Twitter Thread by Jonas L

Jonas L
@jonasLyk

Wanna disable Defender when enabled Isolated Core and Tamper protection?

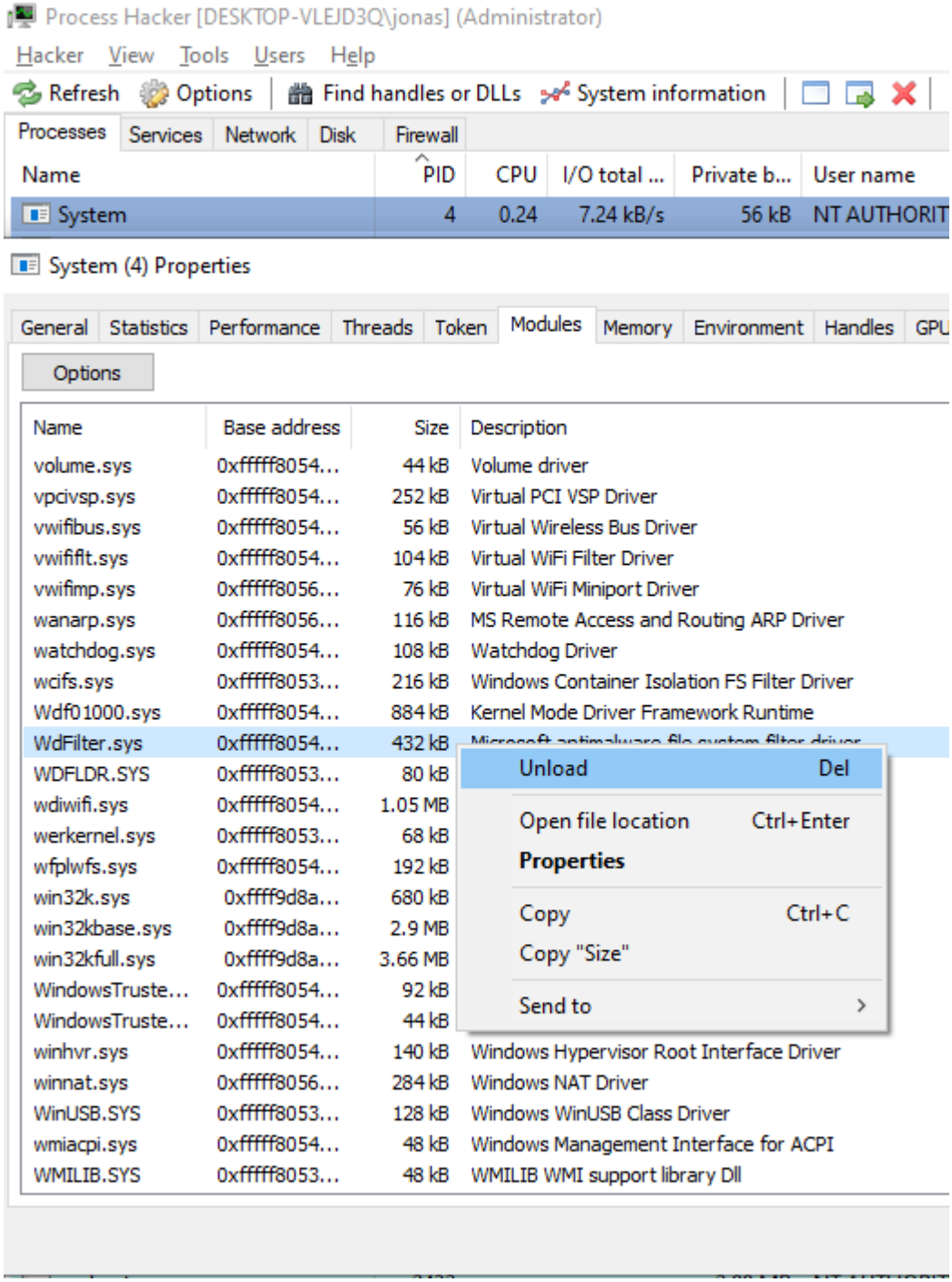
Its a bit more trouble- but doable, without ruining Isolated Core/Secureboot etc.

Defenders process will run as a unkillable protected service- so new tricks needed.

Here we go:

Ok- tamper protection is easy, just make .bat - run as adm:
:again
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdFilter\Instances\WdFilter Instance" /v altitude /t REG_SZ /d -1 /f
goto again

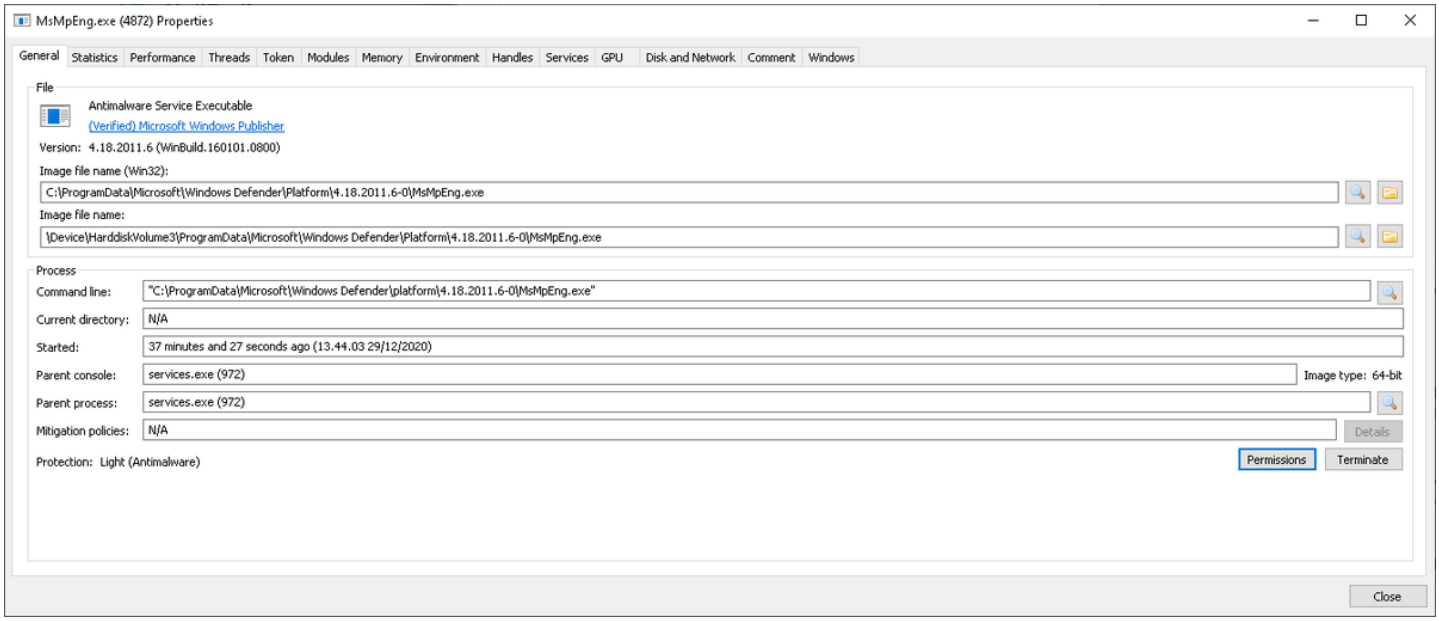
Then unload minifilter with process hacker:



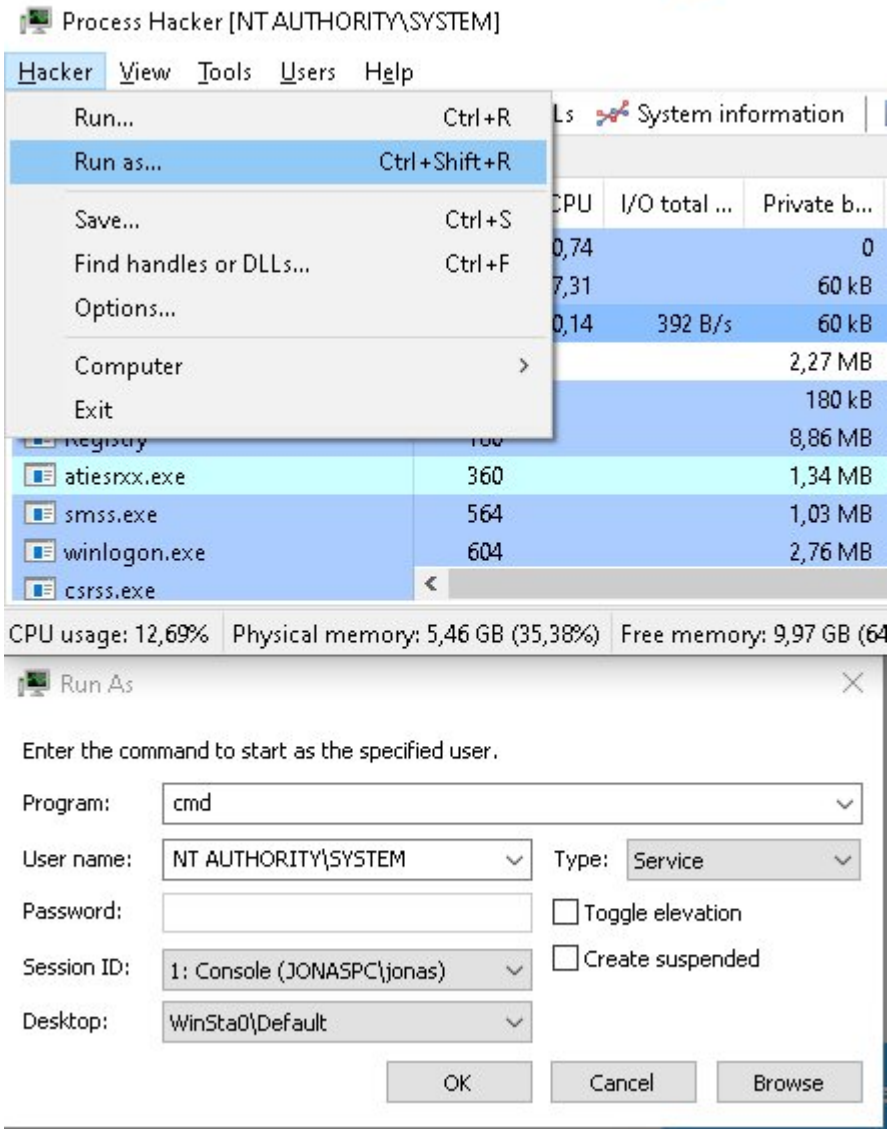
The registry key will be changed while the minifilter do not protect it, when tamper protection makes the driver load again it cannot attach to volumes nor protect registry keys.

Removing it will make it recreate, but invalid altitude do the trick

Notice now the service is: Protected light(antimalware)
Now we cant do anything to the service/process- not even see its open handles.



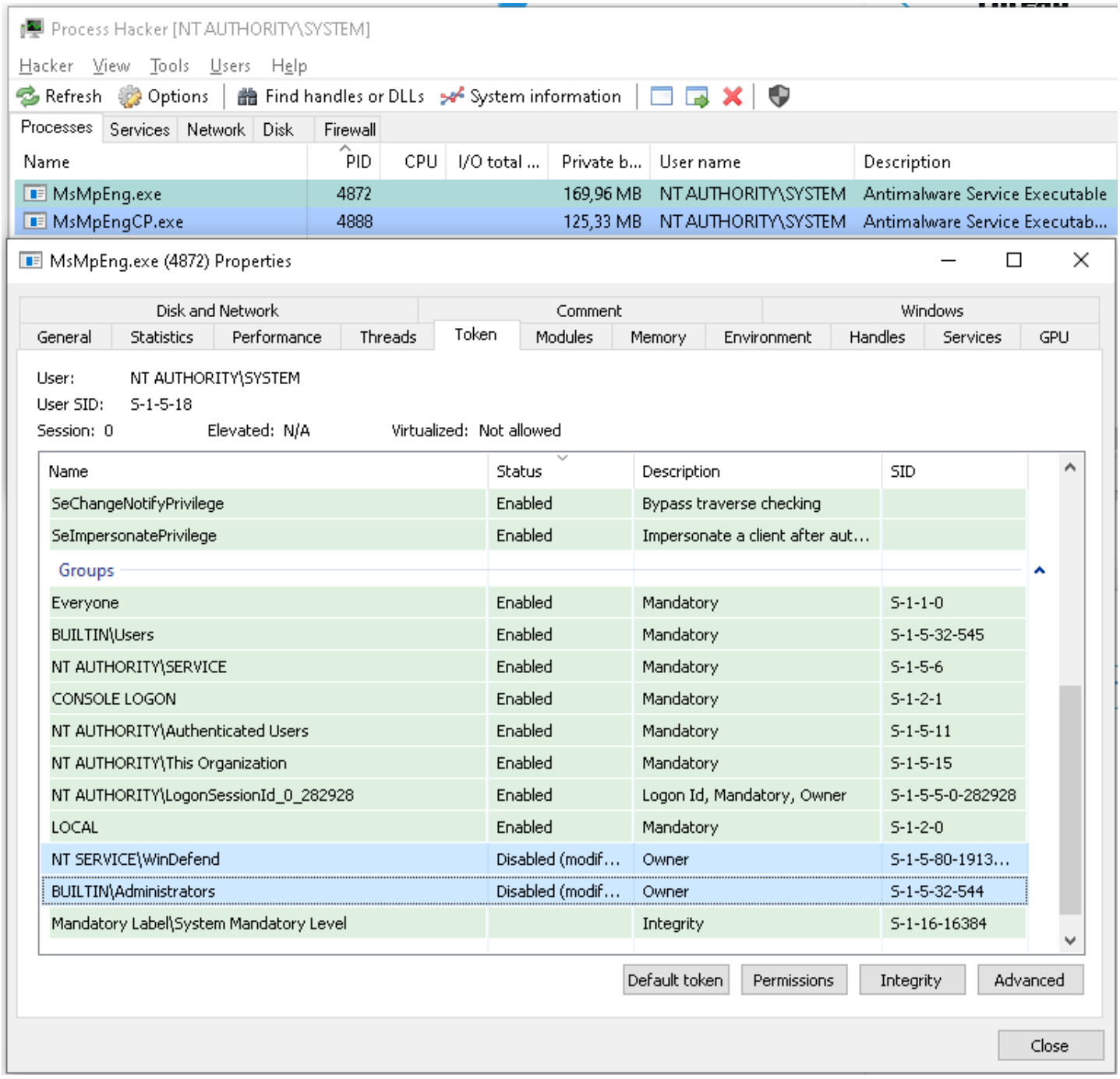
Lets start by elevating to SYSTEM- just launch a command prompt, then close process hacker- and run it again from the command prompt.
Now process hacker runs as SYSTEM



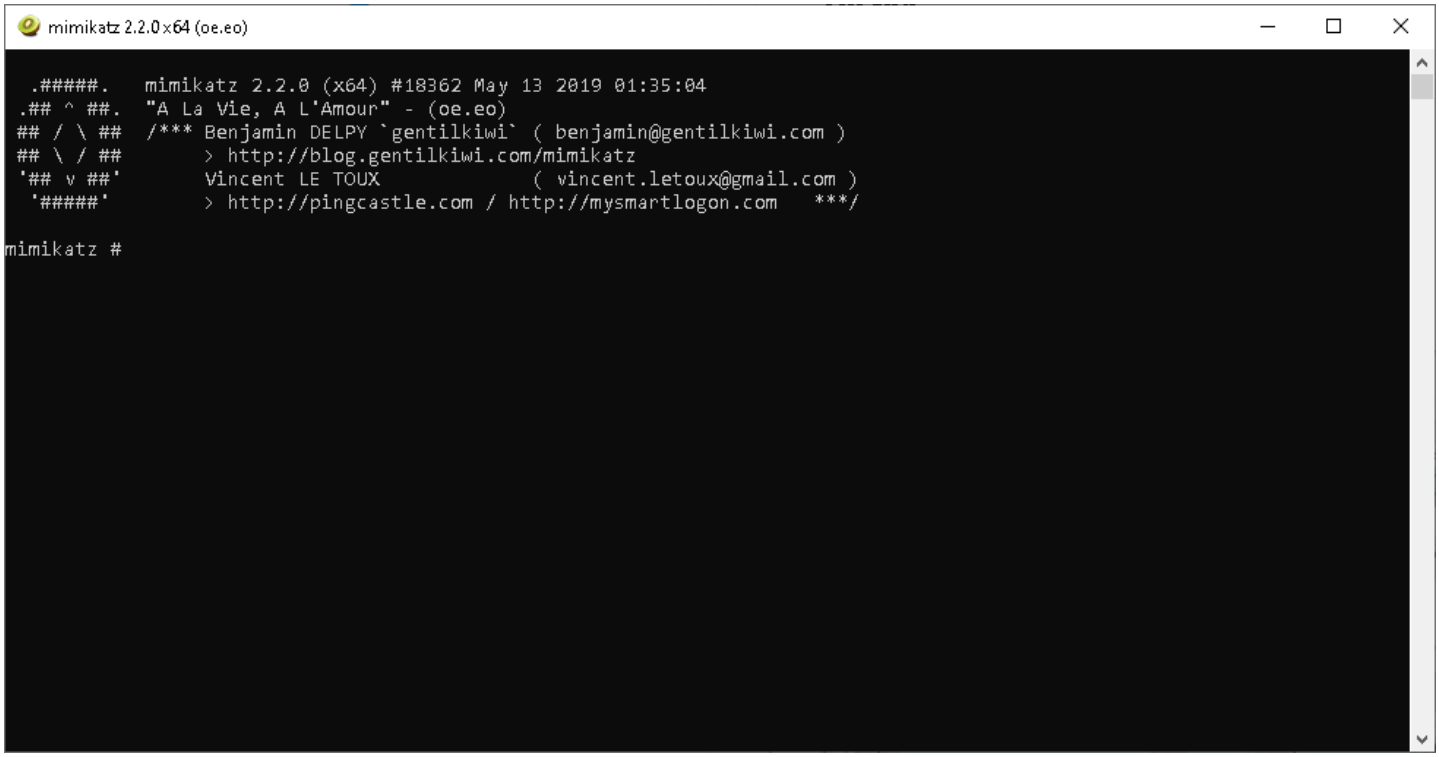
Find the services process again- select the token tab.

Right click and disable the two groups:

WinDefend
Administrators



https://t.co/vSDPatKkXK

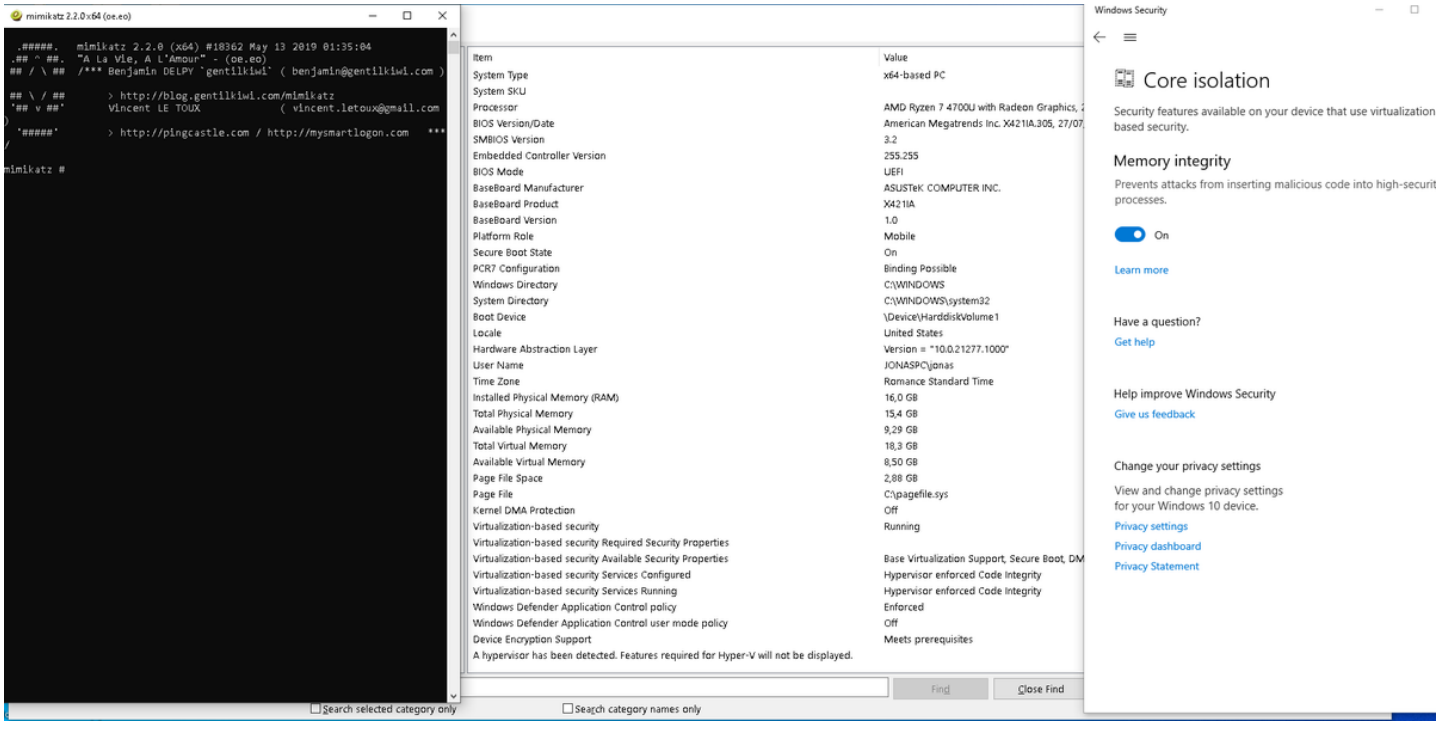


Now defender no more constant opens files- it dosnt do anything actually....

If you wanna permanently disable it its easy enough now there is no protection on its files.

If you mklink MsMpLics.dll:q nul it will not run on restart- but you loose the isolated core status :S

But secure boot and core isolation is still running fine



I am surprised that the protected services tokens are not protected.... that seems like bad design...

It also means we can impersonate them- here I impersonate SecureSystem:

