Let’s check the Windows version

We have the newest one.

Checking the Integrity Level for Microsoft Defender.

It is System Level.

Let’s run process monitor to track files activity.

Apply a filter to monitor only malware activity.

Run CMD with admin privilege.

Run a script that extracts the archive and launches mimikatz.

Attackers failed to run mimikatz.

Microsoft Defender detects a malware sample.

And also, Microsoft Defender removes a malware file.

Let’s double check that the file is removed.

Yes, it is.

Let’s see the logged file system events.

Move to the end.

Microsoft Defender deletes mimikatz file by changing the file information.

And after closing the file handles, the file will be removed.

We’ve just proved that Microsoft Defender is active.

We are launching the DbgView to see the kernel output.

The attacker is launching the app, which loads a driver.

The attacker patches Integrity Level Index.

We can see that Integrity Level Index has been modified.

Let’s extract the archive and run mimikatz again.

We can see that now the situation is different.

Microsoft Defender can st**i**ll detect malware, but it c**á**nnot remove the file.

Let’s run mimikatz.

We can see that OS cannot run mimikatz.

Let’s see the logged file system events.

We move to the end and see that OS returns nine-zero-six status.

Let’s clear the log and relaunch mimikatz.

CMD fails to run the mimikatz, the OS returns nine-zero-six status.

Each time attackers run mimikatz → the OS returns nine-zero-six status.

Let me conclude:

Patching Integrity Level Index helps to prevent removing mimikatz file.

But it is not enough to allow launching mimikatz process.