Checking the Windows version

We have the newest Windows 11

An Attacker is launching the app, which loads a driver

ProcessHacker helps to check the Protection levels for process.

Some of Windows Processes are running as a protected.

The malware app is running as non-protected.

The attacker is dumping NisSrv, and he fails, he does not have enough privilege. OS returns access denied.

First, he is setting Debug Privilege

Second, he is setting the Protection Level 31.

Relaunching ProcessHacker to see the updated Protection levels for process.

Now, the malware app is running as Light (AntiMalware)

The attacker is dumping NisSrv again, and now he succeeded.

The attacker is dumping LSASS, and he fails, malware app Protection Level is not enough. OS returns access denied.

He is setting the Protection Level 62.

Relaunching ProcessHacker to see the updated Protection levels for process.

Now, the malware app is running as Full (WinTcb)

The attacker is dumping LSASS again, and now he succeeded.

The attacker is dumping SgrmBroker and now he succeeded.

Attacker is able to access even Windows Defender Application, which are Protected by PPL mechanisms.

Let’s wait for PatchGuard reaction, which designed to prevent illegal access.

10 hours have passed nothing is happened.

The OS is danger.