

Analise o pacote de diagnóstico do AMP para CPU alta

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Troubleshoot](#)

[Verifique se outro antivírus está instalado na máquina](#)

[Identificar se a CPU alta acontece quando um aplicativo específico está em uso](#)

[Reunir pacote de diagnóstico para análise](#)

[Habilitar nível de log de depuração](#)

[Nível de Depuração no endpoint](#)

[Nível de depuração na política](#)

[Reproduza o problema e reúna um pacote de diagnóstico](#)

[Faça a análise](#)

[Diag_Analyzer.exe](#)

[Amphandlecount.ps1](#)

[Ajustar exclusões](#)

[Envie o pacote para análise ao TAC](#)

Introduction

Este documento descreve as etapas para analisar um pacote de diagnóstico da AMP (Advanced Malware Protection, Proteção avançada contra malware) para endpoints na nuvem pública em dispositivos Windows para solucionar problemas de uso elevado da CPU.

Contribuído por Luis Velazquez e editado por Yeraldin Sánchez, Engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso ao console AMP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- AMP para endpoints Console 5.4.20200204

- dispositivos do sistema operacional 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Troubleshoot

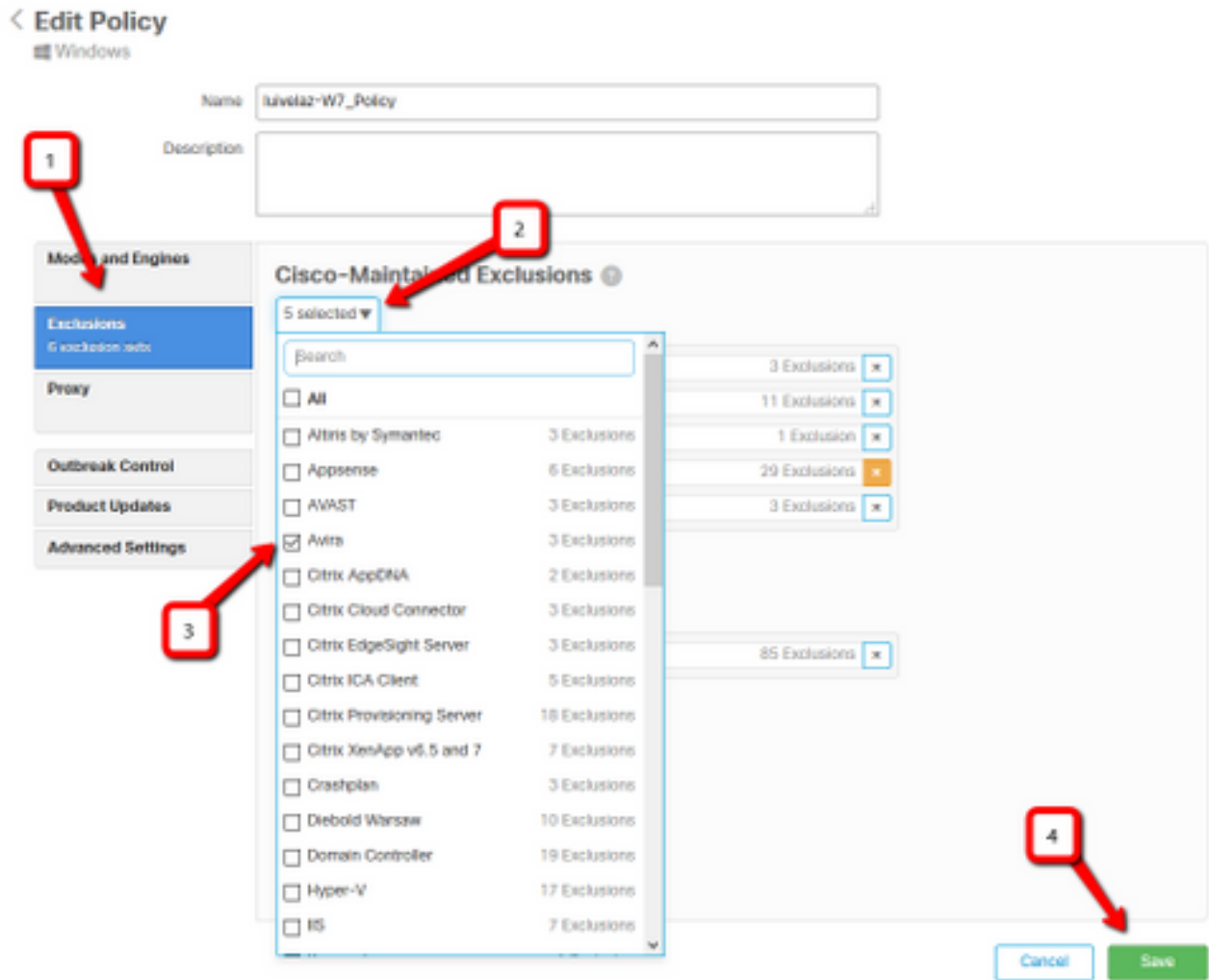
Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Verifique se outro antivírus está instalado na máquina

Se outro antivírus (AV) estiver instalado, verifique se o processo principal do AV está excluído na configuração da política

Tip: Use as exclusões mantidas pela Cisco se o software usado estiver incluído na lista. Lembre-se de que essas exclusões podem ser adicionadas a novas versões de um aplicativo.

Para ver as listas disponíveis na seção exclusões mantidas pela Cisco, navegue para **Gerenciamento > Políticas > Editar > Exclusões > Exclusões mantidas pela Cisco**. Selecione os que seu endpoint precisaria de acordo com o software atualmente instalado na máquina e salve a diretiva, como mostrado na imagem.



Identificar se a CPU alta acontece quando um aplicativo específico está em uso

Identifique se o problema acontece enquanto um ou alguns deles são executados se você puder replicar o problema ajuda no processo de identificação de possíveis exclusões.

Reunir pacote de diagnóstico para análise

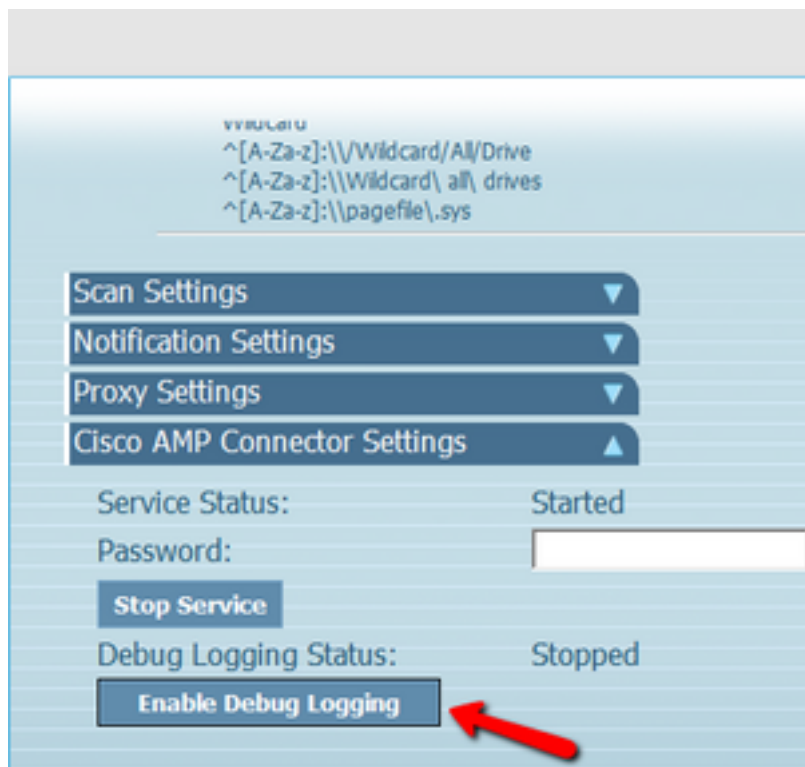
Habilitar nível de log de depuração

Para reunir um pacote de diagnóstico útil, o nível de log de depuração deve ser ativado.

Nível de Depuração no endpoint

Se você puder replicar o problema e tiver acesso ao endpoint, abaixo está o melhor procedimento para capturar o pacote de diagnóstico:

1. Abrir GUI do AMP
2. Navegue até **Configurações**
3. Role até a parte inferior da GUI do AMP e abra **as configurações do conector do Cisco AMP**
4. Clique em **Ativar registro de depuração**
5. O **Status de log de depuração** deve ser alterado para **Iniciado**. Este procedimento ativa o nível de depuração até o próximo heartbeat de política, por padrão, 15 minutos



Nível de depuração na política

Se você não tiver acesso ao endpoint ou se o problema não puder ser reproduzido de forma consistente, o nível de log de depuração deverá ser ativado na política.

Para habilitar o nível de log de depuração por política, navegue para Gerenciamento > Políticas > Editar > Configurações avançadas > **Nível e gerenciamento de log do conector** > Políticas > Editar > Configurações avançadas > Nível de log da bandeja e selecione Depurar e salve a política, como mostrado na imagem.

< Edit Policy

Windows

Name:

Description:

Modes and Engines	<input checked="" type="checkbox"/> Send User Name in Events ⓘ
Exclusions 6 exclusion sets	<input checked="" type="checkbox"/> Send Filename and Path Info ⓘ
Proxy	Heartbeat Interval: <input type="text" value="15 minutes"/> ⓘ
Outbreak Control	Connector Log Level: <input type="text" value="Debug"/> ⓘ
Product Updates	Tray Log Level: <input type="text" value="Debug"/> ⓘ
Advanced Settings	<input checked="" type="checkbox"/> Enable Connector Protection ⓘ
Administrative Features	Connector Protection Password: <input type="password" value="*****"/> ⓘ
Client User Interface	<input checked="" type="checkbox"/> Automated Crash Dump Uploads ⓘ
File and Process Scan	<input checked="" type="checkbox"/> Command Line Capture ⓘ
Cache	<input checked="" type="checkbox"/> Command Line Logging ⓘ
Endpoint Isolation	
Orbitat	
Engines	
ETBA	
Network	
Scheduled Scans	
Identity Persistence	

1 → Heartbeat Interval
2 → Connector Log Level

Caution: Se o modo de depuração estiver ativado na política, todos os endpoints receberão essa alteração.

Note: Sincronize a política do endpoint para garantir que o nível de depuração seja aplicado ou aguarde o intervalo de pulsação, por padrão, é de 15 minutos.

Reproduza o problema e reúna um pacote de diagnóstico

Quando o nível de depuração for configurado, aguarde até que o estado de CPU alta ocorra no sistema ou reproduza manualmente as condições previamente identificadas e, em seguida, reúna o pacote de diagnóstico.

Para coletar o pacote, navegue até **C:\Program Files\Cisco\AMP\X.X.X** (Onde X.X.X é a versão mais recente do AMP instalado no sistema) e execute o aplicativo **ipsupporttool.exe** esse processo cria um arquivo **.7z** na área de trabalho chamada **CiscoAMP_Support_Tool_%date%.7z**

Note: O Connector versão 6.2.3 e posterior pode solicitar um pacote remotamente, navegar para **Management > Computers**, expandir o registro do ponto final e usar a opção **Diagnose**.

Note: O pacote de diagnóstico também pode ser executado a partir de um prompt CMD com o comando: **"C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe"**, ou **"C:\Program**

Files\Cisco\AMP\X.X.X\ipsupporttool.exe" -o "X:\Folder\Can\Get\To", onde X.X.X é a versão mais recente do AMP instalada, o segundo comando pode ser usado para selecionar a pasta de saída para o arquivo .7z.

Faça a análise

Há duas maneiras de analisar um arquivo de diagnóstico:

- Diag_Analyzer.exe
- Amphandlecount.ps1

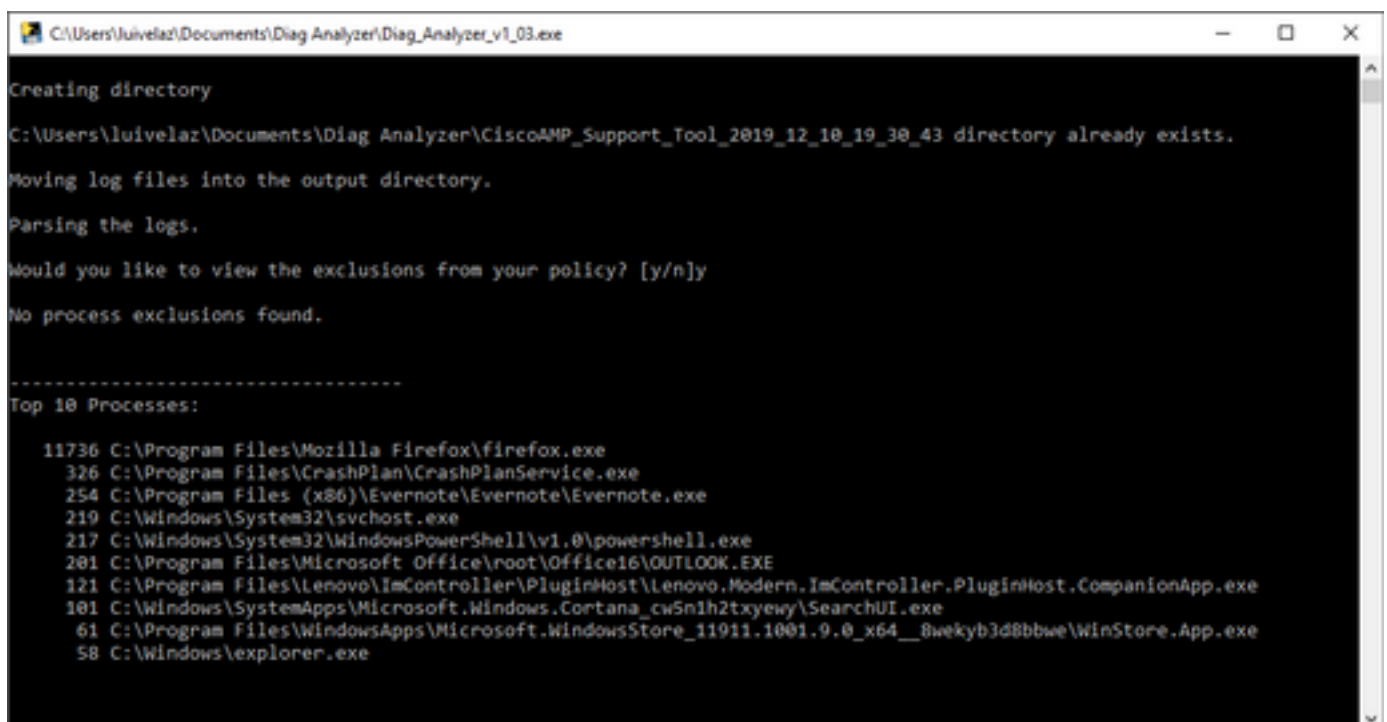
Diag_Analyzer.exe

Etapa 1. Faça o download do aplicativo [aqui](#).

Etapa 2. Na página GitHub, há um arquivo README com instruções adicionais sobre o uso.

Etapa 3. Copie o arquivo de diagnóstico CiscoAMP_Support_Tool_%date%.7z na mesma pasta em que Diag_Analyzer.exe está localizado.

Etapa 4. Executar o aplicativo 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.Modern.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
```

Etapa 5. No novo prompt, confirme se você deseja obter as exclusões da política com um Y ou um N.

Etapa 6. O resultado do script contém:

- 10 principais processos
- 10 principais arquivos
- 10 principais extensões
- 100 principais caminhos

- Todos os arquivos

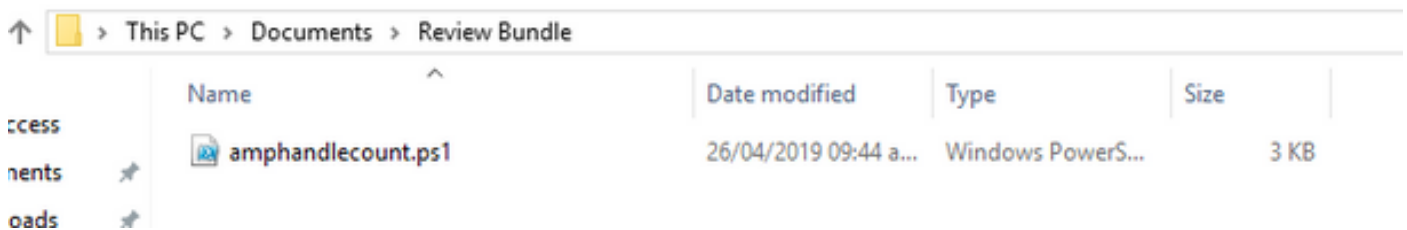
Note: Diag_Analyzer.exe verifica o arquivo de diagnóstico AMP fornecido para arquivos sfc.exe.log. em seguida, cria um novo diretório com o nome do arquivo de diagnóstico e armazena os arquivos de log fora do .7z, no diretório pai do diagnóstico, depois disso, ele analisa os logs e determina os 10 principais processos, arquivos, extensões e caminhos, finalmente, imprime informações na tela e também em um arquivo {Diagnostic}-summary.txt.

Amphandlecount.ps1

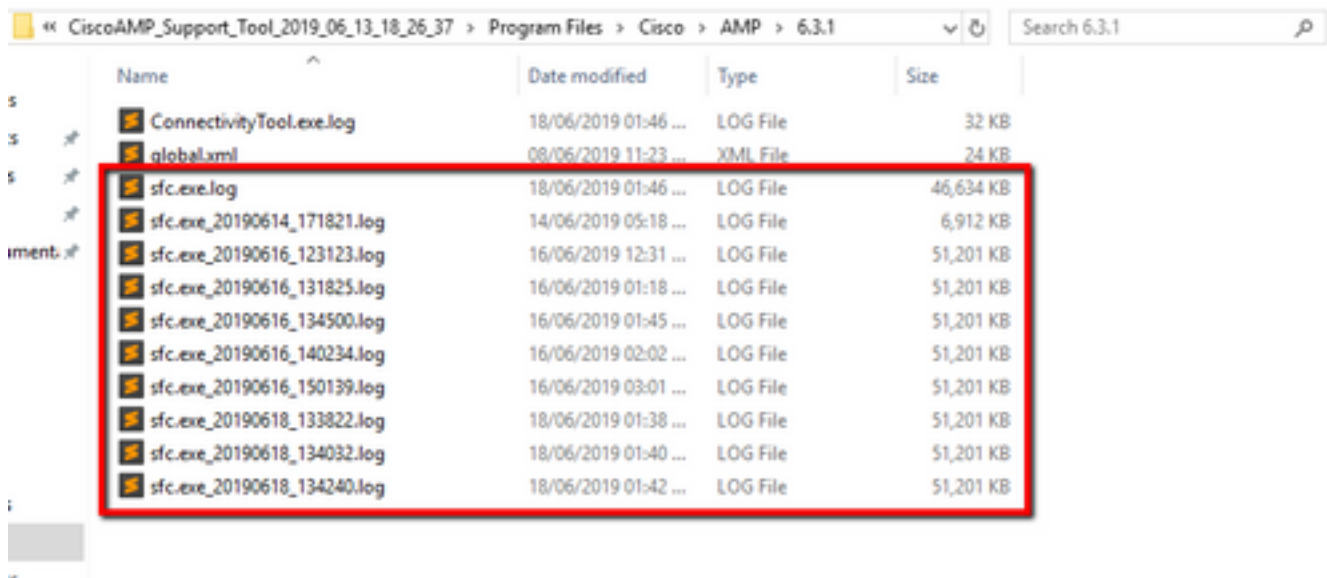
Etapa 1. Baixe o script **anphandlecounts.txt** da parte inferior desta comunidade após [Analisar arquivos digitalizados da AMP](#).

Etapa 2. Para executar o script no Windows, renomeie-o para **anphandlecount.ps1**.

Etapa 3. Para conveniência, copie o arquivo **anphandlecount.ps1** em uma pasta própria.



Etapa 4. Descompacte o arquivo **CiscoAMP_Support_Tool_%date%.7z** e identifique os arquivos **sfc.log** no caminho **CiscoAMP_Support_Tool_2019_06_13_18_26_37\Program Files\Cisco\AMP\X.X.X**.



Etapa 5. Copie os arquivos **sfc.log** na pasta **anphandlecount.ps1**.

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

Etapa 6. Execute o **anphandlecount.ps1** com o PowerShell e, em seguida, uma janela será aberta e, dependendo da política de execução no endpoint, poderá solicitar permissão para execução.

Tip: Para alterar a política de execução, abra um Windows PowerShell e use os próximos comandos:

Defina a política para permitir acesso de execução irrestrito - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted**

Defina a política para restringir o acesso à execução - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restricted**

Passo 7. Permita que o PowerShell termine (Pode demorar algum tempo, dependendo do número de sfc.log na pasta) após a conclusão do PowerShell, quatro arquivos são criados na pasta:

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

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

Etapa 8. Os 4 novos arquivos contêm o resultado da análise:

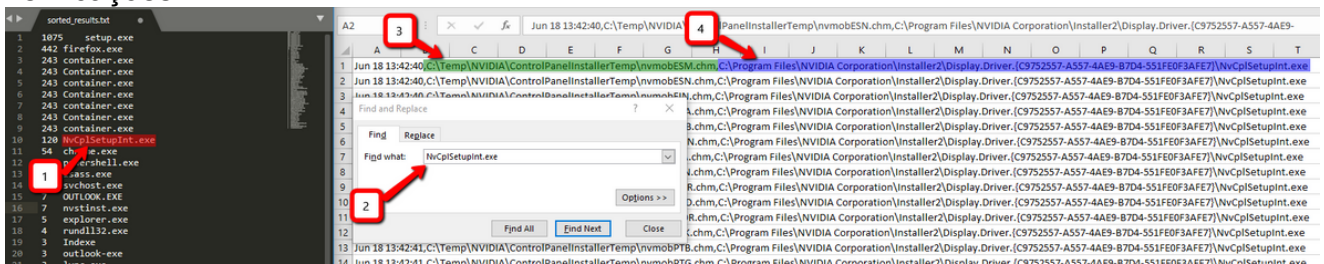
- **data.csv:** contém o caminho completo dos arquivos digitalizados e o processo pai que criou/modificou/moveu o arquivo
- **result.txt:** contém a lista de processos que são verificados pela AMP
- **sorted_results.txt:** contém a lista de processos que são verificados pela AMP com o processo mais verificado
- **terms.txt:** contém o nome dos processos analisados pela AMP

Etapa 9. Filtre o nome do processo com altas contagens do **sorted_results.txt** no **data.csv** você pode identificar o processo pai com seu caminho completo e continuar para adicionar uma exclusão à política em uma lista personalizada se ela for confiável.

Processos para procurar:

1. Ctrl + F em "data.csv" e pesquisa
2. Caminho do arquivo digitalizado pelo AMP
3. Caminho do processo pai que copia/move/modifica o arquivo

Note: Geralmente, a exclusão é do tipo "Processo: File Scan (Verificação de arquivo) com "Child Processes include" (Os processos filho incluem) para o processo pai que está recebendo as verificações:



Note: [Aqui](#) você pode encontrar mais informações relacionadas às práticas recomendadas para criar exclusões.

Ajustar exclusões

Depois que os processos ou caminhos forem identificados, você poderá adicioná-los à lista de exclusões vinculada à política aplicada no endpoint, navegue para **Gerenciamento > Exclusões > Nome da exclusão > Editar**, como mostrado na imagem.

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			

Envie o pacote para análise ao TAC

O TAC ATS pode ajudar a solucionar esses cenários; se for esse o caso, esteja pronto para fornecer as próximas informações sobre a criação do caso:

- Quando esse problema começa?
- Há alguma mudança recente?
- O problema ocorre com um determinado aplicativo? Em caso afirmativo, qual é o aplicativo?
- Há outro antivírus no sistema? Em caso afirmativo, qual antivírus?
- Colete um pacote de depuração enquanto o problema é reproduzido: [Etapas para coletar um pacote de depuração](#)