

# el registro de 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

## 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

- 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}

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/windows:regedit:start?rev=1569497081>

Last update: **26/09/2019 04:24**

