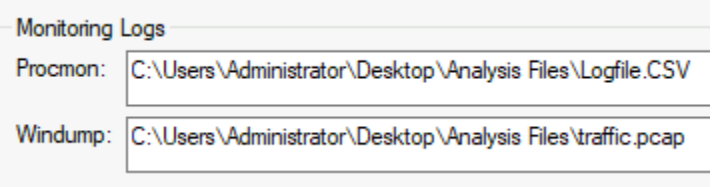
TryHackMe: Dunkle Materie

The following writeup covers the Dunkle Materie room on TryHackMe. It involves investigating a ransomware attack using ProcDOT, a tool that processes Process Monitor logfiles and PCAP-logs to generate a graph that visualises any relevant activities.

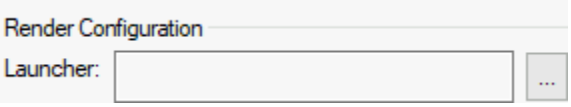
Scenario: The firewall alerted the Security Operations Centre that one of the machines at the Sales department, which stores all the customers' data, contacted the malicious domains over the network. When the Security Analysts looked closely, the data sent to the domains contained suspicious base64-encoded strings. The Analysts involved the Incident Response team in pulling the Process Monitor and network traffic data to determine if the host is infected. But once they got on the machine, they knew it was a ransomware attack by looking at the wallpaper and reading the ransomware note. Can you find more evidence of compromise on the host and what ransomware was involved in the attack?

Provide the two PIDs spawned from the malicious executable. (In the order as they appear in the analysis tool)

Start by launching ProcDOT and supplying the path of the Procmon and Windump logs:



After ProcDOT has analysed the Procmon log file, click the three-dot menu seen here:



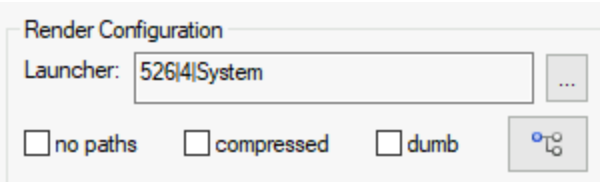
This will show you a list of processes found in the Procmon log file. After exploring the processes, I found two that stand out:

8644	exploreer.exe
1104	consent.exe
1796	DllHost.exe
7144	WpcTok.exe
5956	Conhost.exe
7128	exploreer.exe

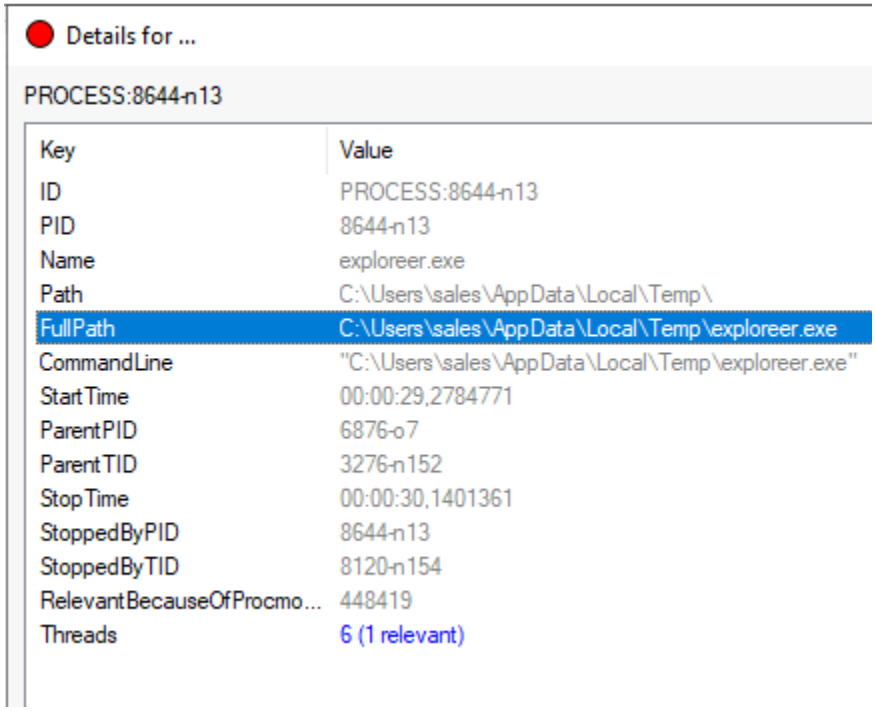
These are clearly trying to impersonate explorer.exe, and therefore the answer is 8644,7129.

Provide the full path where the ransomware initially got executed?

When you open the three-dot menu, select the system process like as follows:



We can now look for the suspicious process we identified earlier, right click it and select details:



Note, press CTRL+F and enter "exploreer.exe" to find the process in the graph.

This ransomware transfers the information about the compromised system and the encryption results to two domains over HTTP POST. What are the two C2 domains?

If you look at the other suspicious process we identified (PID 7128), you can see that it makes connects to:

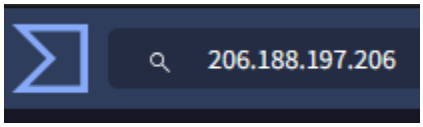
- 146.112.61.108
- 206.188.197.206

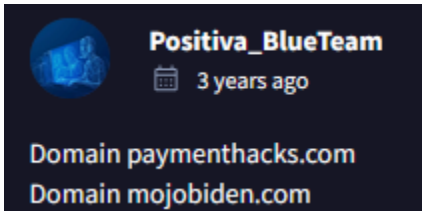
Let's dig deeper into the network traffic by using Wireshark. Once you have opened the pcap up in Wireshark, lets filter for HTTP POST requests made to these addresses:

http.request.method == POST

No.	Time	Source	Destination	Protocol	Length	Host	Info
5643	606.816386	192.168.75.232	146.112.61.108	HTTP	923	mojobiden.com	POST /?gAAyj3aK=9vYQ0N9cS&rGE=Fqqx

Theres only one POST request and it is made to mojobiden.com. This is likely one C2 domain, lets try to find the other one by searching for the IP in VirusTotal:





Please note, several other domains were identified by this comment, however, the two seen in the image above is the answer.

What are the IPs of the malicious domains?

We found these earlier: 146.112.61.108,206.188.197.206.

Provide the user-agent used to transfer the encrypted data to the C2 channel?

```
User-Agent: Firefox/89.0\r\n
```

Aka Firefox/89.0.

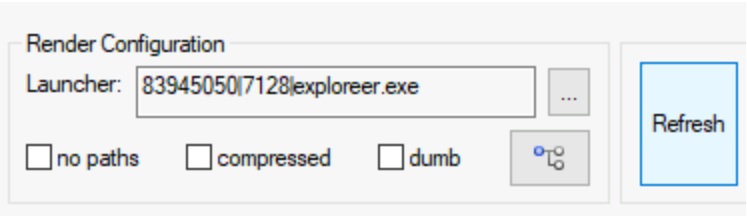
Provide the cloud security service that blocked the malicious domain.

If you right-click on the POST request we identified earlier and select follow TCP stream, you can see that Cisco Umbrella has blocked the malicious domain:

```
HTTP/1.1 403 Forbidden
Server: Cisco Umbrella
Date: Sat, 21 Aug 2021 20:40:29 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
```

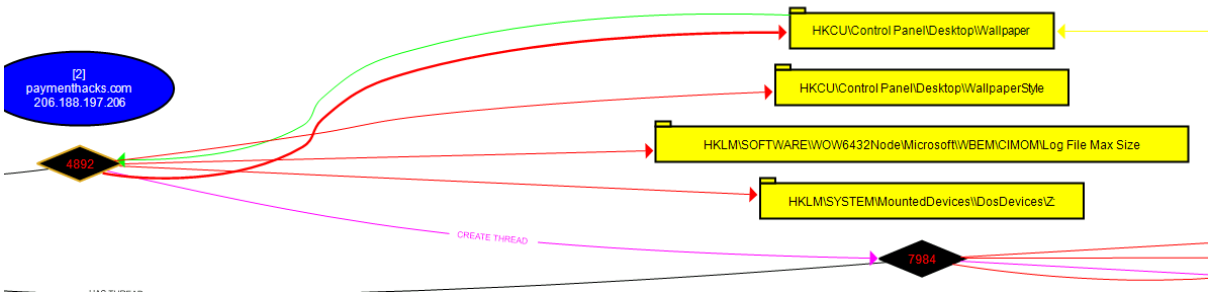
Provide the name of the bitmap that the ransomware set up as a desktop wallpaper.

To answer this question, its best to only analyse the malicious process we found earlier (PID 7128) rather than all processes:



The wallpaper file is ley9kpi9r.bmp.

Find the PID (Process ID) of the process which attempted to change the background wallpaper on the victim's machine.



As you can see, a process with the PID 4892 attempted to change the wallpaper.

The ransomware mounted a drive and assigned it the letter. Provide the registry key path to the mounted drive, including the drive letter.

You can see the same process that attempted to change the wallpaper, also mounted a drive:

HKLM\SYSTEM\MountedDevices\DosDevices\Z:

Now you have collected some IOCs from this investigation. Provide the name of the ransomware used in the attack.

The name of the ransomware is Blackmatter (the answer is Blackmatter Ransomware). This can be found by using VirusTotal:

This was a really enjoyable room, especially if you have a fundamental understanding of malware analysis. If you need any help with the questions, feel free to reach out and ask.