

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



TRY HACK ME: Write-Up Dunkle Materie — Ransomware Investigation using ProcDOT



Shefali Kumari · Following

4 min read · Dec 10, 2021

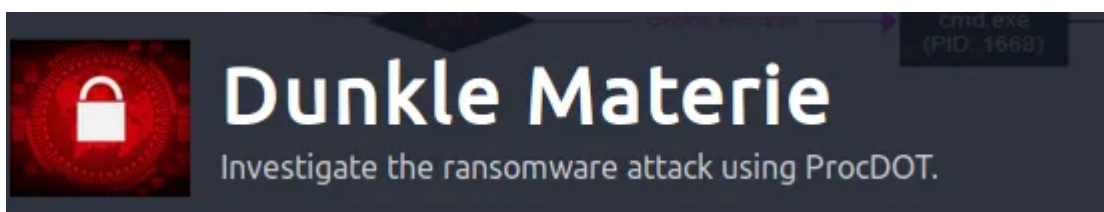


Listen



Share

... More



Task 1 Ransomware Investigation–

The firewall alerted the Security Operations Center 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?

ProcDOT visualizes results on the basis of Process Monitoring logs and Network Traffic logs.

Answer to the questions of this section–

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

Correct Answer

Provide the full path where the ransomware initially got executed? (Include the full path in your answer)

Correct Answer

Hint

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? (no space in the answer)

Correct Answer

What are the IPs of the malicious domains? (no space in the answer)

Correct Answer

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

Correct Answer

Hint

Provide the cloud security service that blocked the malicious domain.

Correct Answer

Hint

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

Correct Answer

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

Correct Answer

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

Correct Answer

Now you have collected some IOCs from this investigation. Provide the name of the ransomware used in the attack. (external research required)

Correct Answer

Answers-

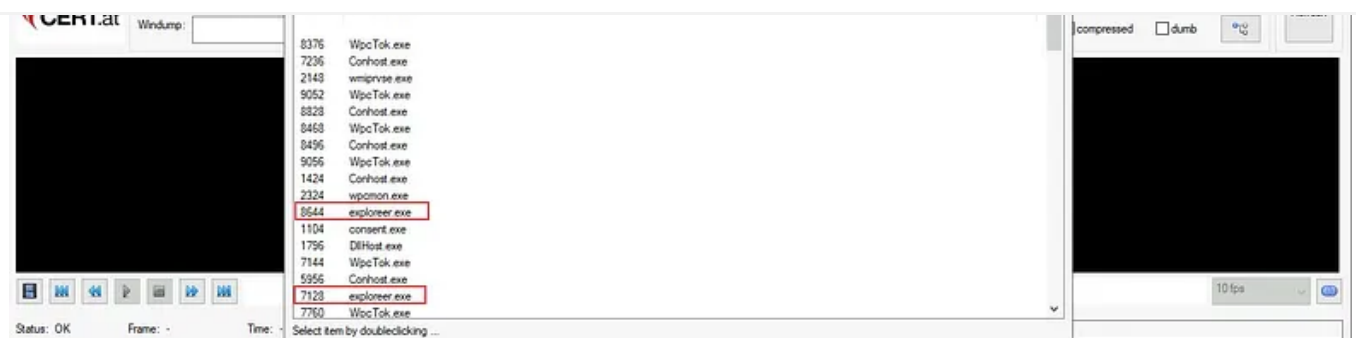
1) Within Monitoring Logs, select Procmon file from Desktop -> Analysis Files -> CSV file. Navigate under Render Configuration hit the launcher button.

2) After this we will be prompted to select the first relevant process name to start the analysis with. I have identified PID — 8644 and 7128 with suspicious process names

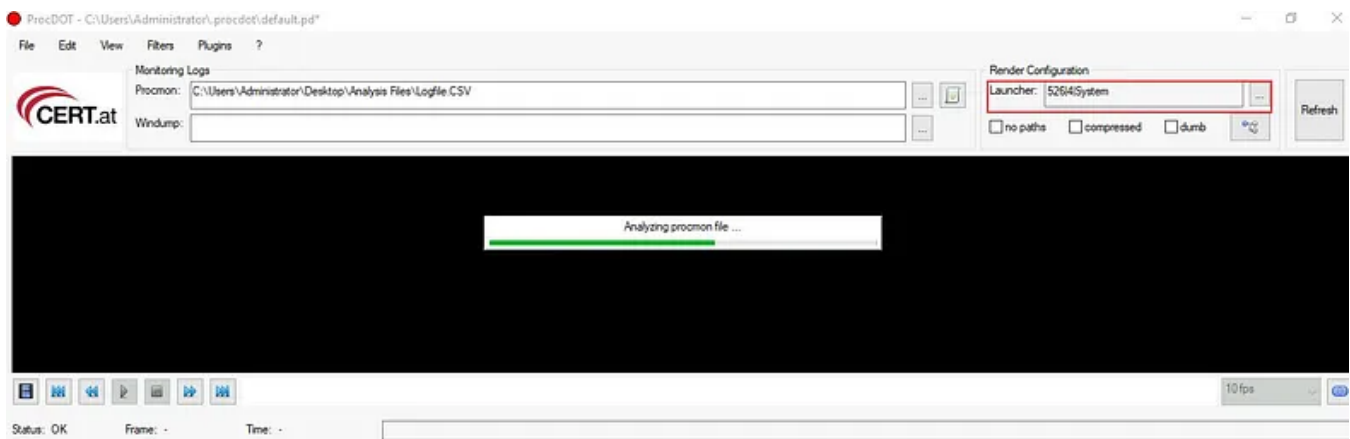
Open in app ↗

Medium

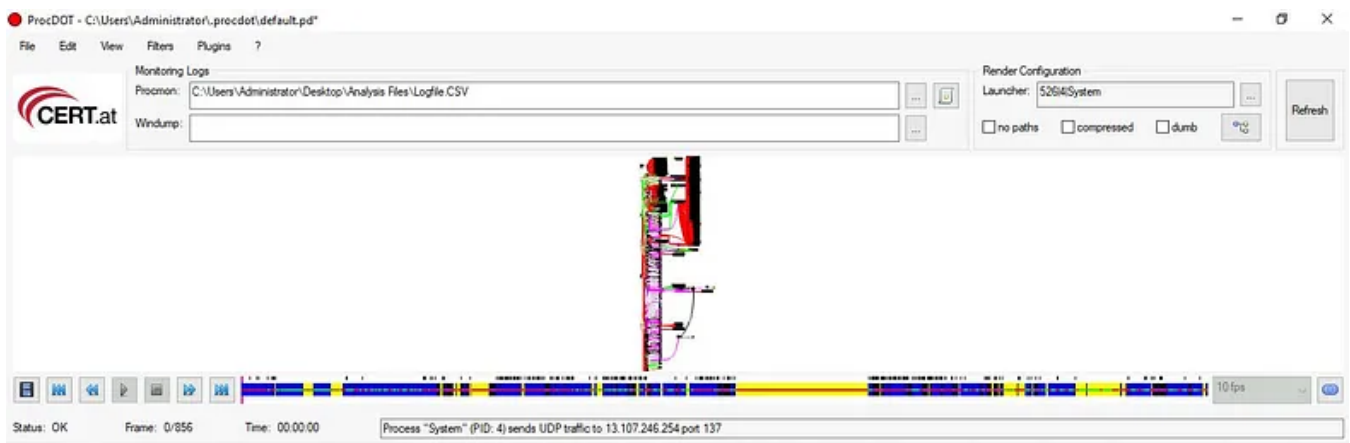
Search



3) Select process name — System, double click on System, and then click on Refresh to visualize.



We will get something like mentioned below.



Zoom in and look for the process itself. [Make use of View tab -> Graph]

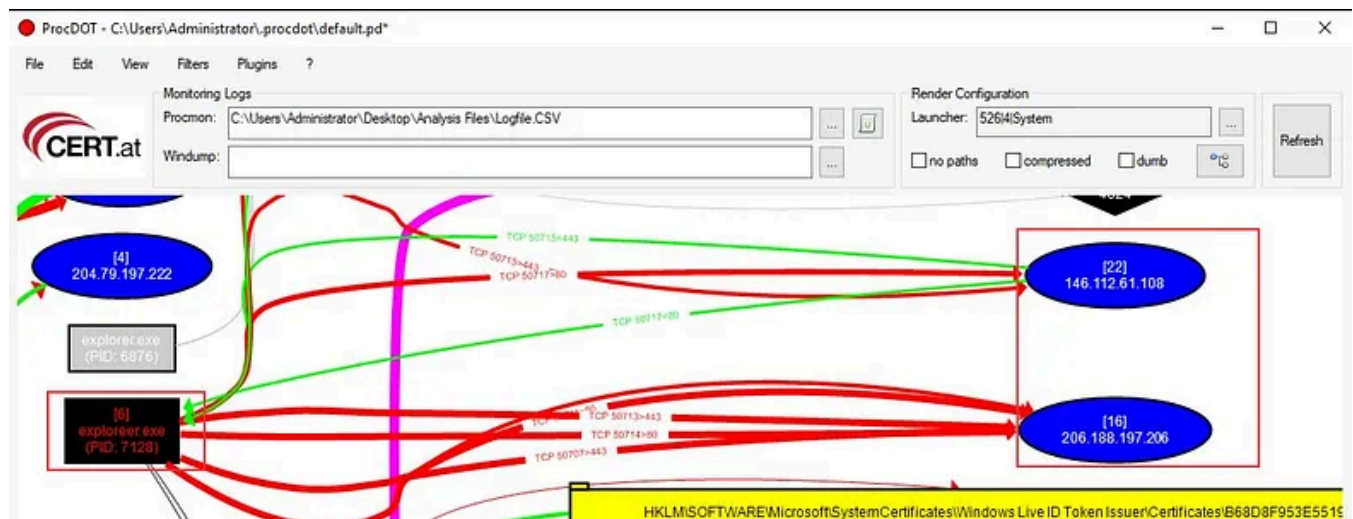
Right-click on PID-8644 explorer.exe and select Details to view Full Path.



4) Look at PID-7128 exploreer.exe and map mentioned IP addresses related to explorer.exe in Wireshark.

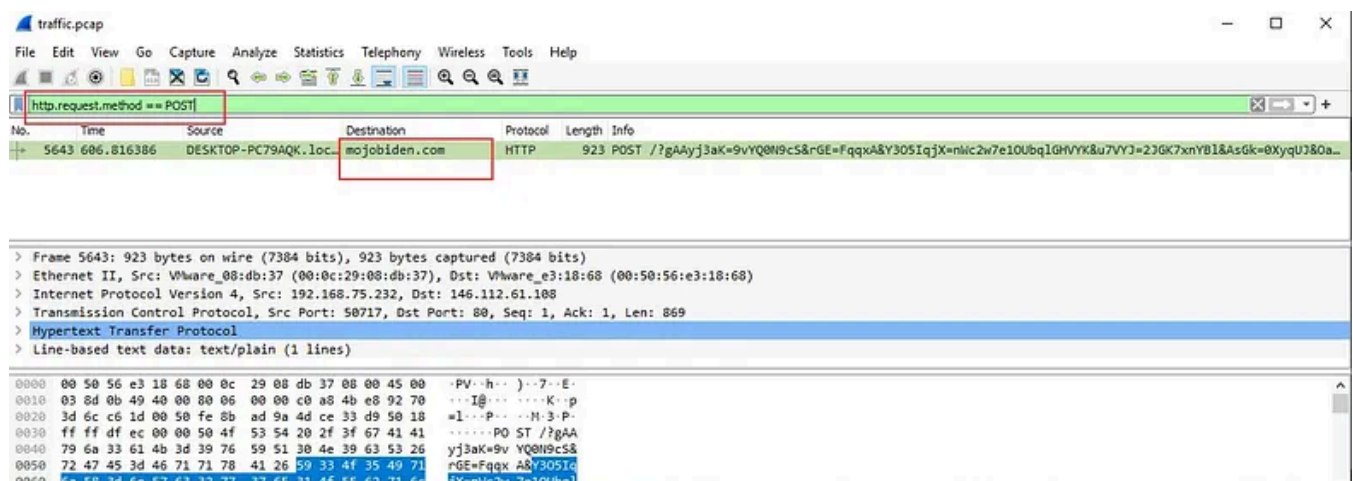
IP address1- 146.112.61.108

IP address 2- 206.188.197.206



Now type `http.request.method == POST` as filter in wireshark and navigate to Edit -> preferences -> Name Resolution -> enable resolve network (IP) addresses.

Domain 1- mojobiden.com



Domain 2- paymenthacks.com

Domain 2 is identified using Threat Hunting Skills by searching information for IP- 206.188.197.206 on Virus Total.

206.188.197.206 (206.188.196.0/23)
AS 399629 (BLNWX)

1 security vendor flagged this IP address as malicious

Community Score: 1/90

DETECTION DETAILS RELATIONS COMMUNITY 10

Contained In Graphs

| Source | Malware | Detection Date |
|-------------------|---|---------------------|
| octohat | Cobalt Strike | 2021-06-28 18:40:42 |
| bgreksza | Blackmatter_Retrohunt_24_10_2021_bgreksza | 2021-10-24 18:43:47 |
| octohat | Cobalt Strike | 2021-11-12 06:20:03 |
| cert_esec | blackmatter | 2021-10-02 19:08:46 |
| nahberry | BlackMatter | 2021-08-02 13:34:58 |
| christianblueteam | Black Matter | 2021-08-05 22:50:19 |
| CTIN_Global | DarkMatter-RW 2021-08-08 | 2021-08-08 23:06:56 |
| CTIN_Global | BlackMatter-Sept10-2021 | 2021-09-10 23:36:27 |

Comments

TinesAtSides
27 days ago
IP Found in <https://ankura.com/insights/ankura-cyber-threat-intelligence-bulletin-8/>

Domain 2 identified.

206.188.197.206

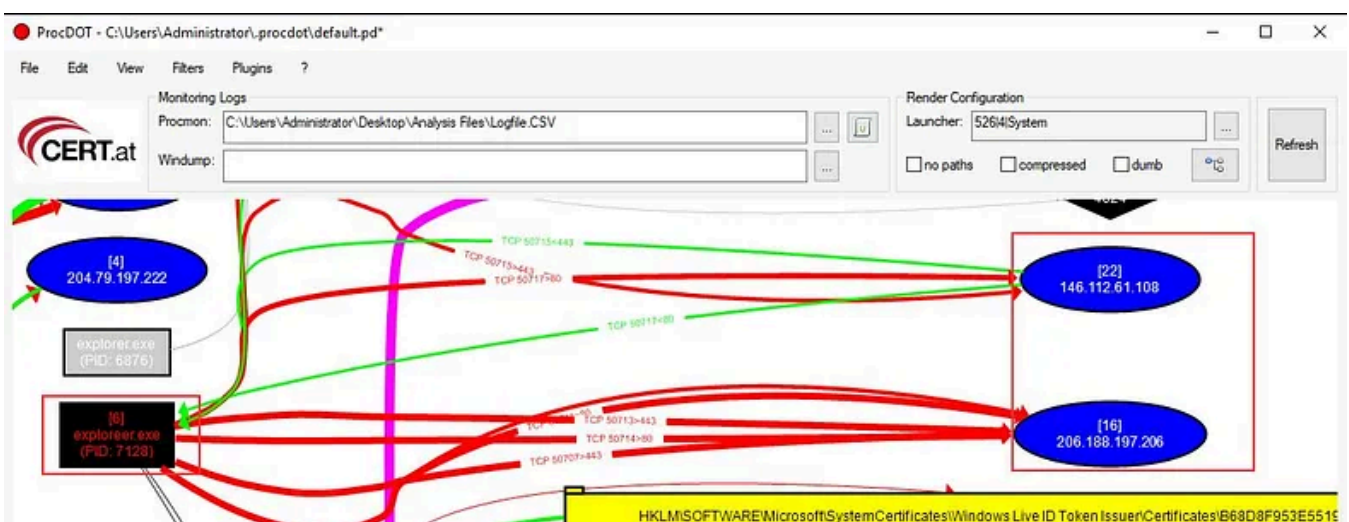
| Source | Malware | Detection Date |
|-------------------|--------------------------|---------------------|
| nahberry | BlackMatter | 2021-08-02 13:34:58 |
| christianblueteam | Black Matter | 2021-08-05 22:50:19 |
| CTIN_Global | DarkMatter-RW 2021-08-08 | 2021-08-08 23:06:56 |
| CTIN_Global | BlackMatter-Sept10-2021 | 2021-09-10 23:36:27 |

Comments

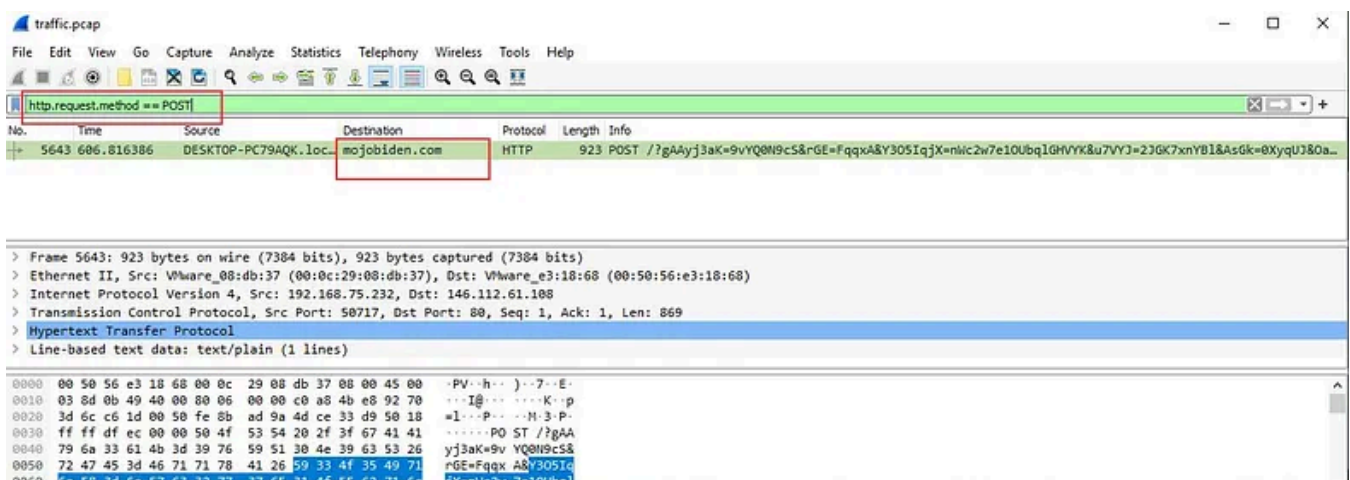
TinesAtSides
27 days ago
IP Found in <https://ankura.com/insights/ankura-cyber-threat-intelligence-bulletin-8/>

Positive_BlueTeam
3 months ago
Domain paymenthacks.com
Domain mojobiden.com

5) Malicious IP address for the identified domains are mentioned below



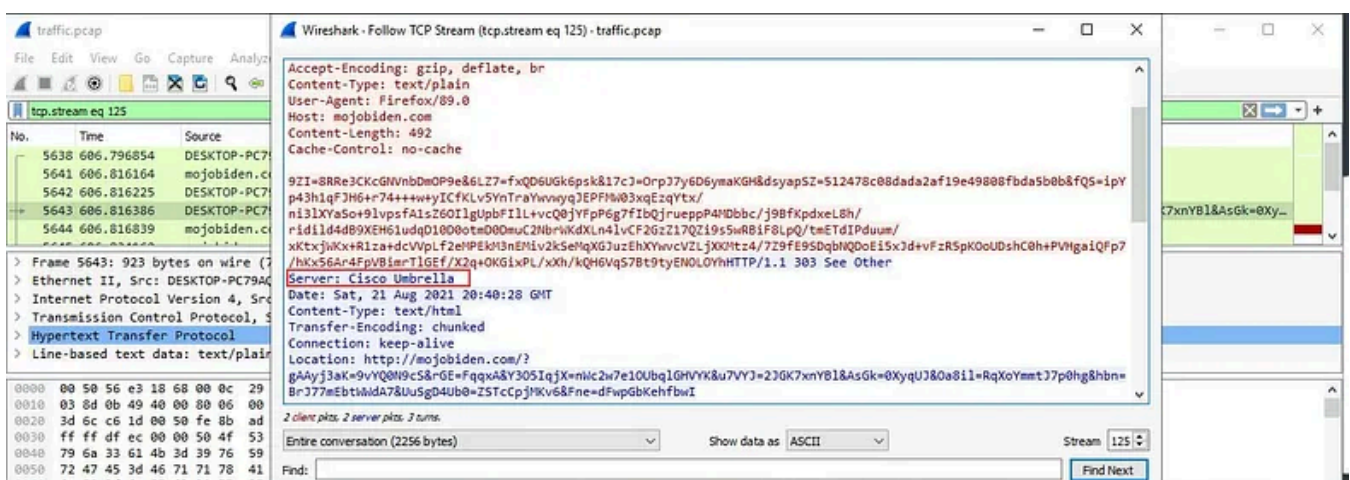
6) Now type `http.request.method == POST` as filter in Wireshark and navigate to Edit -> preferences -> Name Resolution -> enable resolve network (IP) addresses.



Following TCP Stream for the traffic mentioned above, we will get User-Agent for the same.



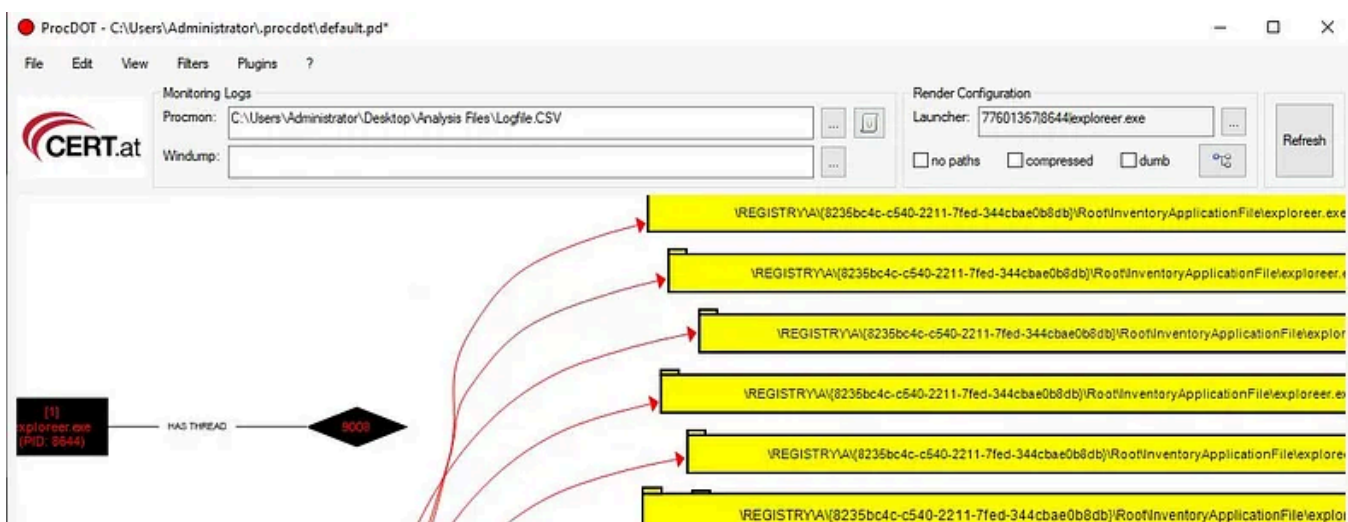
7) Follow TCP Stream for the domain -mojobiden.com



8) Now in ProcDot, click the launcher button to view the process listing. Select PID-7128 explorer.exe and double click on 7128 explorer.exe



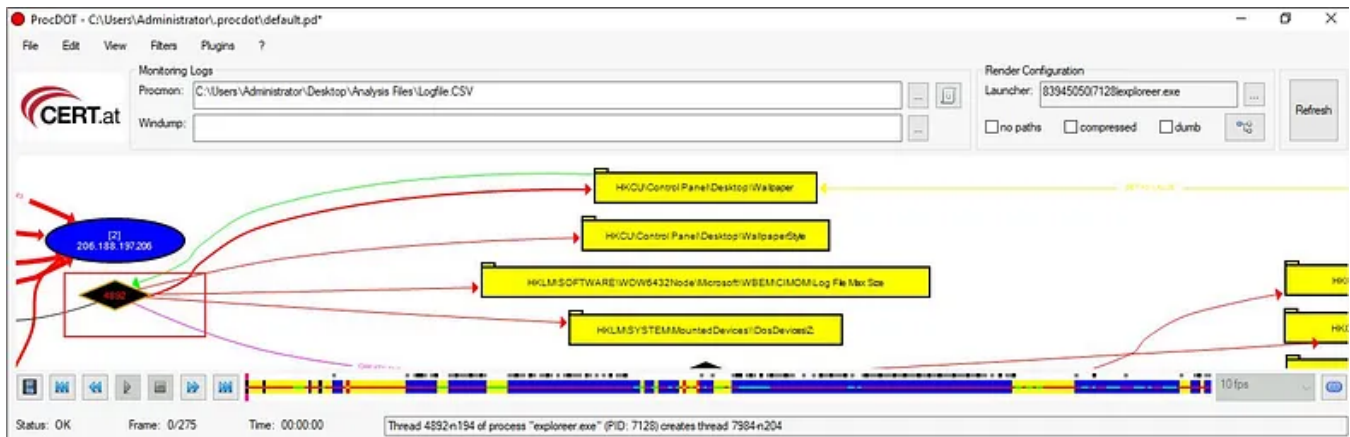
Now visualize PID-7128 explorer.exe



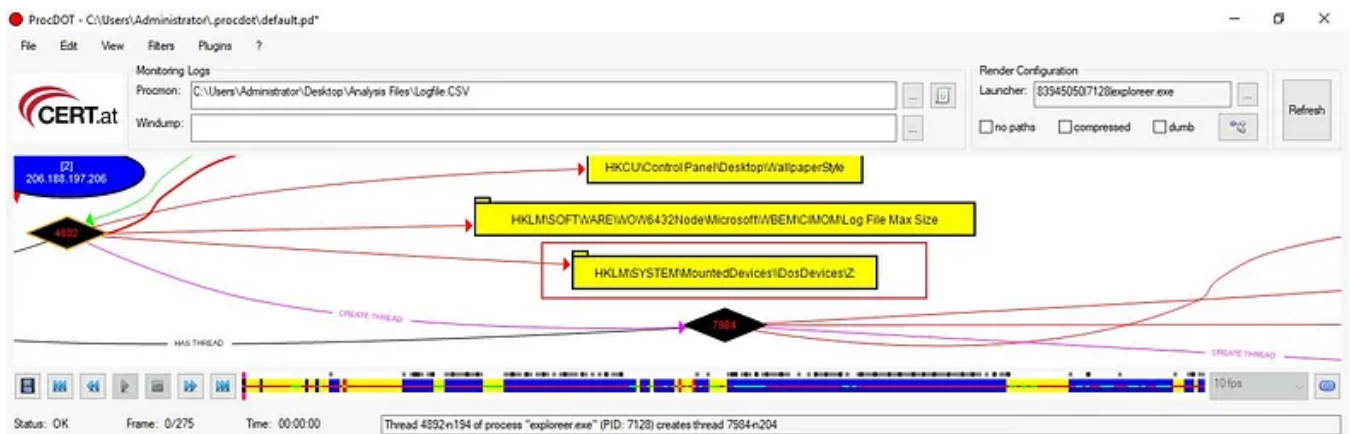
9) Answer 7 — ley9kpi9r.bmp



10) Answer 8- 4892



11) Answer 10- HKLM\SYSTEM\MountedDevices\\DosDevices\Z:



12) Answer 11- black matter ransomware

Visit AlienVault or Virus Total with IOCs to fetch the ransomware names.

| DETECTION | DETAILS | RELATIONS | COMMUNITY |
|---------------------|---|-----------|---------------------|
| Contained In Graphs | | | 10 |
| octohat | Cobalt Strike | | 2021-06-28 18:40:42 |
| bgreksza | Blackmatter_Retrohunt_24_10_2021_bgreksza | | 2021-10-24 18:43:47 |
| octohat | Cobalt Strike | | 2021-11-12 06:20:03 |
| cert_esec | blackmatter | | 2021-10-02 19:08:46 |
| nahberry | BlackMatter | | 2021-08-02 13:34:58 |
| christianblueteam | Black Matter | | 2021-08-05 22:50:19 |
| CTIN_Global | DarkMatter-RW 2021-08-08 | | 2021-08-08 23:06:56 |
| CTIN_Global | BlackMatter-Sept10-2021 | | 2021-09-10 23:36:27 |

That is all for this Write-up, hoping this will help you in solving the challenges of Dunkle Materie. Have Fun and Enjoy Hacking! Do visit other rooms and modules on TryHackMe for more learning.

-by Shefali Kumari

Tryhackme Writeup

Dunkle Materie

Ransomware

Wireshark

Malware Analysis



Following

Written by Shefali Kumari

383 Followers · 17 Following

Love Learning about Malware analysis, Threat hunting, Network Security and Incident Response Management professionally | <https://youtube.com/channel/UCf-F-eATCU>

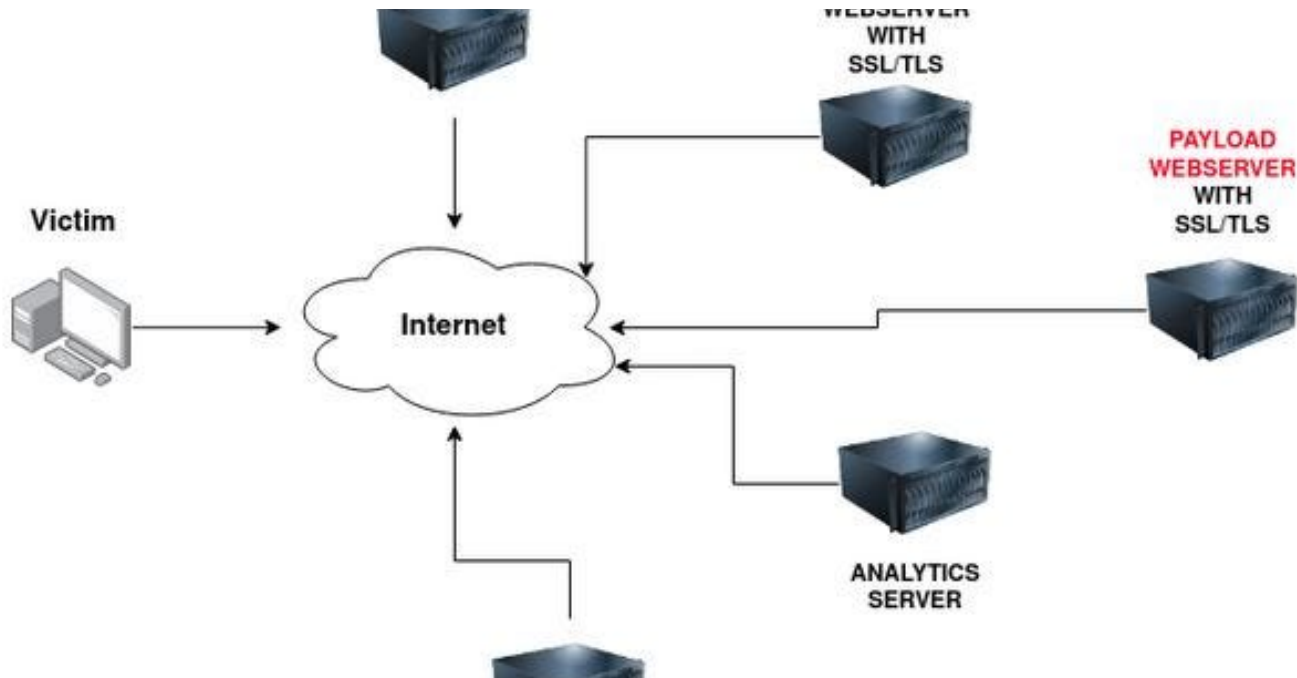
No responses yet



What are your thoughts?

Respond

More from Shefali Kumari

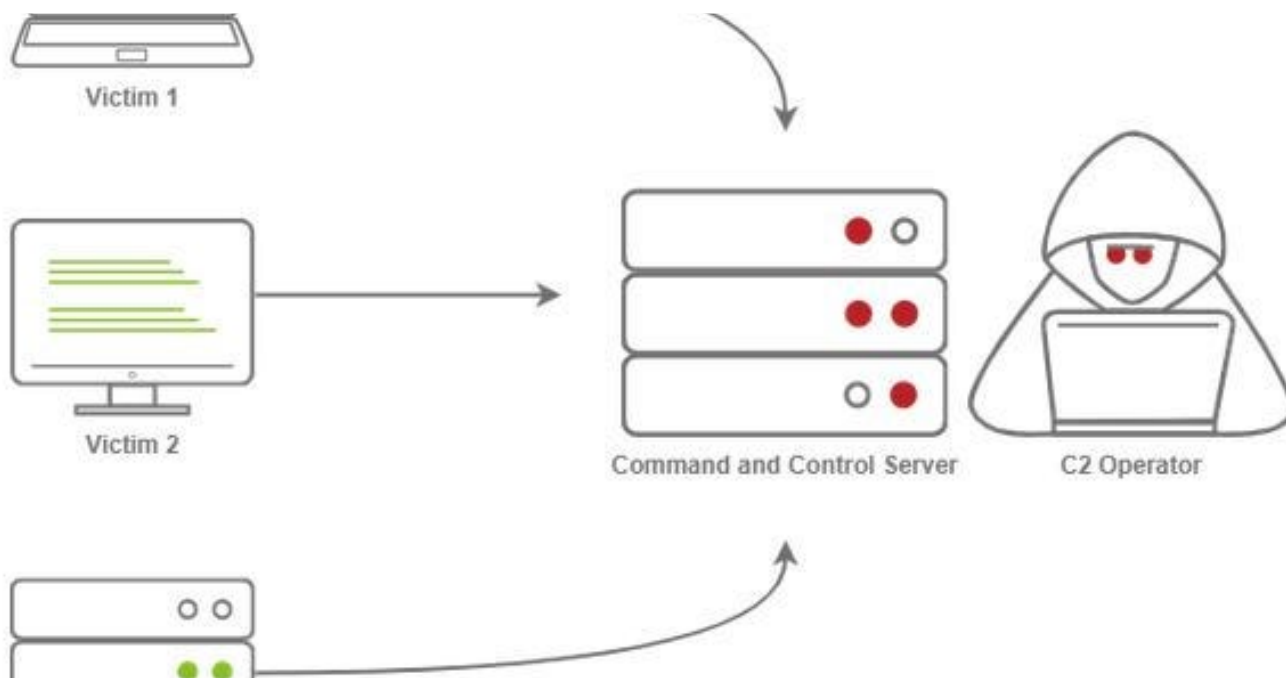


 Shefali Kumari

TRY HACK ME: Write-Up Phishing

Task 2 Intro To Phishing Attacks -

Nov 12, 2021  12



 Shefali Kumari

TRY HACK ME: Intro to C2 Write-Up

Task 1 Introduction -

Mar 14, 2022  54





Shefali Kumari

TRY HACK ME: Write-Up Module-Vulnerability Research: Exploit Vulnerabilities

TASK 1: INTRODUCTION –

Oct 13, 2021 🖱 55 💬 2



| | MBC Behavior |
|----------|--|
| ANALYSIS | Debugger Detection::Process Environment Block BeingDebugged Debugger Detection::Process Environment Block NtGlobalFlag Debugger Detection::Software Breakpoints [B0001.025] Virtual Machine Detection::Human User Check [B0009.012] Virtual Machine Detection::Instruction Testing [B0009.029] |
| SIS | Disassembler Evasion::Argument Obfuscation [B0012.001] Keylogging::Polling [F0002.002] HTTP Communication::Read Header [C0002.014] Encoding::XOR [C0026.002] Non-Cryptographic Hash::MurmurHash [C0030.001] Obfuscated Files or Information::Encoding-Standard Algorithm Create Directory [C0046] Delete File [C0047] Get File Attributes [C0049] Read File [C0051] |



Shefali Kumari

TRY HACK ME: Basic Static Analysis Write-Up

Task 1 Introduction-

Mar 13, 2023  1



See all from Shefali Kumari

Recommended from Medium



Trnty

TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

★ Sep 7, 2024  10





In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations



Nov 5, 2024



60

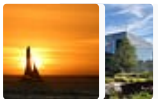


Lists



Staff picks

796 stories · 1561 saves



Stories to Help You Level-Up at Work

19 stories · 912 saves



Self-Improvement 101

20 stories · 3193 saves



Productivity 101

20 stories · 2707 saves

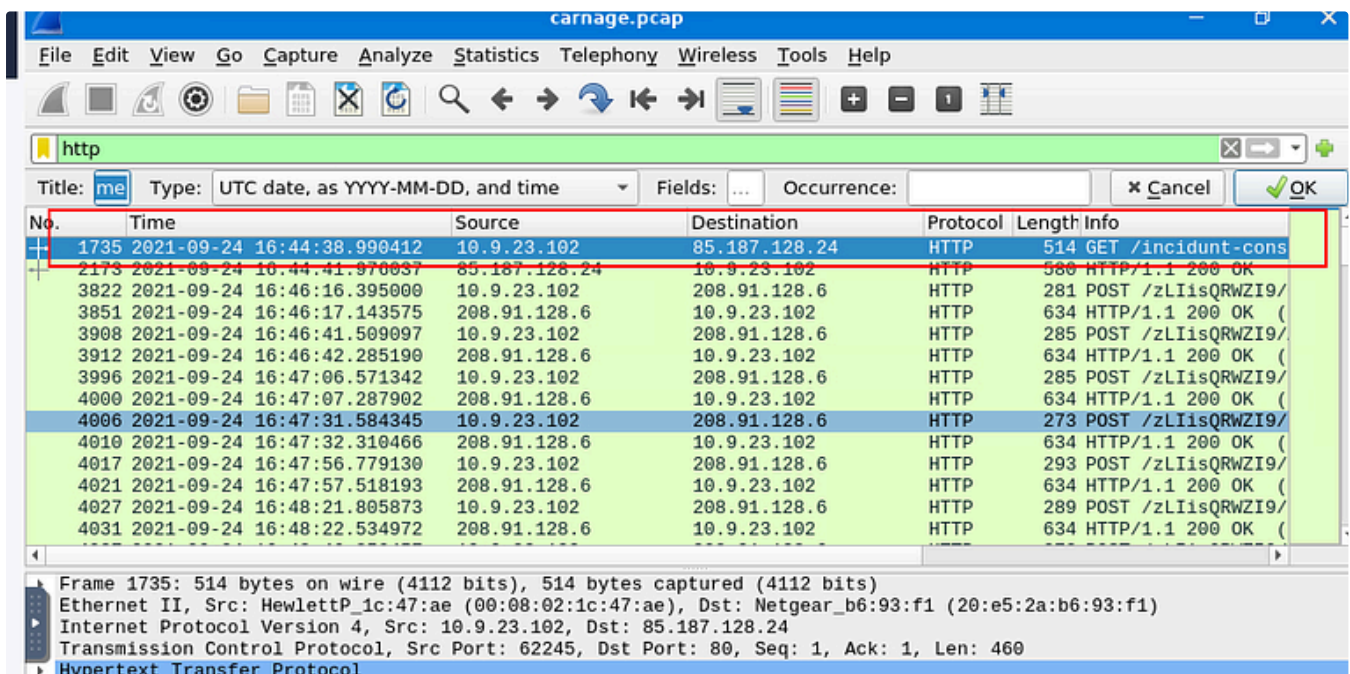


 In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

★ Nov 28, 2024 🖱 50



The image shows a Wireshark capture of a network packet. The packet list pane shows a table of captured packets. The selected packet is frame 1735, which is an HTTP GET request to /incidunt-cons. The packet details pane shows the structure of the packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|----------------------------|---------------|---------------|----------|--------|--------------------|
| 1735 | 2021-09-24 16:44:38.990412 | 10.9.23.102 | 85.187.128.24 | HTTP | 514 | GET /incidunt-cons |
| 2173 | 2021-09-24 16:44:41.970037 | 85.187.128.24 | 10.9.23.102 | HTTP | 580 | HTTP/1.1 200 OK |
| 3822 | 2021-09-24 16:46:16.395000 | 10.9.23.102 | 208.91.128.6 | HTTP | 281 | POST /zLIisQRWZI9/ |
| 3851 | 2021-09-24 16:46:17.143575 | 208.91.128.6 | 10.9.23.102 | HTTP | 634 | HTTP/1.1 200 OK (|
| 3908 | 2021-09-24 16:46:41.509097 | 10.9.23.102 | 208.91.128.6 | HTTP | 285 | POST /zLIisQRWZI9/ |
| 3912 | 2021-09-24 16:46:42.285190 | 208.91.128.6 | 10.9.23.102 | HTTP | 634 | HTTP/1.1 200 OK (|
| 3996 | 2021-09-24 16:47:06.571342 | 10.9.23.102 | 208.91.128.6 | HTTP | 285 | POST /zLIisQRWZI9/ |
| 4000 | 2021-09-24 16:47:07.287902 | 208.91.128.6 | 10.9.23.102 | HTTP | 634 | HTTP/1.1 200 OK (|
| 4006 | 2021-09-24 16:47:31.584345 | 10.9.23.102 | 208.91.128.6 | HTTP | 273 | POST /zLIisQRWZI9/ |
| 4010 | 2021-09-24 16:47:32.310466 | 208.91.128.6 | 10.9.23.102 | HTTP | 634 | HTTP/1.1 200 OK (|
| 4017 | 2021-09-24 16:47:56.779130 | 10.9.23.102 | 208.91.128.6 | HTTP | 293 | POST /zLIisQRWZI9/ |
| 4021 | 2021-09-24 16:47:57.518193 | 208.91.128.6 | 10.9.23.102 | HTTP | 634 | HTTP/1.1 200 OK (|
| 4027 | 2021-09-24 16:48:21.805873 | 10.9.23.102 | 208.91.128.6 | HTTP | 289 | POST /zLIisQRWZI9/ |
| 4031 | 2021-09-24 16:48:22.534972 | 208.91.128.6 | 10.9.23.102 | HTTP | 634 | HTTP/1.1 200 OK (|

Frame 1735: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits)
Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: 10.9.23.102, Dst: 85.187.128.24
Transmission Control Protocol, Src Port: 62245, Dst Port: 80, Seq: 1, Ack: 1, Len: 460
Hypertext Transfer Protocol

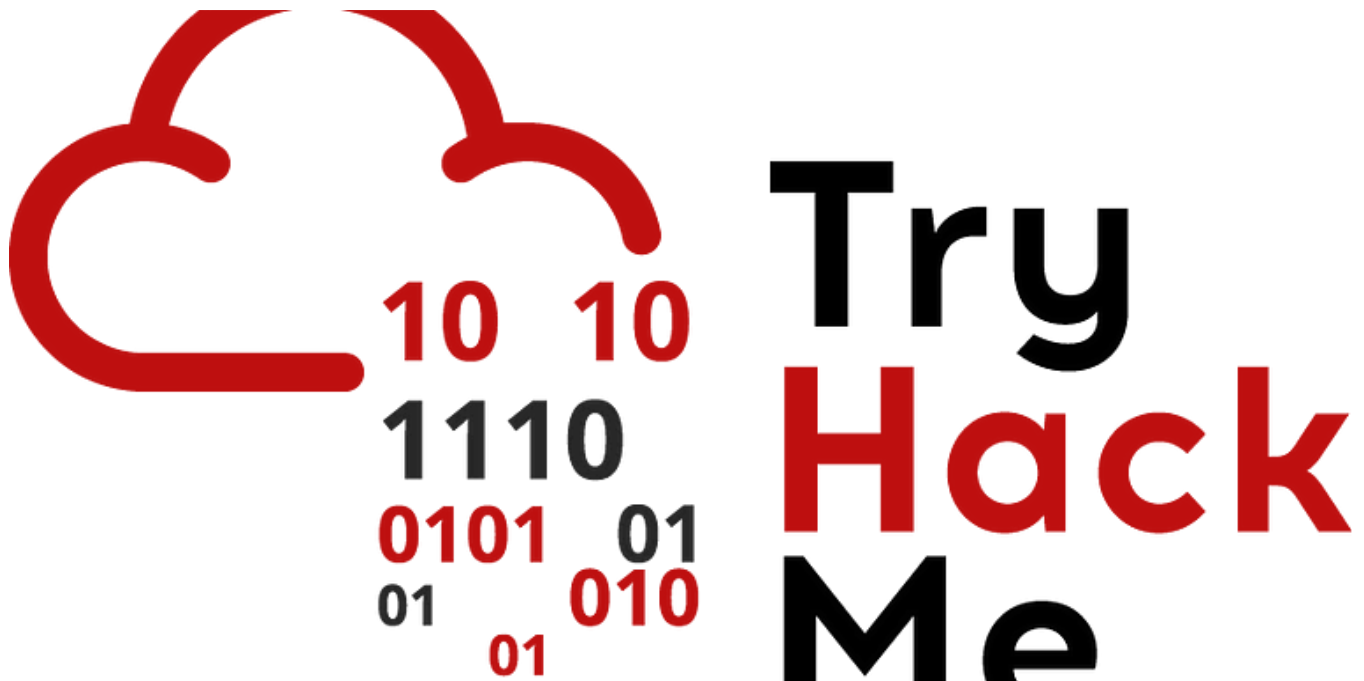
 Chicken0248

[TryHackMe Write-up] Carnage

Apply your analytical skills to analyze the malicious network traffic using Wireshark.

Aug 17, 2024 🖱 50





Rich

Advent of Cyber 2024

TL;DR Walkthrough of the first & current days of the 2024 Advent of Cyber, covering Google Fu, PowerShell, AD, a little Entra ID, and some...

Dec 17, 2024



```
d
rd.img.old  lib64      media  opt    root  sbin  srv  tmp  var      vmlinuz.old
            lost+found mnt    proc   run   snap sys  usr      vmlinuz
var/log
log# ls
cloud-init-output.log  dpkg.log      kern.log      lxd          unattended-upgrades
cloud-init.log         fontconfig.log  landscape     syslog       wtmp
dist-upgrade          journal       lastlog      tallylog
log# cat auth.log | grep install
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chow
hare/dokuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/s
hare/dokuwiki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
log#
```



Dan Molina

Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here:
<https://tryhackme.com/room/disgruntled>

Oct 22, 2024



See more recommendations