Windows registry

windows

autoejecución de ficheros

- XP: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell=Explorer.exe virus.exe`
- Vista/7: `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell=Explorer.exe virus.exe`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`

impedir automontaje USB

- W11: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR = 4` (disabled, valor original = 3 ?)

arranque

- renombrando estas ramas impedimos el arranque en modo safe o minimal (pantalla azul)
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\minimal`
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network`

ocultar usuarios login screen

> El usuario desaparece a todos los niveles. Si es el único administrador de la máquina, no podrás acceder como tal NUNCA!

- ocultar usuarios en la pantalla de bienvenida:
  - crear un DOWRD = 0 con el nombre de usuario a ocultar en `HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\SpecialAccounts\UserList` (crear si no existe)

cmd

- `reg {ADD,DELETE,QUERY} <rama>`
- `reg {EXPORT,IMPORT}`