2025年停電行動：幻影檢查

關於“2025停電行動：幻影檢查”
這個 Sherlock 主要是使用來自該組織的 Mitre Att&ck 頁面的數據來研究 Sandworm 團隊的歷史和能力

福爾摩斯場景
在工業控制系統 (ICS) 產業，你的安全團隊需要隨時保持最新狀態，並了解產業內針對組織的威脅。你剛開始擔任威脅情報實習生，並擁有一些安全營運中心 (SOC) 經驗。你的經理給你佈置了一項任務，旨在測試你的研究技能，以及你如何有效利用 Mitre ATT&CK 來獲得優勢。你應該研究一下 Sandworm 團隊（又稱 BlackEnergy 集團和 APT44）。利用 Mitre ATT&CK 了解如何以可操作的形式繪製對手的行為和策略。爭取通過評估，給你的經理留下深刻印象，因為你對威脅情報充滿熱情。

獲取2個evtx檔案

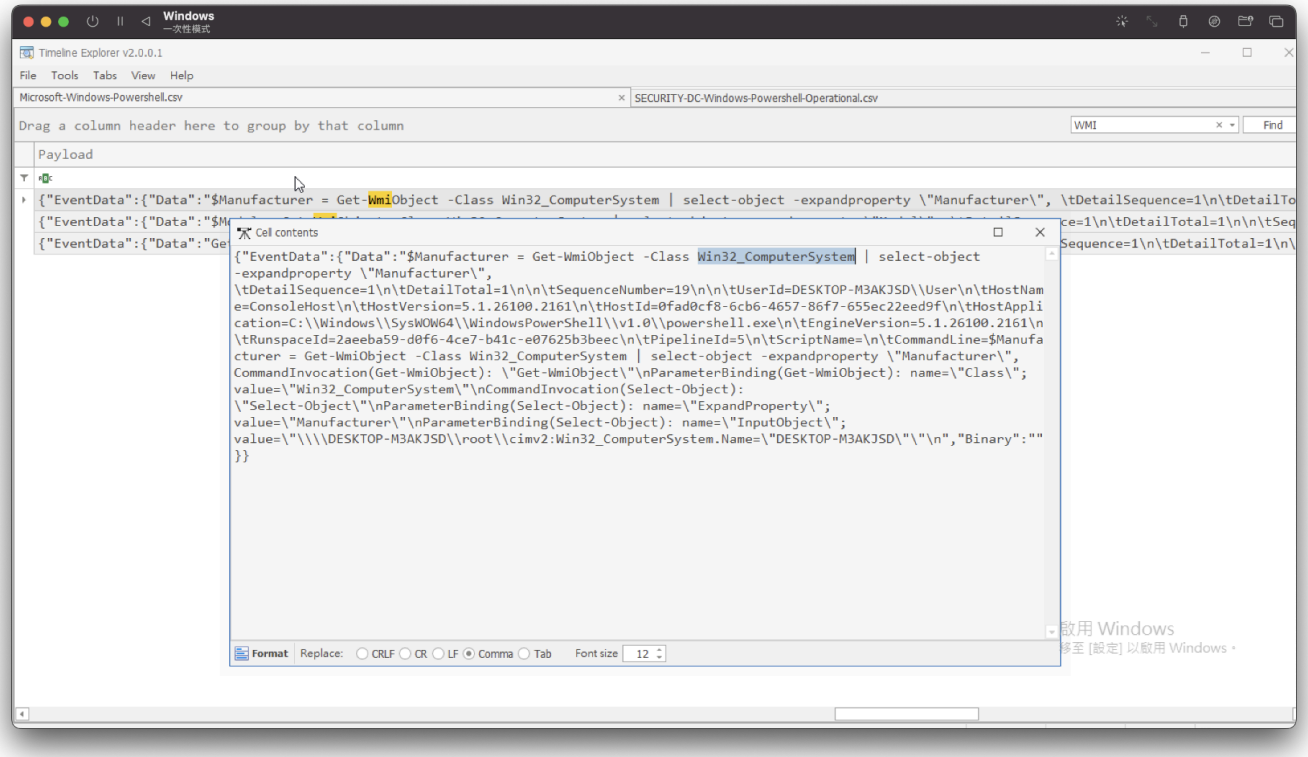
```
EvtxECmd.exe -f "C:\Users\TSO\Downloads\Windows-Powershell-Operational.evtx" --csv "C:\Users\TSO\Downloads" --csvf Windows-Powershell-Operational.csv

EvtxECmd.exe -f "C:\Users\TSO\Downloads\Microsoft-Windows-Powershell.evtx" --csv "C:\Users\TSO\Downloads" --csvf Microsoft-Windows-Powershell.csv
```

Task 1

Which WMI class did the attacker use to retrieve model and manufacturer information for virtualization detection?

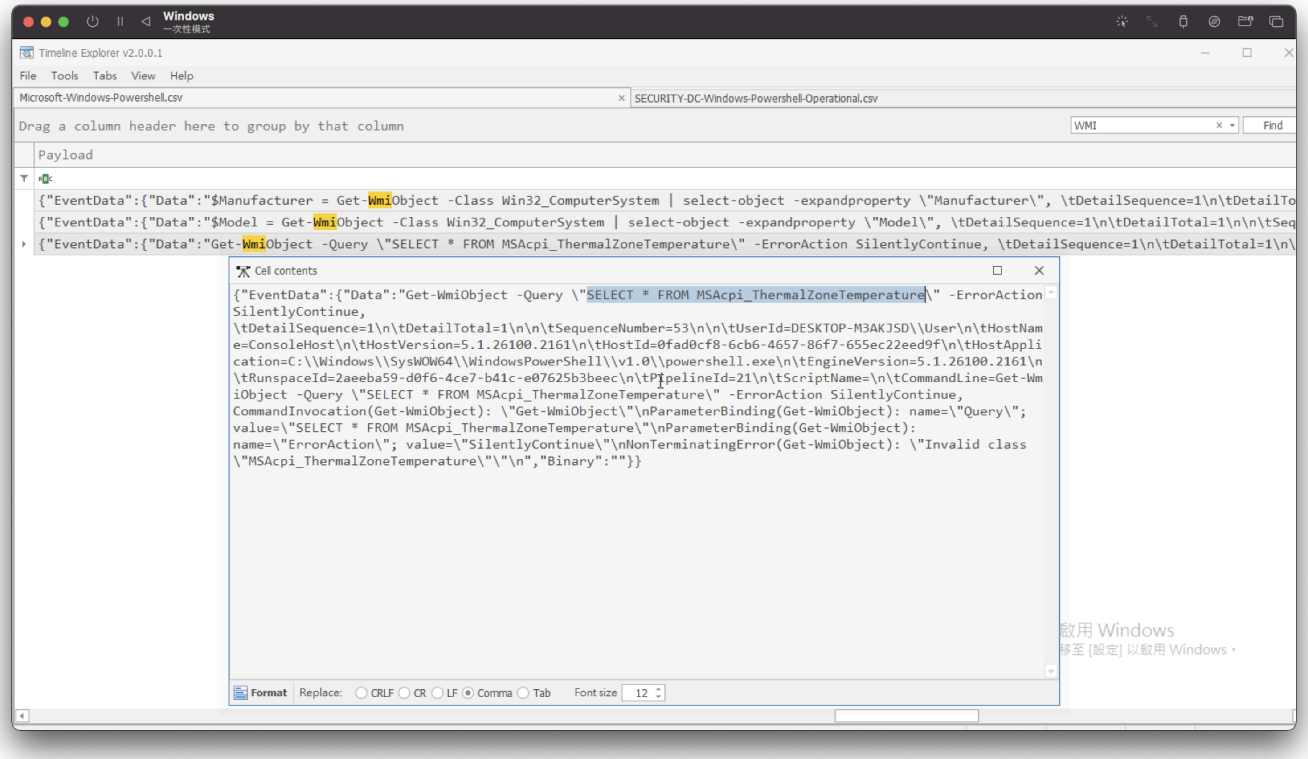
`Win32_ComputerSystem`



Task 2

Which WMI query did the attacker execute to retrieve the current temperature value of the machine?

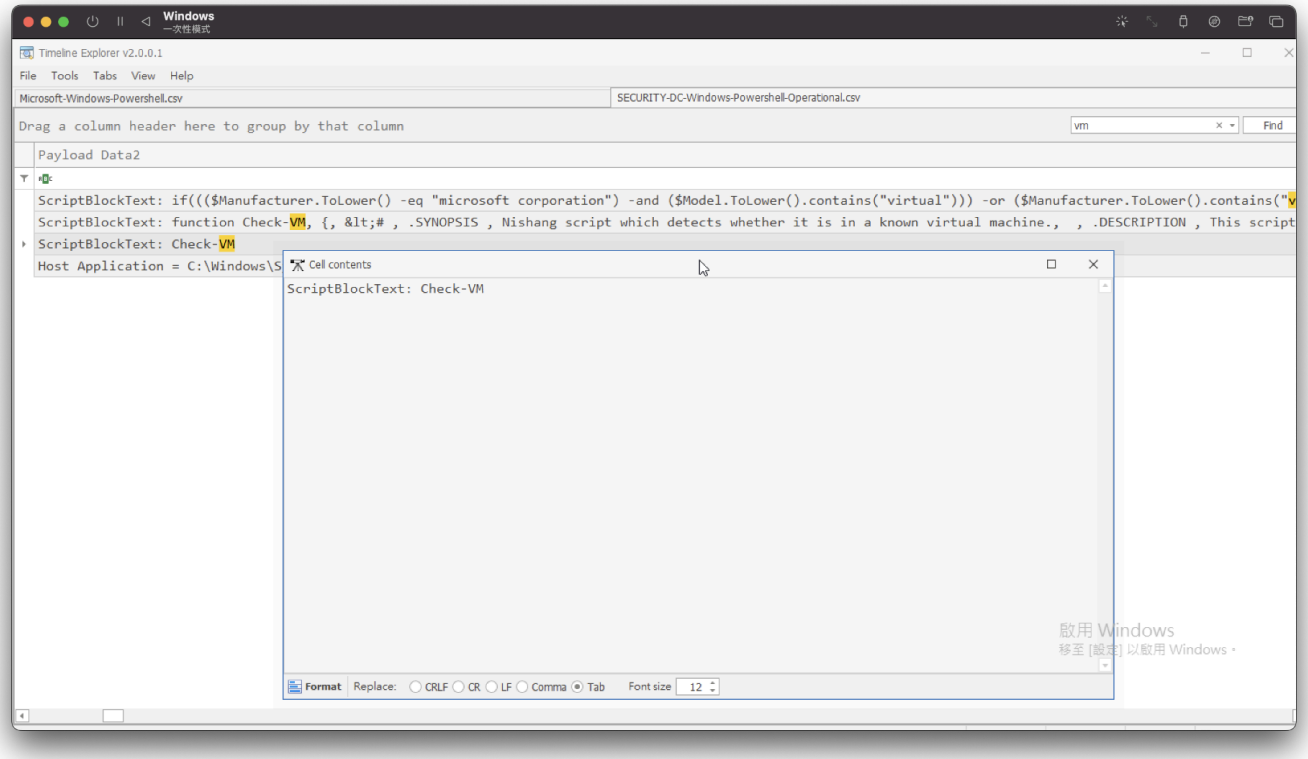
`SELECT * FROM MSAcpi_ThermalZoneTemperature`



Task 3

The attacker loaded a PowerShell script to detect virtualization. What is the function name of the script?

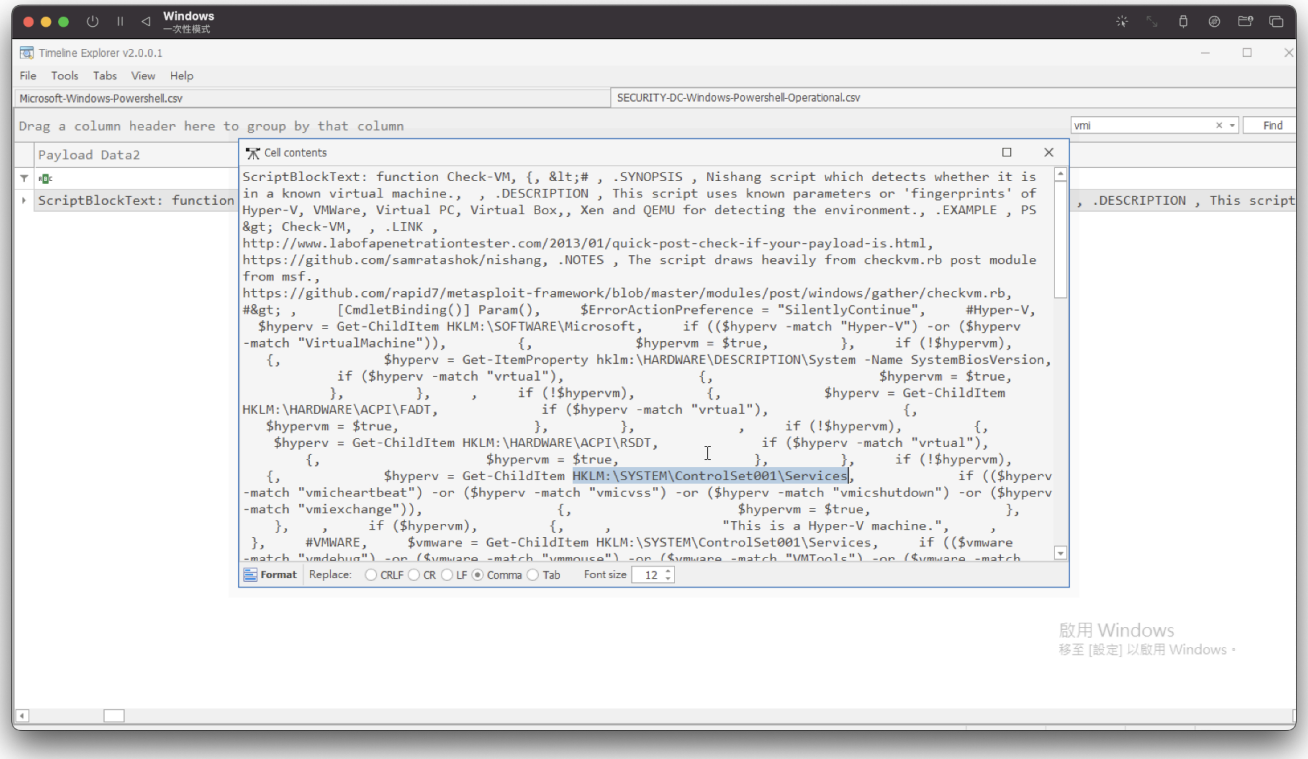
`Check-VM`



Task 4

Which registry key did the above script query to retrieve service details for virtualization detection?

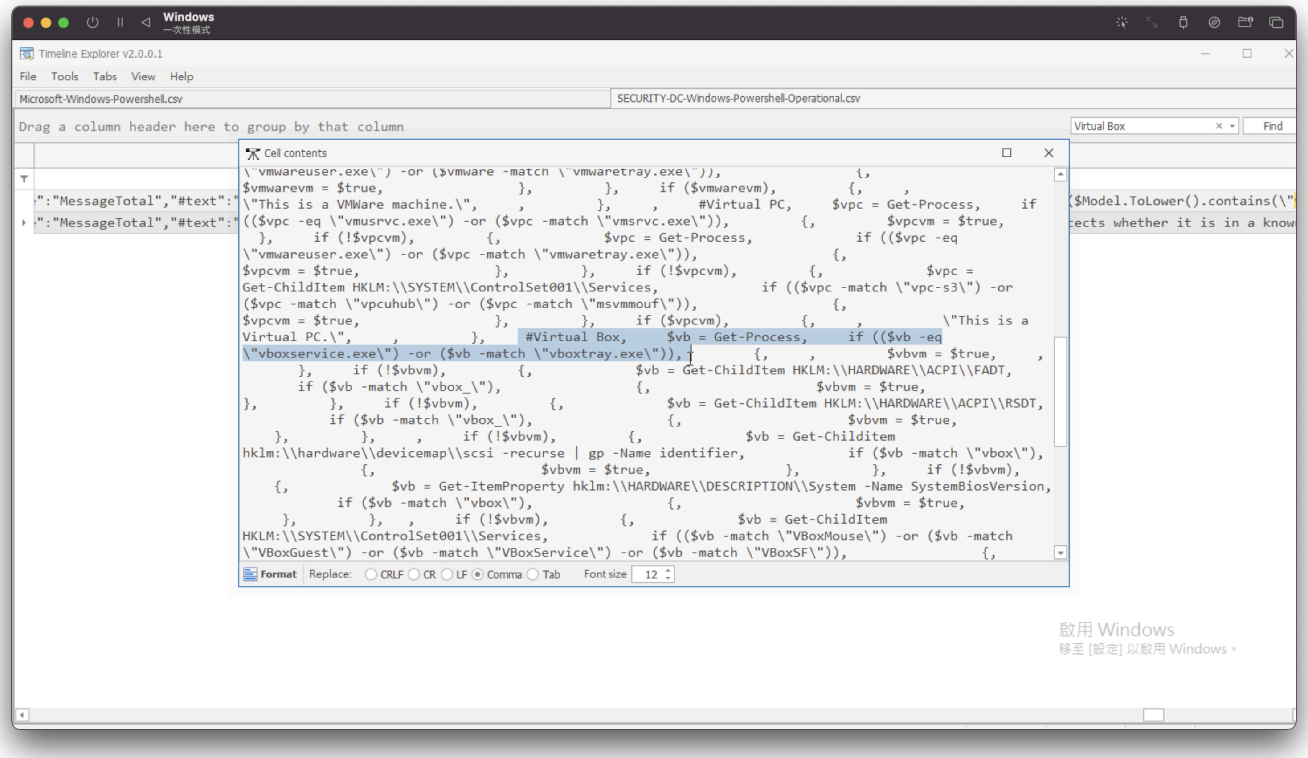
`HKLM:\SYSTEM\ControlSet001\Services`



Task 5

The VM detection script can also identify VirtualBox. Which processes is it comparing to determine if the system is running VirtualBox?

`vboxservice.exe, vboxtray.exe`



Task 6

The VM detection script prints any detection with the prefix 'This is a'. Which two virtualization platforms did the script detect?

Hyper-V, Vmware