[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender]

"DisableAntiSpyware"=dword:00000001

"DisableRealtimeMonitoring"=dword:00000001

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection]

"DisableBehaviorMonitoring"=dword:00000001

"DisableOnAccessProtection"=dword:00000001

"DisableScanOnRealtimeEnable"=dword:00000001

Depuis 20H1 windows defender devient microsoft defender !

On recupere des GPO update admx pour 2 admx



Une nouvelle version de windowsdefender.admx

Avant, jusqu’à la version 1809, pour désactiver l’antivirus, il fallait aller dans Windows defender / désactiver Windows defender :



Depuis la 1903 une nouvelle protection apparait qui a l’air de poser soucis avec la GPo de désactivation de defender. C’est la notion de « tamper » quie est paramétrable par l’utilisateur

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows Defender\Features. It’s a DWORD named TamperProtection

Comme son nom le laisse deviner (protection anti-sabotage) son rôle est d’empêcher les logiciels malveillants de désactiver les fonctionnalités de sécurité de Windows 10. Les attaques informatiques et les programmes malveillants comportant parfois des composants œuvrant à ces tâches. En clair, ils tentent de désactiver certaines protections de Windows 10. Ainsi, l’environnement créé est propice à générer davantage de dommages et à compromettre davantage de données.

Ce type de menace est de plus en plus utilisée si bien que Microsoft souhaite agir. Comment ? Windows 10 va s’armer d’une sorte de nouveau bouclier de protection. Le but est de pouvoir s’assurer que la désactivation de ses fonctionnalités de sécurité n’est pas possible

Maintenant depuis la 20H1 pour désactiver l’antivirus, il faut aller dans Antivirus Microsoft Defender et demander Désactiver l’Antivirus Microsoft defender :



Un nouvel admx WindowsDefenderSecurityCenter.admx





Il faut absolument désactiver depuis 1903 la protection contre les faclsifications, sinon non ne peut pas desactiver l’anti-virus





Donnant



HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows Defender\Features

**TamperProtection** DWORD

**0** = Off
**5** = On

