Let’s check the Windows version

We have the newest one.

We are launching the DbgView to see the kernel output.

Run MemoryRanger to protect kernel memory.

We can see that MemoryRanger is ready to protect token memory.

Attackers are launching the app, which loads a driver.

And look – MemoryRanger has moved the attacker’s driver to the separate enclave.

Attackers are patching Integrity Level Index.

And look – MemoryRanger has blocked the illegal access, – so that attacker’s driver reads fake null index.

Attackers are revoking a Process Privilege.

And look – MemoryRanger has blocked this illegal access as well, – so that attacker’s driver reads fake null Token.

Run CMD with admin privilege.

Run a script that [***é***] extracts the archive and launches mimikatz.

Attackers failed to run mimikatz.

Microsoft Defender detects a malware sample.

And also, Microsoft Defender removes the malware file.

Let’s double check that the file is removed.

Yes, it is.

Checking the Integrity Level for Microsoft Defender.

It is still System Level.

Checking its privileges.

The debug privilege is still enabled.

MemoryRanger has prevented disabling Microsoft Defender.

Thanks to MemoryRanger the Windows OS and Microsoft Defender are protected.