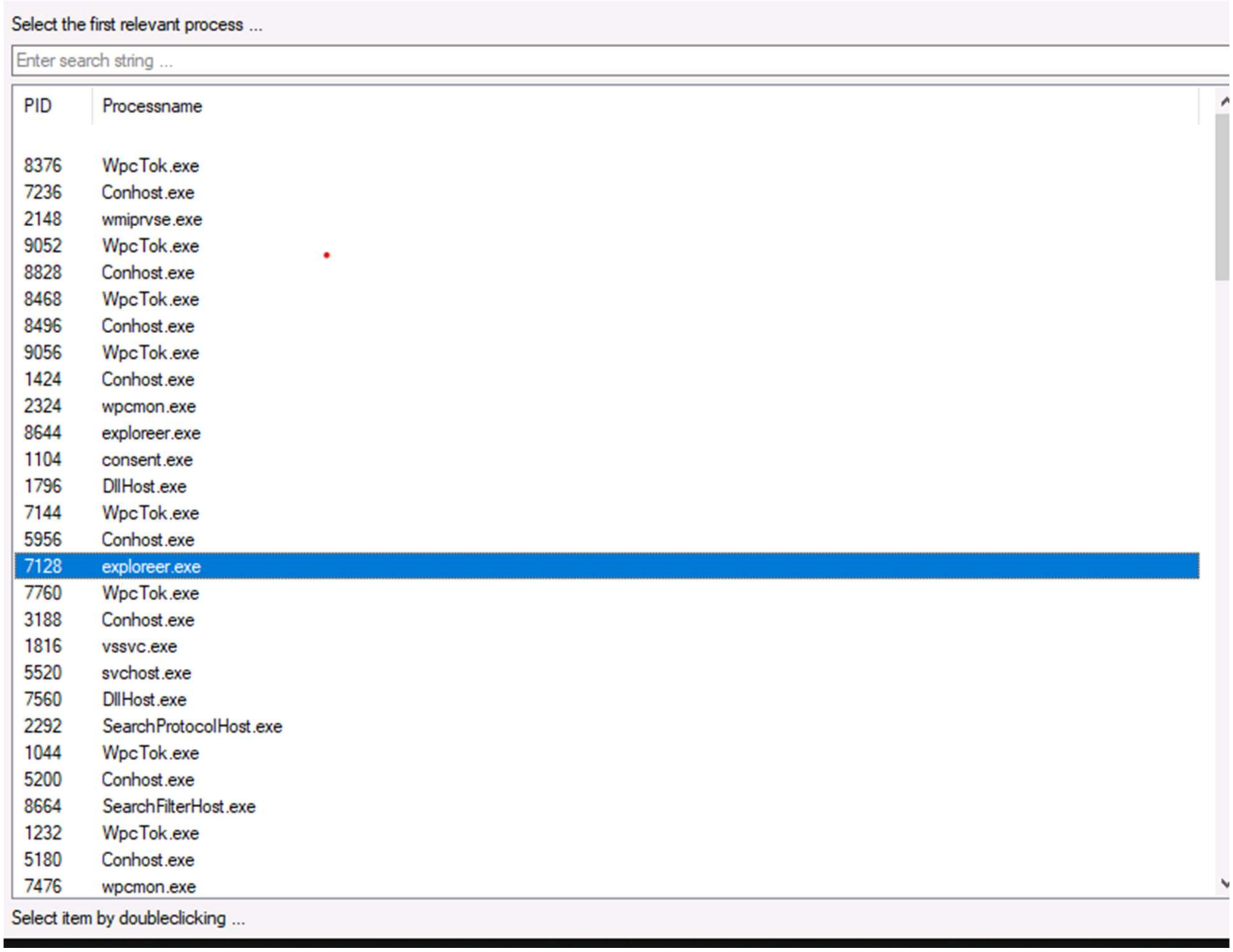
First: load the file and press the launcher button.After analyzing a gui pops up showing pids and processname. There seems to be an odd processname running i.e exploreer.exe . From that we can get the pid and our first flag

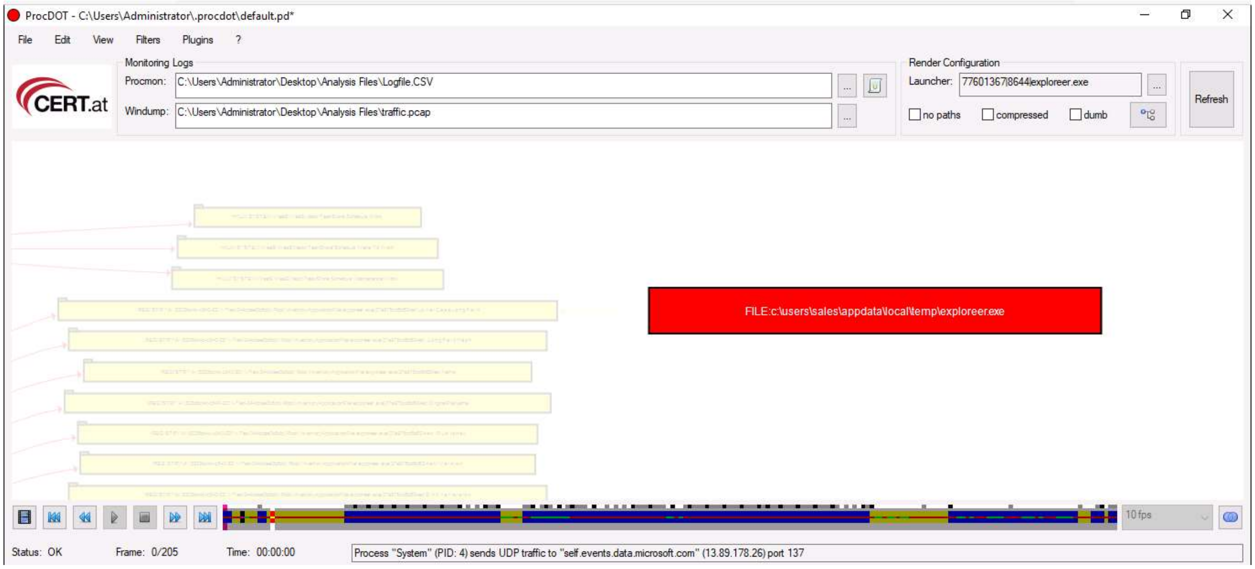


Select the first relevant process ...

PID	Processname
8376	WpcTok.exe
7236	Conhost.exe
2148	wmiprvse.exe
9052	WpcTok.exe
8828	Conhost.exe
8468	WpcTok.exe
8496	Conhost.exe
9056	WpcTok.exe
1424	Conhost.exe
2324	wpcmon.exe
8644	exploreer.exe
1104	consent.exe
1796	DllHost.exe
7144	WpcTok.exe
5956	Conhost.exe
7128	exploreer.exe
7760	WpcTok.exe
3188	Conhost.exe
1816	vssvc.exe
5520	svchost.exe
7560	DllHost.exe
2292	SearchProtocolHost.exe
1044	WpcTok.exe
5200	Conhost.exe
8664	SearchFilterHost.exe
1232	WpcTok.exe
5180	Conhost.exe
7476	wpcmon.exe

Select item by doubleclicking ...

Second: Then we open the first exploreer.exe processname. Then by going on exploreer.exe thread we can see a box at the right most corner which shows the path to exploreer.exe which is our second flag.



ProcDOT - C:\Users\Administrator\.procdot\default.pd*

Monitoring Logs

Procmon: C:\Users\Administrator\Desktop\Analysis Files\Logfile.CSV

Windump: C:\Users\Administrator\Desktop\Analysis Files\traffic.pcap

Render Configuration

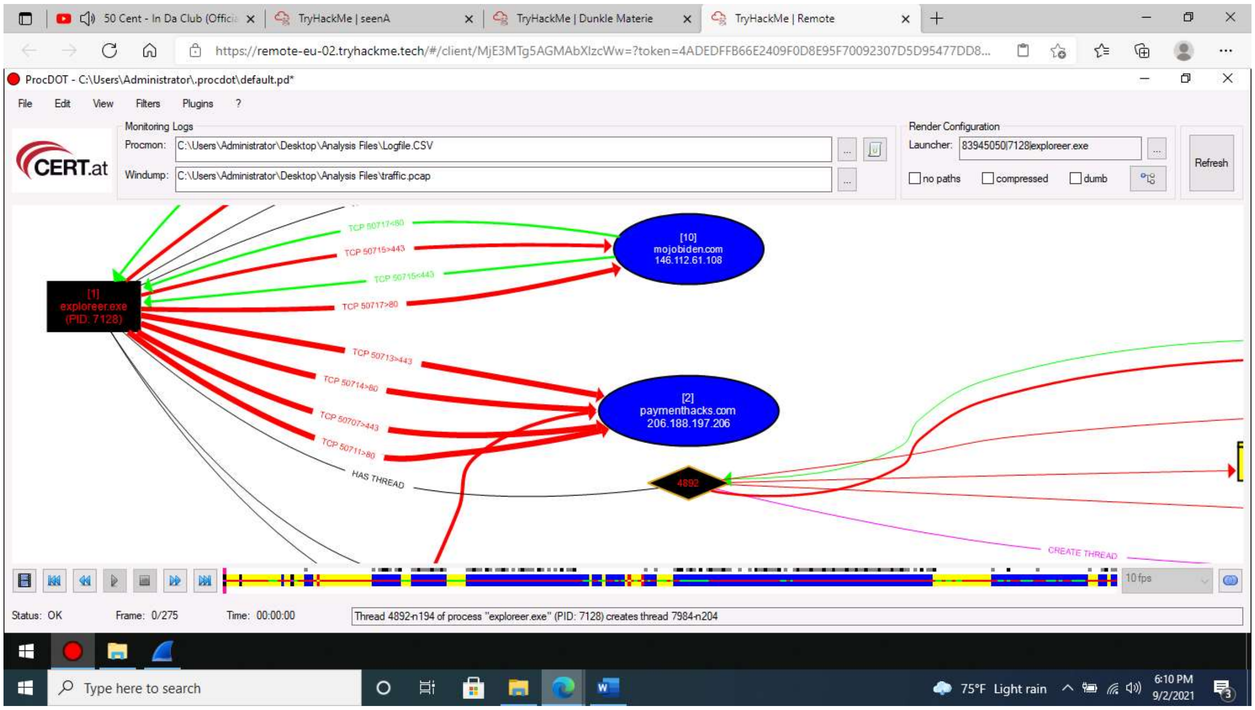
Launcher: 77601367|8644|exploreer.exe

□ no paths □ compressed □ dumb

Status: OK Frame: 0/205 Time: 00:00:00

Process "System" (PID: 4) sends UDP traffic to "self.events.data.microsoft.com" (13.89.178.26) port 137

Third: By opening pid 7128 or exploreer.exe second pid and looking at the pcap box we can see that most of the domains seems to be legit except these two mojobiden.com,paymenthacks.com. We can also view that at wireshark.



https://remote-eu-02.tryhackme.tech/#/client/MjE3MTg5AGMAbXlzcWw=?token=4ADEDFFB66E2409F0D8E95F70092307D5D95477DD8...

ProcDOT - C:\Users\Administrator\.procdot\default.pd*

Monitoring Logs

Procmon: C:\Users\Administrator\Desktop\Analysis Files\Logfile.CSV

Windump: C:\Users\Administrator\Desktop\Analysis Files\traffic.pcap

Render Configuration

Launcher: 83945050|7128|exploreer.exe

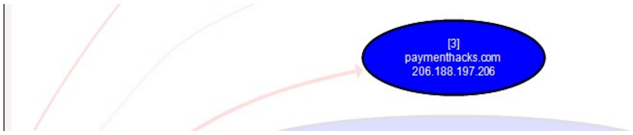
□ no paths □ compressed □ dumb

Status: OK Frame: 0/275 Time: 00:00:00

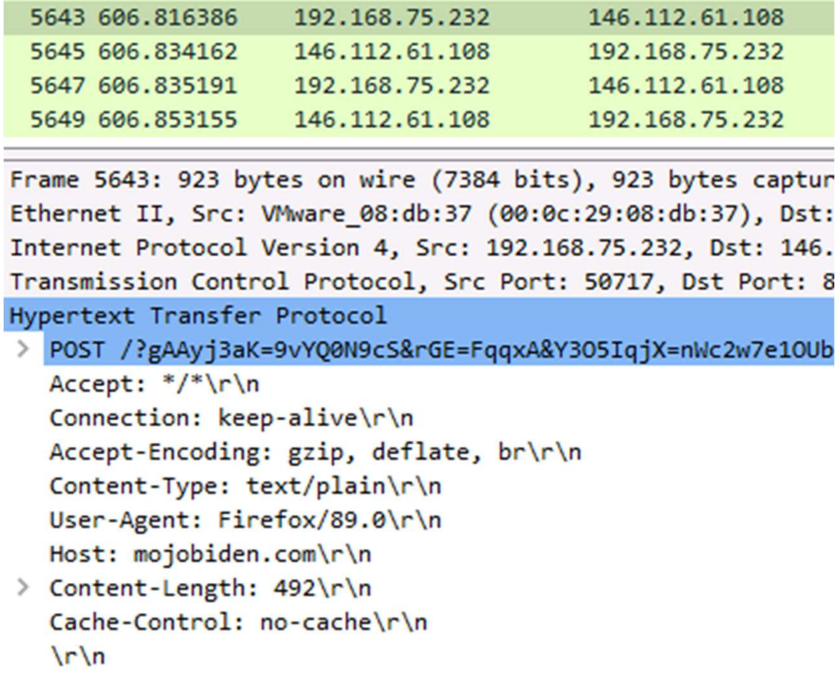
Thread 4892-n194 of process "exploreer.exe" (PID: 7128) creates thread 7984-n204

Fourth : open the pacp file and the wireshark will be opened. Go to statistics and conversations. Then you will se victim Ip communicating with the malicious domain IP.

We can see the Ip on the chart with the domain name also.

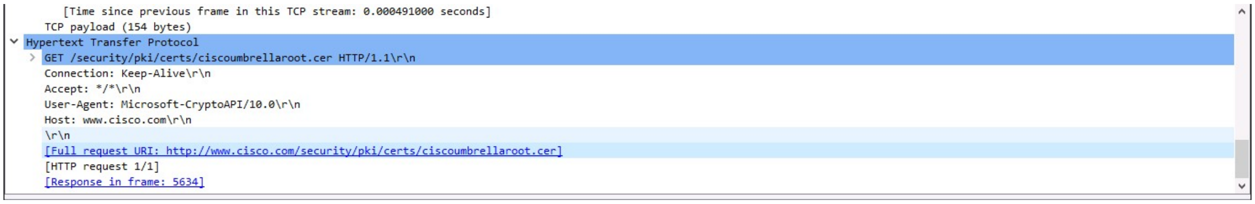


Fifth: by adding filter to http on wireshark we can then see some request at bottom sending .When opening the packet and going on to http protocol we can get the browser info at user-agent header.



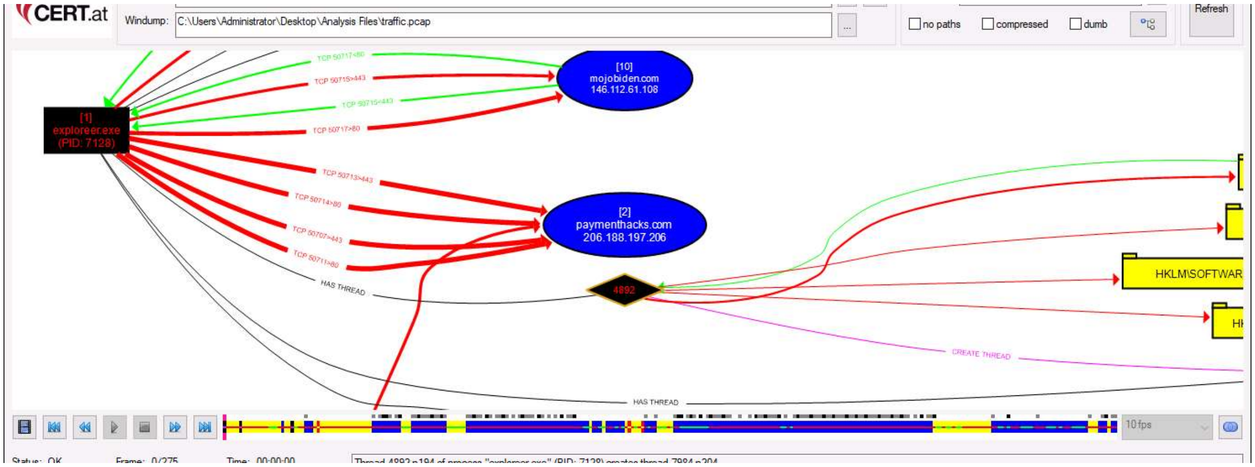
```
 5643 606.816386    192.168.75.232       146.112.61.108
 5645 606.834162    146.112.61.108       192.168.75.232
 5647 606.835191    192.168.75.232       146.112.61.108
 5649 606.853155    146.112.61.108       192.168.75.232

Frame 5643: 923 bytes on wire (7384 bits), 923 bytes captur
Ethernet II, Src: VMware_08:db:37 (00:0c:29:08:db:37), Dst:
Internet Protocol Version 4, Src: 192.168.75.232, Dst: 146.
Transmission Control Protocol, Src Port: 50717, Dst Port: 8
Hypertext Transfer Protocol
 > POST /?gAAyj3aK=9vYQ0N9cS&rGE=FqqxA&Y3O5IqjX=nWc2w7e1OUb
   Accept: */*\r\n
   Connection: keep-alive\r\n
   Accept-Encoding: gzip, deflate, br\r\n
   Content-Type: text/plain\r\n
   User-Agent: Firefox/89.0\r\n
   Host: mojobiden.com\r\n
 > Content-Length: 492\r\n
   Cache-Control: no-cache\r\n
   \r\n
```

Sixth: In a http get request we can see a get request on /security/... we can see the cloud security there.



```
      [Time since previous frame in this TCP stream: 0.000491000 seconds]
    TCP payload (154 bytes)
v Hypertext Transfer Protocol
  > GET /security/pki/certs/ciscoumbrellaroot.cer HTTP/1.1\r\n
    Connection: Keep-Alive\r\n
    Accept: */*\r\n
    User-Agent: Microsoft-CryptoAPI/10.0\r\n
    Host: www.cisco.com\r\n
    \r\n
    [Full request URI: http://www.cisco.com/security/pki/certs/ciscoumbrellaroot.cer]
    [HTTP request 1/1]
    [Response in frame: 5634]
```

Seventh and eight: opening the 7128 process after launching . we can se exploreer.exe thread where we can get the image file and pid

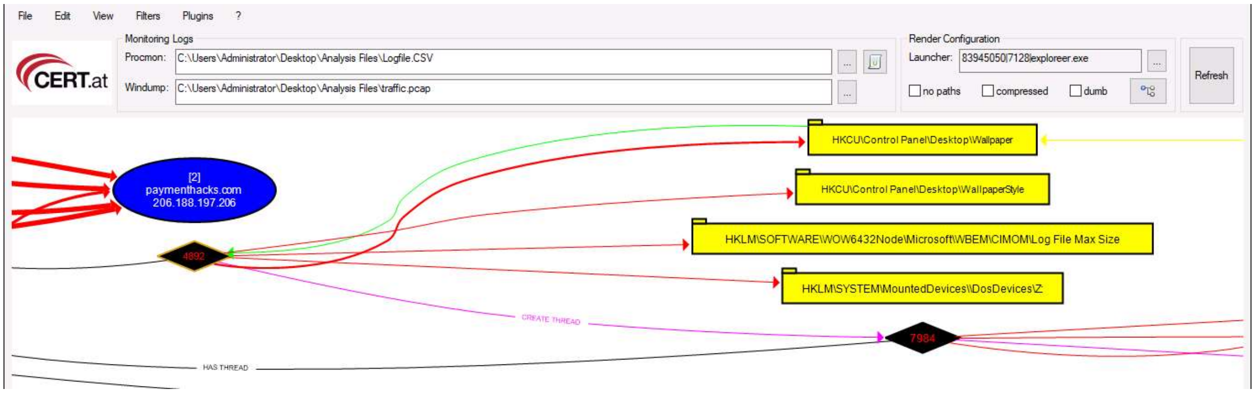


Windump: C:\Users\Administrator\Desktop\Analysis Files\traffic.pcap

□ no paths □ compressed □ dumb

Status: OK Frame: 0/275 Time: 00:00:00 Thread 4892 n194 of process "exploreer.exe" (PID: 7128) creates thread 7984 n204

Ninth: On the same thread we can get the answer..



Monitoring Logs

Procmon: C:\Users\Administrator\Desktop\Analysis Files\Logfile.CSV

Windump: C:\Users\Administrator\Desktop\Analysis Files\traffic.pcap

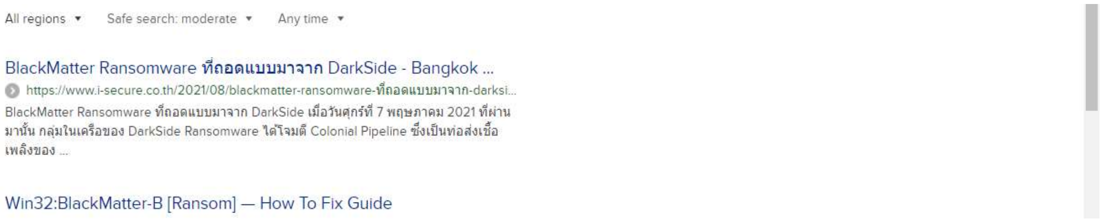
Render Configuration

Launcher: 83945050|7128|exploreer.exe

□ no paths □ compressed □ dumb

File
Edit
View
Filters
Plugins
?
CERT.at
Refresh
[2]
paymenthacks.com
206.188.197.206
4892
HKCU\Control Panel\Desktop\Wallpaper
HKCU\Control Panel\Desktop\WallpaperStyle
HKLM\SOFTWARE\WOW6432Node\Microsoft\WBEM\CIMOM\Log File Max Size
HKLM\SYSTEM\MountedDevices\\DosDevices\Z:
CREATE THREAD
7984
HAS THREAD

Tenth: by doing google dork on the domain name which we found earlier will leads to the final answer



BlackMatter Ransomware ที่ถอดแบบมาจาก DarkSide - Bangkok ...

https://www.i-secure.co.th/2021/08/blackmatter-ransomware-ที่ถอดแบบมาจาก-darksi...

BlackMatter Ransomware ที่ถอดแบบมาจาก DarkSide เมื่อวันศุกร์ที่ 7 พฤษภาคม 2021 ที่ผ่านมานั้น กลุ่มในเครือของ DarkSide Ransomware ได้โจมตี Colonial Pipeline ซึ่งเป็นท่อส่งเชื้อเพลิงของ ...

Win32:BlackMatter-B [Ransom] — How To Fix Guide