Windows Persistence Map v0.1

https://how2itsec.blogspot.com/ | Florian Thiele | 2025

Mitre Att&ck – TA0003 Persistence
- https://attack.mitre.org/tactics/TA0003/
- „The adversary is trying to maintain their foothold.“

Windows Registry
- HKCU = HKEY_CURRENT_USER
- HKLM = HKEY_LOCAL_MACHINE

Startup/Logon

- C:\Users*username*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell
- HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKCU\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
- HKCU\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnceEx
- HKCU\Environment\UserInitMprLogonScript
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
- HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
- HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AppSetup
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
- HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\TaskMan
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells
- HKLM\Environment\UserInitMprLogonScript
- HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\IconServiceLib
- HKLM\SOFTWARE\Microsoft\Windows CE Services\AutoStartOnConnect
- HKLM\SOFTWARE\Microsoft\Windows CE Services\AutoStartDisconnect
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnceEx
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows CE Services\AutoStartOnConnect
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows CE Services\AutoStartOnDisconnect
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
- HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\InitialProgram
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Policies\Microsoft\Windows\System\Scripts\Logon
- HKCU\Software\Policies\Microsoft\Windows\System\Scripts\Logoff
- HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup
- HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logon
- HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logoff
- HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Shutdown
- HKLM\Software\Policies\Microsoft\Windows\System\Scripts\Startup
- HKLM\Software\Policies\Microsoft\Windows\System\Scripts\Logon
- HKLM\Software\Policies\Microsoft\Windows\System\Scripts\Logoff
- HKLM\Software\Policies\Microsoft\Windows\System\Scripts\Shutdown
- HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Shutdown
- HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logoff
- HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logon
- HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup

https://attack.mitre.org/techniques/T1037/ & https://attack.mitre.org/techniques/T1547/

Boot Execution

- HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute
- HKLM\System\CurrentControlSet\Control\Session Manager\SetupExecute
- HKLM\System\CurrentControlSet\Control\Session Manager\Execute
- HKLM\System\CurrentControlSet\Control\Session Manager\S0InitialCommand

https://attack.mitre.org/techniques/T1547/

Image Hijacks

- HKCU\Software\Microsoft\Command Processor\Autorun
- HKCU\SOFTWARE\Classes\Exefile\Shell\Open\Command\(Default)
- HKCU\SOFTWARE\Classes\Htmlfile\Shell\Open\Command\(Default)
- HKCU\Software\Classes\.exe
- HKCU\Software\Classes\.cmd
- HKLM\Software\Microsoft\Command Processor\Autorun
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
- HKLM\SOFTWARE\Classes\Exefile\Shell\Open\Command\(Default)
- HKLM\SOFTWARE\Classes\Htmlfile\Shell\Open\Command\(Default)
- HKLM\Software\Classes\.exe
- HKLM\Software\Classes\.cmd
- HKLM\Software\Wow6432Node\Microsoft\Command Processor\Autorun
- HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

https://attack.mitre.org/techniques/T1547/

LSA Providers

- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SecurityProviders
- HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Authentication Packages
- HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages
- HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages
- HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages

https://attack.mitre.org/techniques/T1547/

Office

- HKCU\Software\Microsoft\Office\Outlook\Addins
- HKCU\Software\Microsoft\Office\Excel\Addins
- HKCU\Software\Microsoft\Office\PowerPoint\Addins
- HKCU\Software\Microsoft\Office\Word\Addins
- HKCU\Software\Microsoft\Office\Access\Addins
- HKCU\Software\Microsoft\Office\OneNote\Addins
- HKCU\SOFTWARE\Microsoft\Office test\Special\Perf\(Default)
- HKCU\Software\Wow6432Node\Microsoft\Office\Outlook\Addins
- HKCU\Software\Wow6432Node\Microsoft\Office\Excel\Addins
- HKCU\Software\Wow6432Node\Microsoft\Office\PowerPoint\Addins
- HKCU\Software\Wow6432Node\Microsoft\Office\Word\Addins
- HKCU\Software\Wow6432Node\Microsoft\Office\Access\Addins
- HKCU\Software\Wow6432Node\Microsoft\Office\OneNote\Addins
- HKCU\SOFTWARE\Wow6432Node\Microsoft\Office test\Special\Perf\(Default)
- HKLM\Software\Microsoft\Office\Outlook\Addins
- HKLM\Software\Microsoft\Office\Excel\Addins
- HKLM\Software\Microsoft\Office\PowerPoint\Addins
- HKLM\Software\Microsoft\Office\Word\Addins
- HKLM\Software\Microsoft\Office\Access\Addins
- HKLM\Software\Microsoft\Office\OneNote\Addins
- HKLM\SOFTWARE\Microsoft\Office test\Special\Perf\(Default)
- HKLM\Software\Wow6432Node\Microsoft\Office\Outlook\Addins
- HKLM\Software\Wow6432Node\Microsoft\Office\Excel\Addins
- HKLM\Software\Wow6432Node\Microsoft\Office\PowerPoint\Addins
- HKLM\Software\Wow6432Node\Microsoft\Office\Word\Addins
- HKLM\Software\Wow6432Node\Microsoft\Office\Access\Addins
- HKLM\Software\Wow6432Node\Microsoft\Office\OneNote\Addins
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Office test\Special\Perf\(Default)

https://attack.mitre.org/techniques/T1137/

Compromise Host Software Binary

https://attack.mitre.org/techniques/T1554/

Internet Explorer

- HKCU\Software\Microsoft\Internet Explorer\UrlSearchHooks
- HKCU\Software\Microsoft\Internet Explorer\Explorer Bars
- HKCU\Software\Microsoft\Internet Explorer\Extensions
- HKCU\Software\Wow6432Node\Microsoft\Internet Explorer\Explorer Bars
- HKCU\Software\Wow6432Node\Microsoft\Internet Explorer\Extensions
- HKLM\Software\Microsoft\Internet Explorer\Toolbar
- HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
- HKLM\Software\Microsoft\Internet Explorer\Explorer Bars
- HKLM\Software\Microsoft\Internet Explorer\Extensions
- HKLM\Software\Wow6432Node\Microsoft\Internet Explorer\Toolbar
- HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
- HKLM\Software\Wow6432Node\Microsoft\Internet Explorer\Explorer Bars
- HKLM\Software\Wow6432Node\Microsoft\Internet Explorer\Extensions]

Scheduled Tasks

- C:\Windows\System32\Tasks
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\Taskcache\Tasks
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\Taskcache\Tree

https://attack.mitre.org/techniques/T1053/ & https://attack.mitre.org/techniques/T1543

Services

- HKLM\System\CurrentControlSet\Services

https://attack.mitre.org/techniques/T1543/

Drivers

- HKLM\System\CurrentControlSet\Services
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers

https://attack.mitre.org/techniques/T1547/

Codecs

- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
- HKCU\Software\Classes\Filter
- HKCU\Software\Classes\CLSID\{083863F1-70DE-11d0-BD40-00A0C911CE86}\Instance
- HKCU\Software\Classes\CLSID\{AC757296-3522-4E11-9862-C17BE5A1767E}\Instance
- HKCU\Software\Classes\CLSID\{7ED96837-96F0-4812-B211-F13C24117ED3}\Instance
- HKCU\Software\Classes\CLSID\{ABE3B9A4-257D-4B97-BD1A-294AF496222E}\Instance
- HKCU\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
- HKCU\Software\Wow6432Node\Classes\CLSID\{083863F1-70DE-11d0-BD40-00A0C911CE86}\Instance
- HKCU\Software\Wow6432Node\Classes\CLSID\{AC757296-3522-4E11-9862-C17BE5A1767E}\Instance
- HKCU\Software\Wow6432Node\Classes\CLSID\{7ED96837-96F0-4812-B211-F13C24117ED3}\Instance
- HKCU\Software\Wow6432Node\Classes\CLSID\{ABE3B9A4-257D-4B97-BD1A-294AF496222E}\Instance
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
- HKLM\Software\Classes\Filter
- HKLM\Software\Classes\CLSID\{083863F1-70DE-11d0-BD40-00A0C911CE86}\Instance
- HKLM\Software\Classes\CLSID\{AC757296-3522-4E11-9862-C17BE5A1767E}\Instance
- HKLM\Software\Classes\CLSID\{7ED96837-96F0-4812-B211-F13C24117ED3}\Instance
- HKLM\Software\Classes\CLSID\{ABE3B9A4-257D-4B97-BD1A-294AF496222E}\Instance
- HKLM\Software\Wow6432Node\Classes\Filter
- HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
- HKLM\Software\Wow6432Node\Classes\CLSID\{083863F1-70DE-11d0-BD40-00A0C911CE86}\Instance
- HKLM\Software\Wow6432Node\Classes\CLSID\{AC757296-3522-4E11-9862-C17BE5A1767E}\Instance
- HKLM\Software\Wow6432Node\Classes\CLSID\{7ED96837-96F0-4812-B211-F13C24117ED3}\Instance
- HKLM\Software\Wow6432Node\Classes\CLSID\{ABE3B9A4-257D-4B97-BD1A-294AF496222E}\Instance

AppInit

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls
- HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls

https://attack.mitre.org/techniques/T1546/

Known DLLs

- HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls

https://attack.mitre.org/techniques/T1574/

Print Monitors

- HKLM\System\CurrentControlSet\Control\Print\Monitors
- HKLM\System\CurrentControlSet\Control\Print\Providers

Network Providers

- HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order
- HKLM\SYSTEM\CurrentControlSet\Services\<NetworkProviderName>\NetworkProvider\ProviderPath

https://attack.mitre.org/techniques/T1556/

Create Accout

- Local Account
- Domain Account
- Cloud Account

https://attack.mitre.org/techniques/T1136/ & https://attack.mitre.org/techniques/T1098 & https://attack.mitre.org/techniques/T1078/

Browser Extensions

https://attack.mitre.org/techniques/T1176/

Powershell Profile

- $PsHome\Profile.ps1
- $PsHome\Microsoft.{HostProgram}_profile.ps1
- $Home\My Documents\PowerShell\Profile.ps1
- $Home\My Documents\PowerShell\Microsoft.{HostProgram}_profile.ps1

https://attack.mitre.org/techniques/T1546/

Explorer

- HKCU\SOFTWARE\Classes\Protocols\Filter
- HKCU\SOFTWARE\Classes\Protocols\Handler
- HKCU\SOFTWARE\Microsoft\Internet Explorer\Desktop\Components
- HKCU\Software\Classes*\ShellEx\ContextMenuHandlers
- HKCU\Software\Classes\Drive\ShellEx\ContextMenuHandlers
- HKCU\Software\Classes*\ShellEx\PropertySheetHandlers
- HKCU\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers
- HKCU\Software\Classes\AllFileSystemObjects\ShellEx\DragDropHandlers
- HKCU\Software\Classes\AllFileSystemObjects\ShellEx\PropertySheetHandlers
- HKCU\Software\Classes\Directory\ShellEx\ContextMenuHandlers
- HKCU\Software\Classes\Directory\ShellEx\DragDropHandlers
- HKCU\Software\Classes\Directory\ShellEx\PropertySheetHandlers
- HKCU\Software\Classes\Directory\ShellEx\CopyHookHandlers
- HKCU\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers
- HKCU\Software\Classes\Folder\ShellEx\ContextMenuHandlers
- HKCU\Software\Classes\Folder\ShellEx\DragDropHandlers
- HKCU\Software\Classes\Folder\ShellEx\PropertySheetHandlers
- HKCU\Software\Classes\Folder\ShellEx\ColumnHandlers
- HKCU\Software\Classes\Folder\ShellEx\ExtShellFolderViews
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
- HKCU\Software\Classes\CLSID\{AB8902B4-09CA-4bb6-B78D-A8F59079A8D5}\InProcServer32
- HKCU\Software\Microsoft\Ctf\LangBarAddin
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler
- HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects
- HKLM\SOFTWARE\Classes\Protocols\Filter
- HKLM\SOFTWARE\Classes\Protocols\Handler
- HKLM\Software\Classes*\ShellEx\ContextMenuHandlers
- HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers
- HKLM\Software\Classes*\ShellEx\PropertySheetHandlers
- HKLM\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers
- HKLM\Software\Classes\AllFileSystemObjects\ShellEx\DragDropHandlers
- HKLM\Software\Classes\AllFileSystemObjects\ShellEx\PropertySheetHandlers
- HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers
- HKLM\Software\Classes\Directory\ShellEx\DragDropHandlers
- HKLM\Software\Classes\Directory\ShellEx\PropertySheetHandlers
- HKLM\Software\Classes\Directory\ShellEx\CopyHookHandlers
- HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers
- HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers
- HKLM\Software\Classes\Folder\ShellEx\DragDropHandlers
- HKLM\Software\Classes\Folder\ShellEx\PropertySheetHandlers
- HKLM\Software\Classes\Folder\ShellEx\ColumnHandlers
- HKLM\Software\Classes\Folder\ShellEx\ExtShellFolderViews
- HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
- HKLM\Software\Microsoft\Ctf\LangBarAddin
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler
- HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects
- HKLM\Software\Wow6432Node\Classes*\ShellEx\ContextMenuHandlers
- HKLM\Software\Wow6432Node\Classes\Drive\ShellEx\ContextMenuHandlers
- HKLM\Software\Wow6432Node\Classes*\ShellEx\PropertySheetHandlers
- HKLM\Software\Wow6432Node\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers
- HKLM\Software\Wow6432Node\Classes\AllFileSystemObjects\ShellEx\DragDropHandlers
- HKLM\Software\Wow6432Node\Classes\AllFileSystemObjects\ShellEx\PropertySheetHandlers
- HKLM\Software\Wow6432Node\Classes\Directory\ShellEx\ContextMenuHandlers
- HKLM\Software\Wow6432Node\Classes\Directory\ShellEx\DragDropHandlers
- HKLM\Software\Wow6432Node\Classes\Directory\ShellEx\PropertySheetHandlers
- HKLM\Software\Wow6432Node\Classes\Directory\ShellEx\CopyHookHandlers
- HKLM\Software\Wow6432Node\Classes\Directory\Background\ShellEx\ContextMenuHandlers
- HKLM\Software\Wow6432Node\Classes\Folder\ShellEx\ContextMenuHandlers
- HKLM\Software\Wow6432Node\Classes\Folder\ShellEx\DragDropHandlers
- HKLM\Software\Wow6432Node\Classes\Folder\ShellEx\PropertySheetHandlers
- HKLM\Software\Wow6432Node\Classes\Folder\ShellEx\ColumnHandlers
- HKLM\Software\Wow6432Node\Classes\Folder\ShellEx\ExtShellFolderViews
- HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
- HKLM\Software\Wow6432Node\Microsoft\Ctf\LangBarAddin

Winlogon

- HKCU\SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop\Scrnsave.exe
- HKCU\Control Panel\Desktop\Scrnsave.exe
- HKLM\SYSTEM\Setup\CmdLine
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Taskman
- HKLM\System\CurrentControlSet\Control\BootVerificationProgram\ImagePath
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GpExtensions

https://attack.mitre.org/techniques/T1547/

Winsock Providers

- HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries
- HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries
- HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries64
- HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64

WMI

https://attack.mitre.org/techniques/T1546/003/

Pre-OS Boot

- System Firmware
- Component Firmware
- Bootkit
- TFTP Boot

https://attack.mitre.org/techniques/T1542/

BITS Jobs - Background Intelligent Transfer Service

- Powershell
- BITSAdmin

https://attack.mitre.org/techniques/T1197/

External Remote Service

- WMI
- RDP
- SMB/CIFS
- WinRM (over HTTP/HTTPS)
- NetBios

https://attack.mitre.org/techniques/T1133/