AUTOrUN AND AUTOLOAD INFORMATION

C: \> wmic startup list full

C: \> wmic ntdomain list brief

C: \> dir

“%SystyemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup”

C: \> dir “%SystemDrive%\Documents and Settings\All Users\Start Menu\Programs\Startup

C: \> dir %userprofile%\Start Menu\Programs\Startup

C: \> %ProgramFiles%\Startup\

C: \> dir C:\Windows\Start Menu\Programs\startup

C: \> dir “C:\Users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup”

C: \> “%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup”

C: \> dir “%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Startup”

C: \> dir “%ALLUSERSPROFILES%\Start Menu\Programs\Startup”

C: \> type C:\Windows\winstart.bat

C: \> type %windir%\wininit.ini

C: \> type %windir%\win.ini

**View autoruns, hide Microsoft files:**

Ref. <https://technet.microsft.com/enus/sysinternals/bb963902.aspx>

C: \> autorunsc -accepteula –m

C: \> type C:\Autoexec.bat”

**Show all autorun files, export to csv and check with VirusTotal:**

C: \> autorunsc.exe –accepteula –a –c –I –e –f –l –m –v

**HKEY\_CLASSES\_ROOT:**

C: \> reg query HKCR\Comfile\Shell\Open\Command

C: \> reg query HKCR\Batfile\Shell\Open\Command

C: \> reg query HKCR\htafile\Shell\Open\Command

C: \> reg query HKCR\Exefile\Shell\Open\Command

C: \> reg query HKCR\Exefiles\Shell\Open\Command

C: \> reg query HKCR\piffile\Shell\Open\Command

**HKEY\_CURRENT\_USERS:**

C: \> reg query “HKCU\Control Panel\Desktop”

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Runonce

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Windows\Load

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Windows\Scripts

C: \> reg query “HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows” /f run

C: \> reg query “HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows” /f load

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU /s

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders”

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders”

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Apple ts\RegEdit /v LastKey

C: \> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Apple ts\RegEdit /v LastKey

C: \> reg query “HKCU\Software\Microsoft\Internet Explorer\TypedURLs”

C: \> reg query “HKCU\Software\Microsoft\Internet Explorer\TypedURLs”

C: \> reg query “HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop”

**HKEY\_LOCAL\_MACHINE:**

C: \> reg query “HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components” /s

C: \> reg query “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders”

C: \> reg query “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders”

C: \> reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks

C: \> reg query “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects” /s

C: \> reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer