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 [***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 **has been removed**.

Yes, **it has**.

Let’s see the logged file system events.

Move to the end.

Microsoft Defender deletes mimikatz file.

.

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 and revokes a Process Privilege.

We can see that Integrity Level Index has been modified.

Here are the privileges before and after patching. The debug privilege has been cleared.

Checking the Integrity Level for Microsoft Defender.

It is Untrusted Level now.

Checking the privileges. The debug privilege has been disabled.

Let’s [***é***] extract the archive and run mimikatz again.

Mimikatz has been started.

Let’s use these commands to extract passwords hashes.

The hashes have been dumped.

Let’s see the logged file system events.

Move to the end.

We can see that now Mimikatz has been loaded.

Let’s check Windows Security Settings.

We open Virus & threat protection → Allowed Threats

There are no allowed threats.

Let’s check the updates.

Microsoft Defender cannot be updated.

Let’s wait for PatchGuard reaction, which was designed to prevent attacks on Windows Kernel.

10 hours have passed; nothing has happened.

The OS is in danger.