**Demo 3: MemoryRanger prevents attack on Windows Defender**

1. Check Windows version
2. Run dbgview64
3. Run MemoryRanger
4. Patch Integrity Level & Revoke Token for Windows Defender
   1. Run mem\_attacker\_console → Show DbgView
   2. Run the “patch\_integrity MsMpEng.exe” → Show DbgView
   3. Run the “revoke\_privileges MsMpEng.exe” → Show DbgView
5. Run cmd
6. Run cd and Run batch “clear\_extract\_and\_check.bat”
7. Show that CMD cannot found file:  
   Wait 20 secs

|  |
| --- |
| **>"C:\adfsl2022\mimikatz\mimikatz\_trunk\x64\mimikatz.exe"** |
| '"C:\adfsl2022\mimikatz\mimikatz\_trunk\x64\mimikatz.exe"' is not recognized as an internal or external command, operable program or batch file. |

|  |
| --- |
| **>dir "C:\adfsl2022\mimikatz\mimikatz\_trunk\x64"** |
| there is no mimikatz.exe |

1. Windows Defender reacts and detects malware
2. Run Process Hacker to show the Integrity Level and Privilege for MsMpEng.

The OS is protected