

Analizar el paquete de diagnóstico de AMP para una CPU elevada

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Troubleshoot](#)

[Compruebe si hay otro antivirus instalado en el equipo](#)

[Identificar si la CPU alta ocurre cuando una aplicación específica está en uso](#)

[Recopile el paquete de diagnóstico para su análisis](#)

[Activar nivel de registro de depuración](#)

[Nivel de depuración en el terminal](#)

[Nivel de depuración en la política](#)

[Reproduzca el problema y recopile un paquete de diagnóstico](#)

[Realizar el análisis](#)

[Diag_Analyzer.exe](#)

[Anphandlecount.ps1](#)

[Exclusiones de ajuste](#)

[Enviar el paquete para su análisis al TAC](#)

Introducción

Este documento describe los pasos para analizar un paquete de diagnóstico de la protección frente a malware avanzado (AMP) para terminales de nube pública en dispositivos Windows para solucionar problemas de uso elevado de la CPU.

Colaborado por Luis Velázquez y editado por Yeraldin Sánchez, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso a la consola de AMP

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Consola de AMP para terminales 5.4.20200204
- Dispositivos del sistema operativo Windows

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

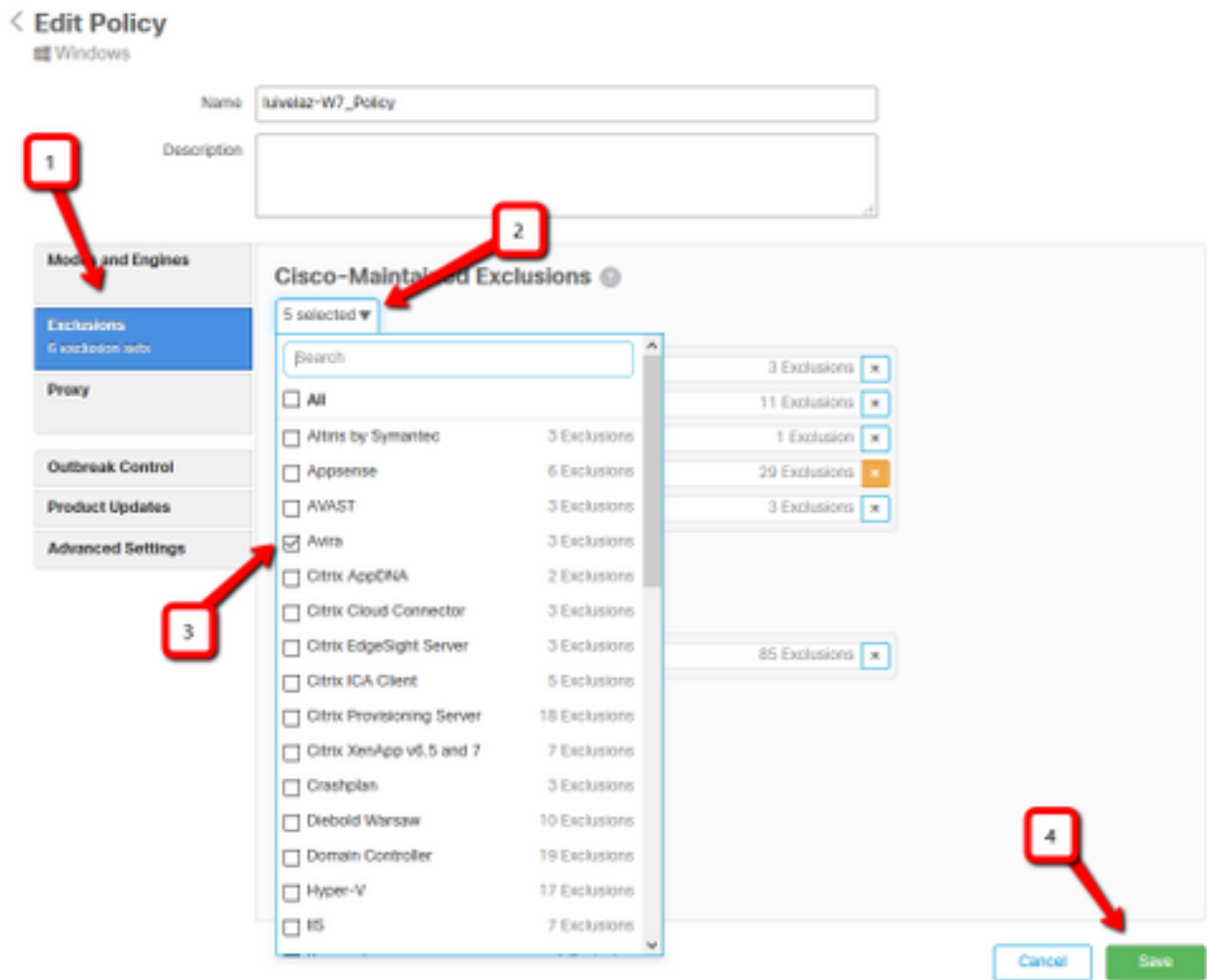
Compruebe si hay otro antivirus instalado en el equipo

Si se instala otro antivirus, asegúrese de que el proceso principal del antivirus esté excluido en la configuración de políticas

Consejo: Utilice las exclusiones de Cisco-Mantenimiento si el software que se utiliza está incluido en la lista, recuerde que estas exclusiones se pueden agregar a las nuevas versiones de una aplicación.

Para ver las listas disponibles en la sección de exclusiones mantenidas por Cisco, navegue hasta **Administración > Políticas > Editar > Exclusiones > Exclusiones Mantenidas por Cisco**.

Seleccione los que el terminal necesitaría según el software instalado actualmente en el equipo y, a continuación, guarde la política, como se muestra en la imagen.



Identificar si la CPU alta ocurre cuando una aplicación específica está en uso

Identifique si el problema ocurre mientras se ejecuta una o varias aplicaciones si puede replicar el problema ayuda en el proceso de identificar posibles exclusiones.

Recopile el paquete de diagnóstico para su análisis

Activar nivel de registro de depuración

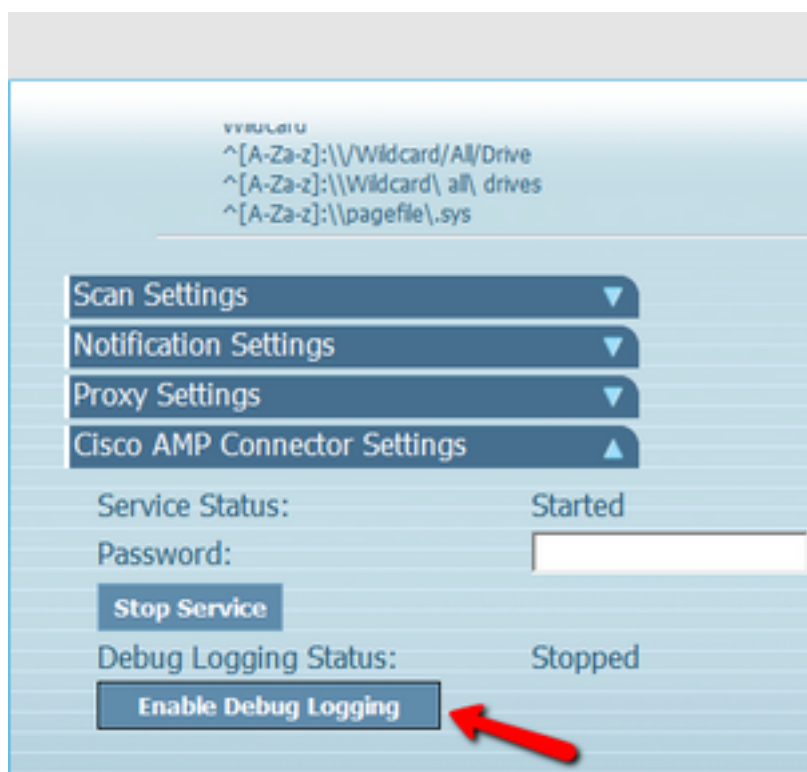
Para recopilar un paquete de diagnóstico útil, se debe habilitar el nivel de registro de depuración.

Nivel de depuración en el terminal

Si puede replicar el problema y tener acceso al terminal, a continuación se muestra el mejor procedimiento para capturar el paquete de diagnóstico:

1. Abrir AMP GUI
2. Vaya a **Settings**
3. Desplácese hasta la parte inferior de AMP GUI y abra **Configuración del conector de Cisco AMP**
4. Haga clic en **Habilitar registro de depuración**
5. **El estado de registro de depuración debe cambiar a Iniciado.** Este procedimiento habilita el

nivel de depuración hasta el siguiente latido de política, de forma predeterminada 15 minutos



Nivel de depuración en la política

Si no tiene acceso al punto final o el problema no se puede reproducir de forma consistente, el nivel de registro de depuración debe estar habilitado en la política.

Para habilitar el nivel de registro de depuración mediante la política, navegue hasta Administración > Políticas > Editar > Configuración avanzada > **Nivel de registro del conector** y Administración > Políticas > Editar > Configuración avanzada > Nivel de registro de la bandeja, seleccione Depurar y guarde la política, como se muestra en la imagen.

< Edit Policy

Windows

Name

Description

Modes and Engines

Exclusions
6 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

Administrative Features

Client User Interface

File and Process Scan

Cache

Endpoint Isolation

Orbita

Engines

ETBA

Network

Scheduled Scans

Identity Persistence

Send User Name in Events ⓘ

Send Filename and Path Info ⓘ

Heartbeat Interval ⓘ

Connector Log Level ⓘ

Tray Log Level ⓘ

Enable Connector Protection ⓘ

Connector Protection Password ⓘ

Automated Crash Dump Uploads ⓘ

Command Line Capture ⓘ

Command Line Logging ⓘ

Precaución: Si el modo de depuración se habilita desde la política, todos los terminales reciben este cambio.

Nota: Sincronice la política del punto final para asegurarse de que se aplica el nivel de depuración o espere el intervalo de latido, de forma predeterminada es de 15 minutos.

Reproduzca el problema y recopile un paquete de diagnóstico

Cuando se configura el nivel de depuración, espere hasta que se produzca el estado de CPU alta en el sistema o reproduzca manualmente las condiciones previamente identificadas y luego reúna el paquete de diagnóstico.

Para recopilar el paquete, navegue hasta **C:\Program Files\Cisco\AMP\X.X.X** (donde X.X.X es la última versión de AMP instalada en el sistema) y ejecute la aplicación **ipsupporttool.exe**, este proceso crea un **archivo .7z** en el escritorio denominado **CiscoAMP_Support_Tool_%date%.7z**

Nota: La versión 6.2.3 y posterior del conector pueden solicitar un paquete remotamente, navegar a **Administración > Equipos**, expandir el registro del terminal y utilizar la opción **Diagnose**.

Nota: El paquete de diagnóstico también puede ejecutarse desde un mensaje CMD con el

comando: "C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe", o "C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe" -o "X:\Folder\Can\Get\To", donde X.X.X es la última versión de AMP instalada, se puede utilizar el segundo comando para seleccionar la carpeta de resultados para el archivo .7z.

Realizar el análisis

Hay dos maneras de analizar un archivo de diagnóstico:

- Diag_Analyzer.exe
- Anphandlecount.ps1

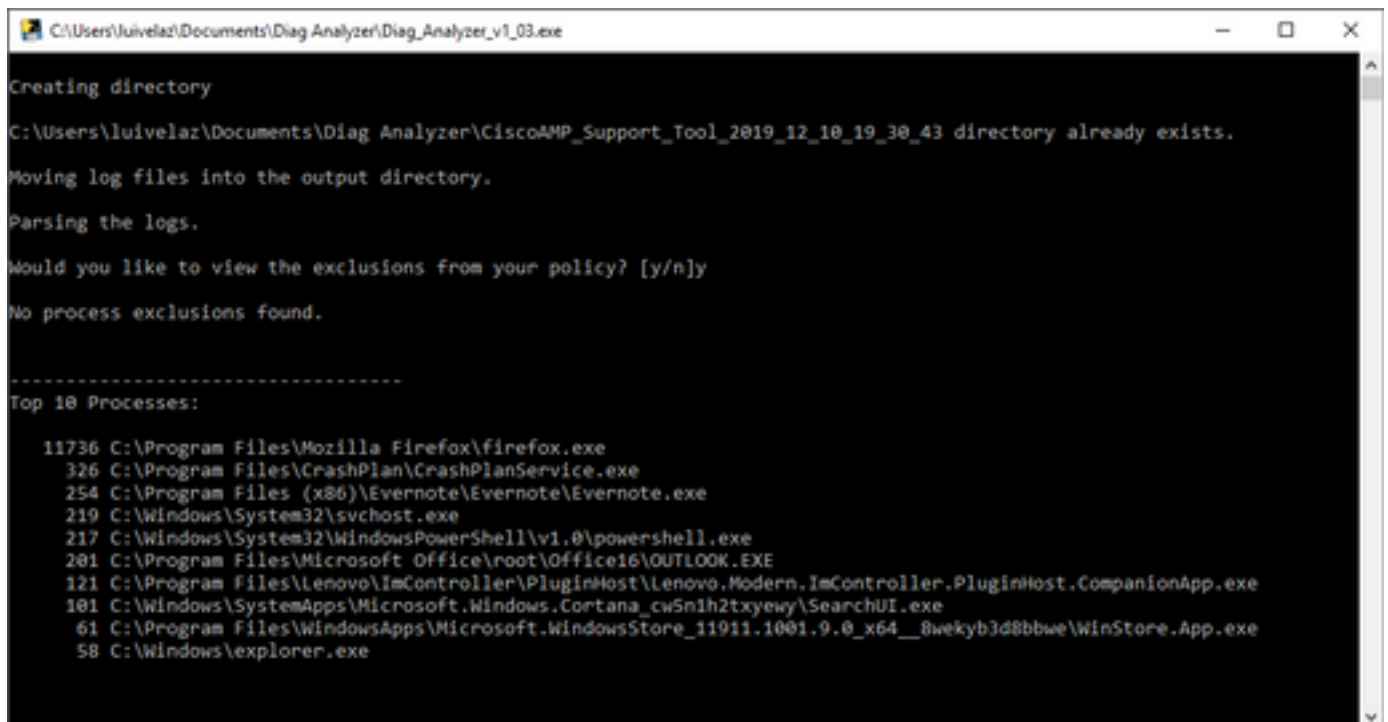
Diag_Analyzer.exe

Paso 1. Descargue la aplicación [aquí](#).

Paso 2. En la página GitHub, hay un archivo README con más instrucciones sobre el uso.

Paso 3. Copie el archivo de diagnóstico **CiscoAMP_Support_Tool_%date%.7z** en la misma carpeta en la que se encuentra Diag_Analyzer.exe.

Paso 4. Ejecutar la aplicación **Diag_Analyzer.exe**.



```
C:\Users\luivelaz\Documents\Diag Analyzer\Diag_Analyzer_v1_03.exe
Creating directory
C:\Users\luivelaz\Documents\Diag Analyzer\CiscoAMP_Support_Tool_2019_12_10_19_30_43 directory already exists.
Moving log files into the output directory.
Parsing the logs.
Would you like to view the exclusions from your policy? [y/n]y
No process exclusions found.

-----
Top 10 Processes:
11736 C:\Program Files\Mozilla Firefox\firefox.exe
326 C:\Program Files\CrashPlan\CrashPlanService.exe
254 C:\Program Files (x86)\Evernote\Evernote\Evernote.exe
219 C:\Windows\System32\svchost.exe
217 C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
201 C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
121 C:\Program Files\Lenovo\ImController\PluginHost\Lenovo.ImController.PluginHost.CompanionApp.exe
101 C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
61 C:\Program Files\WindowsApps\Microsoft.WindowsStore_11911.1001.9.0_x64__8wekyb3d8bbwe\WinStore.App.exe
58 C:\Windows\explorer.exe
```

Paso 5. En el nuevo mensaje confirme si desea obtener las exclusiones de la política con una Y o una N.

Paso 6. El resultado del script contiene:

- Los 10 procesos principales
- 10 archivos principales
- 10 principales extensiones

- 100 rutas principales
- Todos los archivos

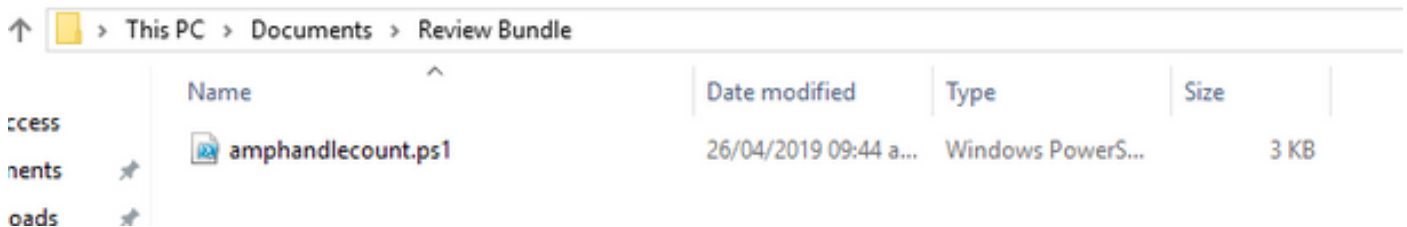
Nota: Diag_Analyzer.exe comprueba el archivo de diagnóstico de AMP proporcionado para los archivos sfc.exe.log. a continuación, crea un nuevo directorio con el nombre del archivo de diagnóstico y almacena los archivos de registro fuera del .7z, en el directorio primario del diagnóstico, después de esto, analiza los registros y determina los 10 principales procesos, archivos, extensiones y rutas, por último, imprime información en la pantalla y también en un archivo {Diagnostic}-summary.txt.

Anphandlecount.ps1

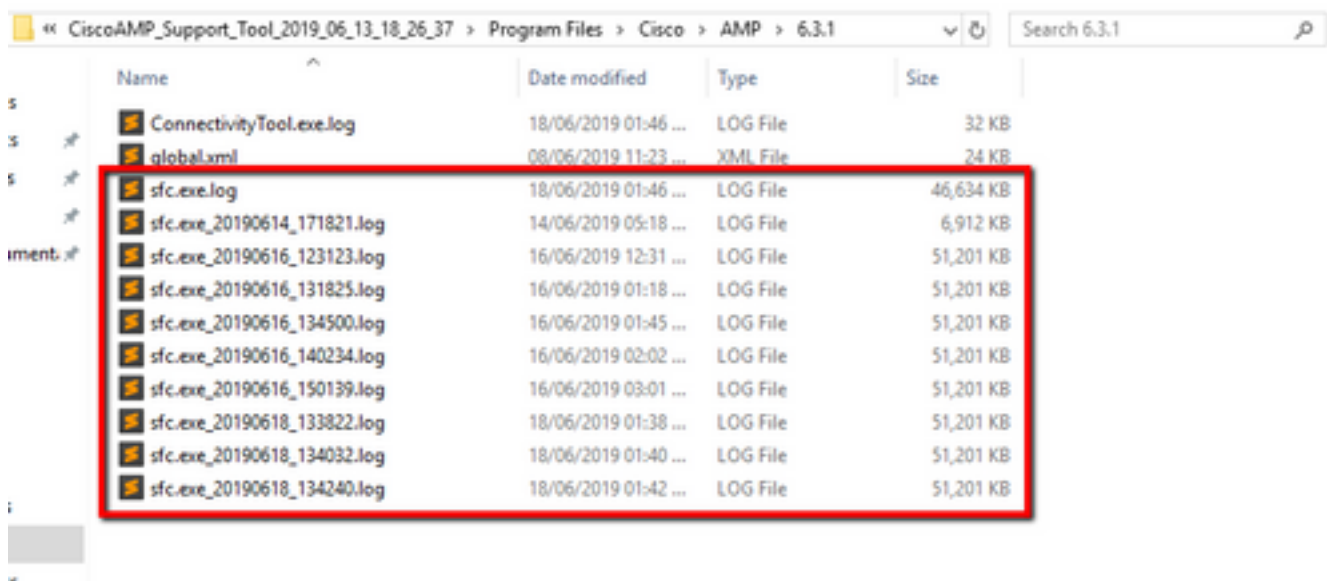
Paso 1. Descargue el script **amphandlecounts.txt** desde la parte inferior de esta publicación de la comunidad [Revisar archivos escaneados desde AMP](#).

Paso 2. Para ejecutar el script en Windows, cámbielo a **anphandlecount.ps1**.

Paso 3. Para mayor comodidad, copie el archivo **anphandlecount.ps1** en su propia carpeta.



Paso 4. Descomprima el archivo **CiscoAMP_Support_Tool_%date%.7z** e identifique los archivos **sfc.log** en la ruta **CiscoAMP_Support_Tool_2019_06_13_18_26_37\Program Files\Cisco\AMPX.X.X**.



Paso 5. Copie los archivos **sfc.log** en la carpeta **anphandlecount.ps1**.

« CiscoAMP_Support_Tool_2019_06_13_18_26_37 > Program Files > Cisco > AMP > 6.3.1 Search 6.3.1

Name	Date modified	Type	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
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
sfc.exe_20190618_134240.log	18/06/2019 01:42 ...	LOG File	51,201 KB

Paso 6. Ejecute **amphandlecount.ps1** con PowerShell, después se abre una ventana y, según la política de ejecución del terminal, se puede solicitar permiso para ejecutarse.

Consejo: Para cambiar la política de ejecución, abra un Windows PowerShell y utilice los siguientes comandos:

Establezca la política para permitir el acceso sin restricciones a la ejecución - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted**

Establezca la política para restringir el acceso a la ejecución - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restringido**

Paso 7. Permita que PowerShell finalice (puede que tarde algún tiempo, dependiendo de cuántos sfc.log haya en la carpeta) después de que PowerShell termine, se crean cuatro archivos en la carpeta:

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

> This PC > Documents > Review Bundle Search Review Bundle

Name	Date modified	Type	Size
amphandlecount.ps1	26/04/2019 09:44 a...	Windows PowerS...	3 KB
data.csv	22/06/2019 03:28 ...	Microsoft Excel C...	754 KB
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
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
sfc.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.txt	22/06/2019 03:28 ...	TXT File	3 KB

Paso 8. Los 4 nuevos archivos contienen el resultado del análisis:

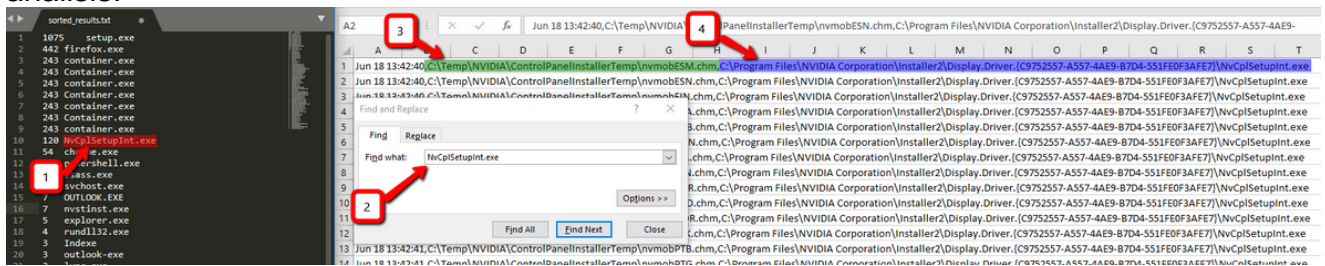
- **data.csv:** contiene la ruta completa de los archivos analizados y el proceso padre que creó/modificó/movió el archivo
- **results.txt:** contiene la lista de procesos escaneados por AMP
- **sorted_results.txt:** contienen la lista de procesos que AMP analiza con el proceso más analizado
- **terms.txt:** contiene el nombre de los procesos analizados por AMP

Paso 9. Filtre el nombre del proceso con recuentos altos de **sorted_results.txt** en **data.csv** puede identificar el proceso primario con su ruta de acceso completa y, a continuación, continúe agregando una exclusión a la política en una lista personalizada si es de confianza.

Procesos a buscar:

1. Ctrl + F en "data.csv" y buscar
2. Ruta del archivo analizado por AMP
3. Ruta del proceso primario que copia/mueve/modifica el archivo

Nota: Normalmente, la exclusión es del tipo "Proceso: Análisis de archivos" con "Procesos secundarios" para el proceso principal que está recibiendo los análisis:



Nota: [Aquí](#) puede encontrar más información relacionada con las mejores prácticas para crear exclusiones.

Exclusiones de ajuste

Una vez que se identifican los procesos o las trayectorias, puede agregarlos a la lista de exclusión vinculada a la política aplicada en el punto final, navegue hasta **Administración > Exclusiones > Nombre de exclusión > Editar**, como se muestra en la imagen.

Threat	CSIDL_WINDOWS\Temp_avast_\	
Path	[Any Drive]:\ pagefile.sys	
File Extension	<input checked="" type="checkbox"/> Apply to all drive letters	
Wildcard	Path exclusion	
Process:	Threat exclusion	
File Scan	Wildcard	
Malicious Activity	<input type="checkbox"/> Apply to all drive letters	
System Process		
Process <input type="checkbox"/>	Path C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-55	
File Scan	SHA	
	You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.	
	<input checked="" type="checkbox"/> Apply to child processes	

Enviar el paquete para su análisis al TAC

El TAC de ATS puede ayudar a resolver estos problemas, si es así, esté listo para proporcionar la siguiente información al crear el caso:

- ¿Cuándo comienza este problema?
- ¿Hay algún cambio reciente?
- ¿El problema ocurre con una aplicación determinada? En caso afirmativo, ¿qué aplicación?
- ¿Hay otro antivirus en el sistema? En caso afirmativo, ¿qué antivirus?
- Recopile un paquete de depuración mientras se reproduce el problema: [Pasos para recopilar un paquete de depuración](#)