File and Process Scan Cache		Automated Crash Dump Uploads Command Line Capture			
	Endpoint Isolation Orbital Engines		Command Line Logging 0			
	TETRA Network					
	Identity Persistence					
					Cancel	Save

警告:如果从策略启用调试模式,则所有终端都会收到此更改。

注意:同步终端的策略以确保应用调试级别或等待心跳间隔(默认为15分钟)。

重现问题并收集诊断捆绑包

当配置调试级别时,请等待系统上出现高CPU状态,或手动重现之前确定的条件,然后收集诊断包 。

要收集捆绑包,请导航至C:\Program Files\Cisco\AMP\X.X.X (其中X.X.X是系统上安装的最新 AMP版本)并运行应用程序ipsupporttool.exe,此过程会在名为 CiscoAMP_Support_Tool_%date%。7z的桌面上创建.7z文件

注意:连接器版本6.2.3及更高版本可以远程请求捆绑包,导航至**Management > Computers**,展开终端记录并使用Diagnose选项。

注意:诊断捆绑包也可以从CMD提示符下使用以下命令运行:**"C:\Program** Files\Cisco\AMP\X.X.X\ipsupporttool.exe"或**"C:\Program** Files\Cisco\AMP\X.X.X\ipsupporttool.exe" -o "X:\Folder\I\Can\Get\To",其中X.X.X是安装的 最新AMP版本,可以使用第二个命令来选择。7z文件的输出文件夹。

进行分析

有两种方法可以分析诊断文件:

- Diag_Analyzer.exe
- Amphandlecount.ps1

Diag_Analyzer.exe

步骤1.在此下载应用程序。

步骤2.在GitHub页面中,有一个README文件,其中包含有关使用的进一步说明。

步骤3.将诊断文件**CiscoAMP_Support_Tool_%date%。7z复制**到Diag_Analyzer.exe所在的文件夹中。

步骤4.执行应用 Diag_Analyzer.exe。



步骤5.在新提示符中,确认是否要从策略中获得Y或N的排除项。。

步骤6.脚本结果包含:

- 前10个流程
- 前10个文件
- 前10个分机
- 前100条路径
- 所有文件

注意:Diag_Analyzer.exe检查提供的AMP诊断文件sfc.exe.log文件。然后,使用诊断文件名 创建新目录并将日志文件存储在。7z之外的。7z目录中,之后,它解析日志并确定前10个进 程、文件、扩展名和路径,最后,它将信息打印到屏幕和{Diagnostic}-summary.txt文件。

Amphandlecount.ps1

步骤1.从此社区底部**下载脚本**amphandlecounts.txt,然后从<u>AMP审阅扫描的文件。</u>

步骤2.要在Windows中运行脚本,请将其重命名为amphandlecount.ps1。

步骤3.为方便起见,将amphandlecount.ps1文件复制到自己的文件夹。

1	> Th	is PC > Documents > Review Bundle				
ccess		Name	Date modified	Туре	Size	
nents	*	amphandlecount.ps1	26/04/2019 09:44 a	Windows PowerS	3 KB	
oads	*					

步骤4.解压CiscoAMP_Support_Tool_%date%。7z文件,并在路**径上标识sfc**.log的文件 CiscoAMP_Support_Tool_2019_06_13_18_26_37\Program Files\Cisco\AMP\X.X.X。

Name	Date modified	Туре	Size		
ConnectivityTool.exe.log	18/06/2019 01:46	LOG File	32 KB		
🦉 🧧 global.xml	08/06/2019 11:23	XML File	24 KB	_	
* 📕 sfc.exe.log	18/06/2019 01:46	LOG File	46,634 KB	1	
* sfc.exe_20190614_171821.log	14/06/2019 05:18	LOG File	6,912 KB		
# sfc.exe_20190616_123123.log	16/06/2019 12:31	LOG File	51,201 KB		
sfc.exe_20190616_131825.log	16/06/2019 01:18	LOG File	51,201 KB		
sfc.exe_20190616_134500.log	16/06/2019 01:45	LOG File	51,201 KB		
sfc.exe_20190616_140234.log	16/06/2019 02:02	LOG File	51,201 KB		
sfc.exe_20190616_150139.log	16/06/2019 03:01	LOG File	51,201 KB		
sfc.exe_20190618_133822.log	18/06/2019 01:38	LOG File	51,201 KB		
sfc.exe_20190618_134032.log	18/06/2019 01:40	LOG File	51,201 KB		
5 sfc.exe 20190618 134240.log	18/06/2019 01:42	LOG File	51,201 KB		

步骤5.将sfc.log的文件复制到amphandlecount.ps1文件夹。

Name	Date modified	Туре	Size	
ConnectivityTool.exe.log	18/06/2019 01:46	LOG File	32 KB	
global.xml	08/06/2019 11:23	XML File	24 KB	
📕 sfc.exe.log	18/06/2019 01:46	LOG File	46,634 KB	
5fc.exe_20190614_171821.log	14/06/2019 05:18	LOG File	6,912 KB	
5fc.exe_20190616_123123.log	16/06/2019 12:31	LOG File	51,201 KB	
sfc.exe_20190616_131825.log	16/06/2019 01:18	LOG File	51,201 KB	
5fc.exe_20190616_134500.log	16/06/2019 01:45	LOG File	51,201 KB	
5fc.exe_20190616_140234.log	16/06/2019 02:02	LOG File	51,201 KB	
sfc.exe_20190616_150139.log	16/06/2019 03:01	LOG File	51,201 KB	
5fc.exe_20190618_133822.log	18/06/2019 01:38	LOG File	51,201 KB	
sfc.exe_20190618_134032.log	18/06/2019 01:40	LOG File	51,201 KB	
sfc.exe_20190618_134240.log	18/06/2019 01:42	LOG File	51,201 KB	

p,

4

步骤6.使**用PowerShell运行**amphandlecount.ps1,然后打开一个窗口,根据终端上的执行策略,可 以请求运行权限。

提示:要更改执行策略,请打开Windows PowerShell并使用下一命令: 将策略设置为允许无限制执行访问 — Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted 设置策略以限制执行访问 — Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restricted

步骤7.在PowerShell完成后,允许PowerShell完成(可能需要一些时间,具体取决于文件夹中的 sfc.log数量),在文件夹上创建四个文件:

- data.csv
- results.txt
- sorted_results.txt
- terms.txt

	ister socurrents i henen bullule			• 0	search memory particle	~
	Name	Date modified	Туре	Size		
	amphandlecount.ps1	26/04/2019 09:44 a	Windows PowerS	3 KB		
s 7°	data.csv	22/06/2019 03:28	Microsoft Excel C	754 KB		
<i>.</i>	results.txt	22/06/2019 03:28	TXT File	3 KB		
*	sfc.exe.log	18/06/2019 01:46	LOG File	46,634 KB		
	sfc.exe_20190614_171821.log	14/06/2019 05:18	LOG File	6,912 KB		
	5 sfc.exe_20190616_123123.log	16/06/2019 12:31	LOG File	51,201 KB		
dle	sfc.exe_20190616_131825.log	16/06/2019 01:18	LOG File	51,201 KB		
	sfc.exe_20190616_134500.log	16/06/2019 01:45	LOG File	51,201 KB		
	sfc.exe_20190616_140234.log	16/06/2019 02:02	LOG File	51,201 KB		
	sfc.exe_20190616_150139.log	16/06/2019 03:01	LOG File	51,201 KB		
	sfc.exe_20190618_133822.log	18/06/2019 01:38	LOG File	51,201 KB		
	sfc.exe_20190618_134032.log	18/06/2019 01:40	LOG File	51,201 KB		
	5fc.exe_20190618_134240.log	18/06/2019 01:42	LOG File	51,201 KB		
	sorted_results.txt	22/06/2019 03:28	TXT File	3 KB		
	📁 terms.bit	22/06/2019 03:28	TXT File	3 KB		

步骤8.4个新文件包含分析结果:

- data.csv:包含已扫描文件的完整路径以及创建/修改/移动文件的父进程
- results.txt:包含AMP扫描的进程列表
- sorted_results.txt:包含AMP扫描的进程列表,其中扫描的进程最多
- terms.txt:包含AMP扫描的进程的名称

步骤9.从**data.csv**中的**sorted_results.txt**中筛选具有高计数的进程名称,然后继续在自定义列表中添 加一个排除项(如果受信任)。

要查看的流程:

•

- 1. 在"data.csv"和搜索上控制+ F
- 2. AMP扫描的文件路径
- 3. 复制/移动/修改文件的父进程的路径

注意:注意:排除通常为"Process:文件扫描"(File Scan),其中"子进程包括"(Child Processes include)用于正在获取扫描的父进程

4 Þ	sorted_results.txt	A2 : X 🗸 Jr Jun 18 13:42:40,C:\Temp\NVIDL	A PanelInstallerTemp\nvmobESN.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.(C9752557-A557-4AE9-
2	10/5 setup.exe 442 firefox.exe 243 container.exe		H J K L M N O P Q R S T
4	243 Container.exe	1 Jun 18 13:42:40,C:\Temp\NVIDIA\ControlPanelInstallerTemp\nvmobE	SM.chm, C:\Program Files\WVIDIA Corporation\Installer2\Display.Driver.[0752557-A557-4AE9-B704-551FE0F3AFE7]\NvCpISetupInt.exe
5	243 container.exe	2 Jun 18 13:42:40,C:\Temp\NVIDIA\ControlPanelInstallerTemp\nvmobe	:SN.cnm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-87D4-551FE0F3AFE7}\NvCpISetupInt.exe
6	243 Container.exe	3 Jun 18 12:42:40 C-\Tomn\NIVIDIA\ControlDanolinctallorTomn\nymobi	Inh.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCpISetupInt.exe
2	243 container.exe	4 Find and Replace ? X	A.chm.C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
8	243 Container.exe	5	Richm C-) Program Eiles NV/IDIA Compration Installer) Display Driver (C9752557, A557, 4A59, 8704, 55155053A557) NV/OISaturint ava
10	129 NuColSaturaTet exe	Find Replace	A charge of the state of the st
11	S4 charle-eve	0	N.cnm,C:\Program Files\WVIDIA Corporation\installer2\Display.Driver.{C9752557-A557-4AE3-B7D4-551FE0F3AFE7}\WVCpiSetupint.exe
12	n ershell.exe	7 Find what: NvCpISetupInt.exe V	.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCpISetupInt.exe
13	1 sass.exe	8 🧾	I.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
14	svchost.exe	9	R.chm.C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7]\NvCplSetupInt.exe
15	7 OUTLOOK.EXE	10 Options >>	D. chm. C.\Program Eiles\NV/IDIA Corporation\Installer2) Display Driver (C9752557.4557.4459.8704.551E6624EE7) NvColSatural even
16	7 nvstinst.exe	10 2 F	scini, c. (rigiani ries) with corporation (instance 2015) as the corporation of the state of the
17	5 explorer.exe	Tradue Contract Contract	R.cnm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-87D4-551FE0F3AFE7}\NvCpISetupInt.exe
18	4 rund1132.exe	12 Find All Find Next Close	Lchm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCpISetupInt.exe
19	3 Indexe	13 Jun 18 13:42:41.C:\Temp\NVIDIA\ControlPaneIInstallerTemp\nvmobF	PTB.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCpISetupInt.exe
20	3 Outlook-exe	14 Jun 18 12:42:41 Cil Tomol MU(DIA) ControlDanolinetallorTomol numobi	TC chm ()) Program Eller/MI/DIA Corporation/Installor/) Diselay Driver (09752557, 4557, 4559, 8704, 551550524557) Mucal Saturdation

注意:<u>在此</u>可以找到与创建例外项的最佳实践相关的详细信息。

调整排除项

确定进程或路径后,可以将其添加到链接到终端上应用的策略的排除列表中,导航至Management > Exclusions > Exclusion name > Edit,如图所示。

Threat	CSIDL_V	VINDOWS\Temp_avast_\	Ì					
Path	[Any Driv	[Any Drive]:\ pagefile.sys						
File Extension	Apply	Apply to all drive letters						
Wildcard	Path exc	ath exclusion						
Process:	Thursday							
File Scan	Threat ex	ireat exclusion						
Malicious Activity	Wildcard	Vildcard						
System Process	Apply	to all drive letters						
Process	Path	C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557.4AE9-B7D4-55		L				
File Scan	SHA			ŀ				
	You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must							
	be met fe	or the process to be excluded.		I				
	and the second sec							
	Apply	/ to child processes		L				
	Apply Apply	r to child processes		v				

ATS TAC可帮助排除这些情况,如果是这种情况,请准备好在创建案例时提供下一信息:

- •此问题何时开始?
- •最近有变化吗?
- •特定应用程序是否出现问题?如果是,哪个应用程序?
- •系统上是否有其他防病毒软件?如果是,哪种防病毒软件?
- 在重现问题时收集调试捆绑包: 收集调试捆绑包的步骤