BUZZ CHRONICLES > INTERNET Saved by @Alex1Powell See On Twitter

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)

<u>Hacker View Tools Users Help</u>

🤣 Refresh	🎲 Opt	ions 🛛 🛗	Find I	handles or	DLLs 🍃	🖋 System inf	ormation	🗆 🗔 🗙
Processes	Services	Network	Disk					
Name				PID	CPU	I/O total	Private b	User name
System	ı			4	0.24	7.24 kB/s	56 kB	NT AUTHORIT

System (4) Properties

eneral	Statistics	Performance	Threads	Token	Modules	Memory	Environment	Handles	(
Optio	ons								
Name		Base addres	s S	Size De	scription				
volume	.sys	0xfffff8054	. 44	lkB Vα	lume driver				
vpcivsp	.sys	0xfffff8054	. 252	kB Vir	tual PCI VSF	P Driver			
vwifibu:	s.sys	0xfffff8054	. 56	i kB Vir	tual Wireles	s Bus Driv	er		
vwififlt.	sys	0xfffff8054	. 104	FkB Vir	tual WiFi Filt	ter Driver			
vwifimp	.sys	0xfffff8056	. 76	i kB Vir	tual WiFi Mir	niport Driv	er		
wanarp.sys		0xfffff8056	. 116	ikB Ms	MS Remote Access and Routing ARP Driver				
watchd	og.sys	0xfffff8054	. 108	kB W	atchdog Driv	/er			
wcifs.sy	ys	0xfffff8053	. 216	ikB W	ndows Cont	tainer Isola	ation FS Filter D	river	
Wdf010	00.sys	0xfffff8054	. 884	FkB Ke	rnel Mode D	river Fram	nework Runtime		
WdFilte	r.sys	0xfffff8054	. 432	2 kB 🔤		nalwara fi	o avatom filtor		
WDFLD	R.SYS	0xfffff8053	. 80) kB	Unload			Del	
wdiwifi.	sys	0xfffff8054	. 1.05	MB	Onen fil	e locatio	n Ctrl+F	ator .	
werkerr	nel.sys	0xfffff8053	. 68	8 kB			n Cui+E	nter	
wfplwfs	s.sys	0xfffff8054	. 192	2 kB	Propert	ties			
win32k.	sys	0xffff9d8a	. 680) kB	Conv		Ct	rl+C	
win32kb	base.sys	0xffff9d8a	. 2.9	MB	Сору		ci		
win32kf	full.sys	0xffff9d8a	. 3.66	MB	Copy "S	ize"			
Window	/sTruste	0xfffff8054	. 92	2 kB	Send to			>	
Window	/sTruste	0xfffff8054	. 44	kB	Sena to				
winhvr.	sys	0xfffff8054	. 140	kB W	ndows Hype	ervisor Ro	ot Interface Dri	iver	
winnat.	sys	0xfffff8056	. 284	ikB W	ndows NAT	Driver			
WinUSB	SYS	0xfffff8053	. 128	kB W	ndows Winl	JSB Class I	Driver		
wmiacpi	i.sys	0xfffff8054	. 48	kB W	ndows Mana	agement I	nterface for AC	PI	
WMILIE	SYS	0xfffff8053	. 48	kB W	MILIB WMI s	support lib	rary Dll		

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.

📧 MsMpEng.exe (48	72) Properties	-		×
General Statistics P	erformance Threads Token Modules Memory Environment Handles Services GPU Disk and Network Comment Windows			
File				
	are Service Executable Microsoft Windows Publisher			
	Microsoft Windows Publisher 1.6 (WinBuild.160101.0800)			
Image file name (W				
	Microsoft/Windows Defender/Platform\4.18.2011.6-0/MsMpEng.exe		٩.	
Image file name:				_
\Device\Harddisk\	Volume3\ProgramData\Mirrosoft\Windows Defender\Platform\4.18.2011.6-0\MisMpEng.exe		٩ (2
Process				
Command line:	"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2011.6-0[MsMpEng.exe"			2
Current directory:	N/A			
Started:	37 minutes and 27 seconds ago (13.44.03 29/12/2020)			
Parent console:	services.exe (972)	Image t	ype: 64	i-bit
Parent process:	services.exe (972)			2
Mitigation policies:	A		Details	s
Protection: Light (A	Permissic Permissic	ns T	erminate	e
				-
			C	ose
				33C

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

👰 Process Hacker [NT AUTHORITY\SYSTEM]

<u>Hacker</u> <u>V</u> ie	w <u>T</u> ools	<u>U</u> sers	H <u>e</u> lp	ġ			
Run				Ctrl+R	Ls 🚦	希 System inf	formation
Run as			Ctr	I+Shift+R			
Save				Ctrl+S	CPU	I/O total	Private b
	indles or D)LLs		Ctrl+F	0,74		0
Option		225111		ourr	7,31		60 kB
opuon	2				0,14	392 B/s	60 kB
Compi	ıter			>			2,27 MB
Exit							180 kB
T			_	100	_		8,86 MB
🔳 atiesrxx	exe			360			1,34 MB
🔳 smss.ex	e			564			1,03 MB
🔳 winlogo	n.exe			604			2,76 MB
csrss.ex	2			<			
CPU usage: 1	2,69% Pł	nysical m	emory	: 5,46 GB (3	5,38%)	Free memo	ry: 9,97 GB (6
💷 Run As							×
Enter the cor	nmand to st	tart as the	e specif	ied user.			
Program:	cmd						~
User name:	NT AUTH	IORITY\S\	/STEM	~	Туре	Service	~
Password:						oggle elevation	
1 33511013.					102 . A	85.5 July 10	
Session ID:	1: Conso	le (JONAS	iPC\jor	nas) 🗸 🗸		eate suspende	ed
Desktop:	WinSta0	,Default		~			
				ОК	С	ancel	Browse

Find the services process again- select the token tab.

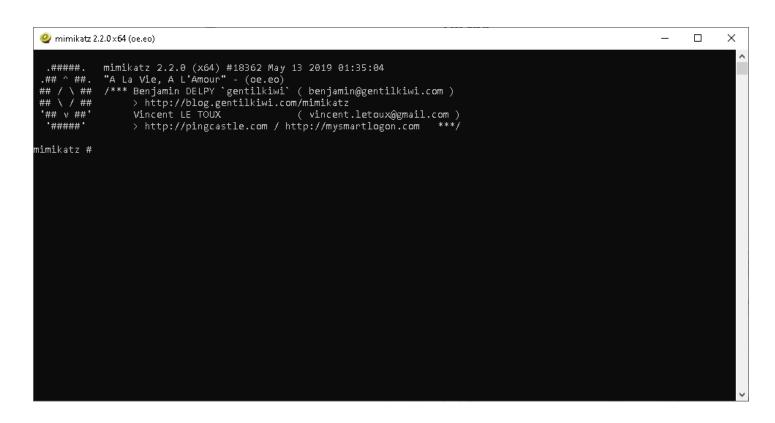
Right click and disable the two groups:

WinDefend

Administrators

ocesses Services Network Disk Firewall	⁴ System information	🗆 🗔 🗙 💱		
	I/O total Private b	User name D	escription	
MsMpEng.exe 4872	169,96 M			xecuta
MsMpEngCP.exe 4888	125,33 M			
MsMpEng.exe (4872) Properties			- 0	>
Disk and Network General Statistics Performance Threads	Comment Token Modules	Memory Environment Han	Windows Idles Services	GPU
Jser: NT AUTHORITY\SYSTEM				
· .	d: Not allowed			
	Status	Description	SID	^
SeChangeNotifyPrivilege	Enabled			
SeImpersonatePrivilege	Enabled	Enabled Impersonate a client after aut		
Groups				^
Everyone	Enabled	Enabled Mandatory		
BUILTIN\Users	Enabled	Mandatory	S-1-5-32-545	
	Enabled	Mandatory	S-1-5-6	
NT AUTHORITY\SERVICE			5-1-2-1	
NT AUTHORITY\SERVICE	Enabled	Mandatory		
CONSOLE LOGON NT AUTHORITY\Authenticated Users	Enabled	Mandatory	5-1-5-11	
CONSOLE LOGON NT AUTHORITY\Authenticated Users NT AUTHORITY\This Organization	Enabled Enabled	Mandatory Mandatory	S-1-5-11 S-1-5-15	
CONSOLE LOGON NT AUTHORITY\Authenticated Users NT AUTHORITY\This Organization NT AUTHORITY\LogonSessionId_0_282928	Enabled Enabled Enabled	Mandatory Mandatory Logon Id, Mandatory, Owner	S-1-5-15 S-1-5-5-0-282928	
CONSOLE LOGON NT AUTHORITY\Authenticated Users NT AUTHORITY\This Organization NT AUTHORITY\LogonSessionId_0_282928 LOCAL	Enabled Enabled Enabled Enabled	Mandatory Mandatory	S-1-5-15 S-1-5-5-0-282928 S-1-2-0	
CONSOLE LOGON NT AUTHORITY\Authenticated Users NT AUTHORITY\This Organization NT AUTHORITY\LogonSessionId_0_282928 LOCAL NT SERVICE\WinDefend	Enabled Enabled Enabled Enabled Disabled (modif	Mandatory Mandatory Logon Id, Mandatory, Owner	5-1-5-15 5-1-5-5-0-282928 5-1-2-0 5-1-5-80-1913	
CONSOLE LOGON NT AUTHORITY\Authenticated Users NT AUTHORITY\This Organization NT AUTHORITY\LogonSessionId_0_282928 LOCAL NT SERVICE\WinDefend BUILTIN\Administrators	Enabled Enabled Enabled Enabled	Mandatory Mandatory Logon Id, Mandatory, Owner Mandatory Owner Owner	5-1-5-15 5-1-5-5-0-282928 5-1-2-0 5-1-5-80-1913 5-1-5-32-544	
CONSOLE LOGON NT AUTHORITY\Authenticated Users NT AUTHORITY\This Organization NT AUTHORITY\LogonSessionId_0_282928 LOCAL NT SERVICE\WinDefend	Enabled Enabled Enabled Enabled Disabled (modif	Mandatory Mandatory Logon Id, Mandatory, Owner Mandatory Owner	5-1-5-15 5-1-5-5-0-282928 5-1-2-0 5-1-5-80-1913	~

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

🎱 mimikatz	2.2.0×64 (oe.eo)	-	o x					Wir	dows Security —	
			~	~				4	=	
	mimikatz 2.2.0 (x64) #18362 May 1	3 2019 01:35:04		Item		Value		`	-	
.## ^ ##.	"A La Vie, A L'Amour" - (oe.eo) /*** Benjamin DELPY `gentilkiwi`	(beniamin@gentilkiw	d.com.)						(D)	
				System Type		x64-based PC			Core isolation	
## \ / ##	> http://blog.gentilkiwi.com	/mimikatz		System SKU						
.** ^ **.	Vincent LE TOUX	(vincent.letoux@gma	11.com	Processor		AMD Ryzen 7 4700U wit			Security features available on your device that use virtual	ization
	> http://pingcastle.com / htt	tp://mysmartlogon.co	m ***	BIOS Version/Date SMBIOS Version		American Megatrends Ir 3.2	nc. X4211A.305, 27/07,		based security.	
/				Embedded Controller Version		3-2 255.255				
mimikatz #				BIOS Mode		UEFI			Memory integrity	
MANAROLL H				BaseBoard Manufacturer		ASUSTEK COMPUTER IN	r.		Prevents attacks from inserting malicious code into high-	-securi
				BaseBoard Product		X421IA	no.		processes.	
				BaseBoard Product		1.0				
				Platform Role		Mobile			On	
				Secure Boot State		On				
				PCR7 Configuration		Binding Possible			Learn more	
				Windows Directory		C:\WINDOWS			cean more	
				System Directory		C:\WINDOWS\system32				
				Boot Device		\Device\HarddiskVolume				
				Locale		United States			Have a question?	
				Hardware Abstraction Laver		Version = "10.0.21277.1	000"		Get help	
				User Name		JONASPC\jonas				
				Time Zone		Romance Standard Time	2			
				Installed Physical Memory (RAM)		16,0 GB			Help improve Windows Security	
				Total Physical Memory		15,4 GB			Give us feedback	
				Available Physical Memory		9,29 GB				
				Total Virtual Memory		18,3 GB				
				Available Virtual Memory		8,50 GB			Change your privacy settings	
				Page File Space		2,88 GB				
				Page File		C:\pagefile.sys			View and change privacy settings	
				Kernel DMA Protection		Off			for your Windows 10 device.	
				Virtualization-based security		Running			Privacy settings	
				Virtualization-based security Required Securit					Privacy dashboard	
				Virtualization-based security Available Securit		Base Virtualization Supp			Privacy Statement	
				Virtualization-based security Services Configu		Hypervisor enforced Co				
				Virtualization-based security Services Running		Hypervisor enforced Co	de Integrity			
				Windows Defender Application Control policy		Enforced				
				Windows Defender Application Control user n	node policy	Off				
				Device Encryption Support		Meets prerequisites				
				A hypervisor has been detected. Features req	uired for Hyper-V will not be displayed.					
						Fin <u>d</u>	<u>C</u> lose Find			
		Search selected ca	ategory only	y Search category name	s only					
4			,,,,,	,						

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:

Process Hacker (NTAU					Select Administrator: C:\WINDOWS\SYSTEM32\cmd.	exe				- 0
cker ⊻iew Tools .U Refresh 🍪 Options		LODIDA SVETAN T		. – – ×	C:\WINDOWS\system32>whoami /all					
					USER INFORMATION					
ocesses Services Ne		fault Dacl Misc 0	perations Token	Source Security						
System	Additional Properties UI Access:	False	Toggle		User Name SID					
Secure System		False	103000							
Registry	Sandbox Inert:				nt authority∖system S-1-5-18					
smss.exe	Virtualization Allowed:	False								
csrss.exe	Virtualization Enabled:	N/A			GROUP INFORMATION					
wininit.exe	Mandatory IL Policy:	NoWriteUp								
csrss.exe services.exe	Handle Access:	AssignPrimary Dupli	cate Impersonate	Query, QuerySource, Adjust	Group Name	Туре		Attributes		
Memory Compressi	Trust Level:	TRUST LEVEL VProt		stach, stach, sause, ristan						
svchost.exe			ected-winit cb		Mandatory Label\System Mandatory Level Evervone	Well-known group	5-1-16-16384 5-1-1-0	Mandatory group, Enabled	by default. F	nabled gro
MsMpEng.exe	Token Flags:	NoLow			BUILTIN\Performance Log Users	Alias	S-1-5-32-559	Mandatory group, Enabled	by default, E	inabled gro
NisSrv.exe	Security Attributes:				BUILTIN\Users NT AUTHORITY\INTERACTIVE	Alias Well-known group		Mandatory group, Enabled Mandatory group, Enabled		
] svchost.exe] SecurityHealthServic	⊕ TSA: //ProcUniq	ue			CONSOLE LOGON	Well-known group	S-1-2-1	Mandatory group, Enabled	by default, E	inabled gro
svchost.exe					NT AUTHORITY\Authenticated Users	Well-known group		Mandatory group, Enabled		
SarmBroker.exe					NT AUTHORITY\This Organization BUILTIN\Administrators	Well-known group Alias		Mandatory group, Enabled Enabled by default, Enabled		
svchost.exe										
					PRIVILEGES INFORMATION					
					Privilege Name	Description				C+++-
					privilege Name					State
					SeCreateTokenPrivilege	Create a toke				Disabled
	1004	Lsarso.exe Isass.exe		NT AUTHORITY/SYSTEM	SeAssignPrimaryTokenPrivilege SeLockMemoryPrivilege	Replace a pro Lock pages in		oken		Disabled Enabled
	1108	sychost.exe		NT AUTHORITY\SYSTEM	SeIncreaseQuotaPrivilege	Adjust memory	quotas for a			Disabled
	1136	fontdrvhost.exe		Font Driver Host\UMFD-0	SeTcbPrivilege SeSecurityPrivilege	Act as part o Manage auditi				Enabled Disabled
	1172	fontdrvhost.exe		Font Driver Host\UMFD-1	SeTakeOwnershipPrivilege			other objects		Disabled
	<				SeLoadDriverPrivilege	Load and unlo				Disabled
					SeSystemProfilePrivilege SeSystemtimePrivilege	Profile syste Change the sy				Enabled Disabled
					SeProfileSingleProcessPrivilege	Profile singl	e process			Enabled
					SeIncreaseBasePriorityPrivilege SeCreatePagefilePrivilege	Increase sche Create a page				Enabled
					SecreatePagetilePrivilege	Create a page Create perman		viects		Enabled Enabled
					SeBackupPrivilege	Back up files	and director	ies		Disabled
					SeRestorePrivilege SeShutdownPrivilege	Restore files Shut down the		les		Disablec Disablec
					SeDebugPrivilege	Debug program				Enabled
					SeAuditPrivilege	Generate secu	rity audits			Enabled
					SeSystemEnvironmentPrivilege SeChangeNotifyPrivilege	Modify firmwa Bypass traver		t values		Disabled Enabled
					SeUndockPrivilege	Remove comput		ng station		Disabled
					SeManageVolumePrivilege	Perform volum	e maintenance	tasks		Disabled
					SeImpersonatePrivilege SeCreateGlobalPrivilege	Impersonate a Create global		authentication		Enabled
					SecreateGlobalPrivilege SeTrustedCredManAccessPrivilege			as a trusted caller 🛛 💼		Enabled
					SeRelabelPrivilege	Modify an obj	ect label		Snipping Tool	
					SeIncreaseWorkingSetPrivilege	Increase a pr		; set	10-10-10-10-10-10-10-10-10-10-10-10-10-1	
					SeTimeZonePrivilege SeCreateSvmbolicLinkPrivilege	Change the ti Create symbol			0	