sor.exe

Is DLL | Packer | Anti Debug | Anti VM | Signed | XOR

MalFamily: Malicious **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	30.00 KB (30720 bytes)
Compile time:	2019-07-17 17:45:19
MD5:	facb332629697bd8b3f64a49768bdabf
SHA1:	033d16ec67f59bd258ea15f3ddd8e8f028a551dc
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2019-08-14 08:12:05

URL(s) file hosting

http://surfcrypto.life/sor.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2019-08-08 23:42:03	51/68	

Import library

mscoree.dll

26 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)

Attempts to stop active services

- servicename: ShellHWDetection

Attempts to repeatedly call a single API many times in order to delay analysis time

- Spam: lsass.exe (484) called API NtClose 58152 times
- Spam: services.exe (476) called API GetSystemTimeAsFileTime 2500632 times

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SteamClient
- data: "C:\Users\Seven01\AppData\Local\Temp\sor.exe"
- file: C:\Windows\Tasks\Adobe Flash Player Updater.job
- file: C:\Windows\Tasks\SCHEDLGU.TXT
- file: C:\Windows\Tasks\SCHEDLGU.TXT
- file: C:\Windows\Tasks\Adobe Flash Player Updater.job
- task: schtasks.exe /create /sc MINUTE /mo 1 /tn "Windows Audio" /tr "C:\Users\Seven01\AppData\Roaming\NVIDIA GeForce Experience\dllhost.exe" /f

Retrieves Windows ProductID, probably to fingerprint the sandbox

Checks the version of Bios, possibly for anti-virtualization

Checks the CPU name from registry, possibly for anti-virtualization

Checks the system manufacturer, likely for anti-virtualization

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\NVIDIA GeForce Experience\dllhost.exe

Collects information to fingerprint the system

Uses Windows utilities for basic functionality

- command: schtasks.exe /create /sc MINUTE /mo 1 /tn "Windows Audio" /tr "C:\Users\Seven01\AppData\Roaming\NVIDIA GeForce Experience\dllhost.exe" /f
- command: schtasks.exe /create /sc MINUTE /mo 1 /tn "Windows Audio" /tr "C:\Users\Seven01\AppData\Roaming\NVIDIA GeForce Experience\dllhost.exe" /f

Creates an autorun.inf file

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.43, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00006e00, virtual_size: 0x00006dc4

A process created a hidden window

- Process: sor.exe -> schtasks.exe

Creates RWX memory

Possible date expiration check, exits too soon after checking local time

- process: schtasks.exe, PID 2820

Anomalous file deletion behavior detected (10+)

- DeletedFile: C:\Windows\Tasks\Windows Audio.job
- DeletedFile: C:\Windows\sysnative\Tasks\Microsoft\Windows\Customer Experience Improvement Program\Uploader
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\WER24BF.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\WER24BF.tmp.WERInternalMetadata.xml
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\WER24BF.tmp.WERInternalMetadata.xml
- DeletedFile: C:\Windows\Temp\WERF14.tmp
- DeletedFile: C:\Windows\Temp\WERF14.tmp.appcompat.txt
- DeletedFile: C:\Windows\Temp\WERF14.tmp.appcompat.txt

- DeletedFile: C:\Windows\Temp\WER16F5.tmp
- DeletedFile: C:\Windows\Temp\WER16F5.tmp.WERInternalMetadata.xml
- DeletedFile: C:\Windows\Temp\WER1792.tmp
- DeletedFile: C:\Windows\Temp\WER1792.tmp.WERDataCollectionFailure.txt
- DeletedFile: C:\Windows\Temp\WERF14.tmp.appcompat.txt
- DeletedFile: C:\Windows\Temp\WER16F5.tmp.WERInternalMetadata.xml
- DeletedFile: C:\Windows\Temp\WER1792.tmp.WERDataCollectionFailure.txt
- DeletedFile: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\WER6FFC.tmp
- DeletedFile: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\WER6FFC.tmp.appcompat.txt
- DeletedFile: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\WER6FFC.tmp.appcompat.txt
- DeletedFile: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\WER74B0.tmp
- DeletedFile: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\WER74B0.tmp.WERInternalMetadata.xml
- DeletedFile: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\WER7BE5.tmp
- DeletedFile: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\WER7BE5.tmp.hdmp
- DeletedFile: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\WERA5E4.tmp
- DeletedFile: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\WERA5E4.tmp.mdmp
- DeletedFile: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\WER6FFC.tmp.appcompat.txt
- DeletedFile: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\WER74B0.tmp.WERInternalMetadata.xml
- DeletedFile: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\WER7BE5.tmp.hdmp
- DeletedFile: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\WERA5E4.tmp.mdmp

Guard pages use detected - possible anti-debugging.

A process attempted to delay the analysis task.

- Process: sor.exe tried to sleep 456 seconds, actually delayed analysis time by 0 seconds
- Process: WmiPrvSE.exe tried to sleep 301 seconds, actually delayed analysis time by 0 seconds
- Process: svchost.exe tried to sleep 541 seconds, actually delayed analysis time by 0 seconds

Loads a driver

- driver service name: \Registry\Machine\System\CurrentControlSet\Services\srv
- driver service name: \Registry\Machine\System\CurrentControlSet\Services\Srv

Dynamic (imported) function loading detected

- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: KERNEL32.dll/FlsAlloc
- DynamicLoader: KERNEL32.dll/FlsFree
- DynamicLoader: KERNEL32.dll/FlsGetValue
- DynamicLoader: KERNEL32.dll/FlsSetValue
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionEx
- DynamicLoader: KERNEL32.dll/CreateEventExW
- DynamicLoader: KERNEL32.dll/CreateSemaphoreExW
- DynamicLoader: KERNEL32.dll/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/CreateThreadpoolTimer
- DynamicLoader: KERNEL32.dll/SetThreadpoolTimer
- DynamicLoader: KERNEL32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: KERNEL32.dll/CloseThreadpoolTimer
- DynamicLoader: KERNEL32.dll/CreateThreadpoolWait
- DynamicLoader: KERNEL32.dll/SetThreadpoolWait
- DynamicLoader: KERNEL32.dll/CloseThreadpoolWait
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers

- DynamicLoader: KERNEL32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: KERNEL32.dll/GetCurrentProcessorNumber
- DynamicLoader: KERNEL32.dll/GetLogicalProcessorInformation
- DynamicLoader: KERNEL32.dll/CreateSymbolicLinkW
- DynamicLoader: KERNEL32.dll/SetDefaultDllDirectories
- DynamicLoader: KERNEL32.dll/EnumSystemLocalesEx
- DynamicLoader: KERNEL32.dll/CompareStringEx
- DynamicLoader: KERNEL32.dll/GetDateFormatEx
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/GetTimeFormatEx
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/IsValidLocaleName
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: KERNEL32.dll/GetCurrentPackageId
- DynamicLoader: KERNEL32.dll/GetTickCount64
- DynamicLoader: KERNEL32.dll/GetFileInformationByHandleExW
- DynamicLoader: KERNEL32.dll/SetFileInformationByHandleW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: MSCOREE.DLL/
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: mscoreei.dll/RegisterShimImplCallback
- DynamicLoader: mscoreei.dll/RegisterShimImplCleanupCallback
- DynamicLoader: mscoreei.dll/SetShellShimInstance
- DynamicLoader: mscoreei.dll/OnShimDllMainCalled
- DynamicLoader: mscoreei.dll/_CorExeMain_RetAddr
- DynamicLoader: mscoreei.dll/_CorExeMain
- DynamicLoader: SHLWAPI.dll/UrlIsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/FlsAlloc
- DynamicLoader: KERNEL32.dll/FlsFree
- DynamicLoader: KERNEL32.dll/FlsGetValue
- DynamicLoader: KERNEL32.dll/FlsSetValue
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionEx
- DynamicLoader: KERNEL32.dll/CreateEventExW
- DynamicLoader: KERNEL32.dll/CreateSemaphoreExW
- DynamicLoader: KERNEL32.dll/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/CreateThreadpoolTimer
- DynamicLoader: KERNEL32.dll/SetThreadpoolTimer
- DynamicLoader: KERNEL32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: KERNEL32.dll/CloseThreadpoolTimer
- DynamicLoader: KERNEL32.dll/CreateThreadpoolWait
- DynamicLoader: KERNEL32.dll/SetThreadpoolWait
- DynamicLoader: KERNEL32.dll/CloseThreadpoolWait
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: KERNEL32.dll/GetCurrentProcessorNumber
- DynamicLoader: KERNEL32.dll/GetLogicalProcessorInformation
- DynamicLoader: KERNEL32.dll/CreateSymbolicLinkW
- DynamicLoader: KERNEL32.dll/SetDefaultDllDirectories
- DynamicLoader: KERNEL32.dll/EnumSystemLocalesEx
- DynamicLoader: KERNEL32.dll/CompareStringEx
- DynamicLoader: KERNEL32.dll/GetDateFormatEx
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/GetTimeFormatEx
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/IsValidLocaleName
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: KERNEL32.dll/GetCurrentPackageId

- DynamicLoader: KERNEL32.dll/GetTickCount64
- DynamicLoader: KERNEL32.dll/GetFileInformationByHandleExW
- DynamicLoader: KERNEL32.dll/SetFileInformationByHandleW
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: clr.dll/SetRuntimeInfo
- DynamicLoader: clr.dll/_CorExeMain
- DynamicLoader: MSCOREE.DLL/CreateConfigStream
- DynamicLoader: mscoreei.dll/CreateConfigStream_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream
- DynamicLoader: KERNEL32.dll/GetNumaHighestNodeNumber
- DynamicLoader: KERNEL32.dll/FlsSetValue
- DynamicLoader: KERNEL32.dll/FlsGetValue
- DynamicLoader: KERNEL32.dll/FlsAlloc
- DynamicLoader: KERNEL32.dll/FlsFree
- DynamicLoader: ntdll.dll/RtlVirtualUnwind
- DynamicLoader: KERNEL32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/AddSIDToBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/CreateBoundaryDescriptorW
- DynamicLoader: KERNEL32.dll/CreatePrivateNamespaceW
- DynamicLoader: KERNEL32.dll/OpenPrivateNamespaceW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/DeleteBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/WerRegisterRuntimeExceptionModule
- DynamicLoader: KERNEL32.dll/RaiseException
- DynamicLoader: MSCOREE.DLL/
- DynamicLoader: mscoreei.dll/
- DynamicLoader: KERNEL32.dll/AddDllDirectory
- DynamicLoader: KERNEL32.dll/SortGetHandle
- DynamicLoader: KERNEL32.dll/SortCloseHandle
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariable
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariableW
- DynamicLoader: KERNEL32.dll/ReleaseMutex
- DynamicLoader: KERNEL32.dll/CreateMutex

- DynamicLoader: KERNEL32.dll/CreateMutexW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/SetThreadErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: KERNEL32.dll/CreateDirectory
- DynamicLoader: KERNEL32.dll/CreateDirectoryW
- DynamicLoader: KERNEL32.dll/CopyFile
- DynamicLoader: KERNEL32.dll/CopyFileW
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetUserPreferredUILanguages
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: shell32.dll/ShellExecuteEx
- DynamicLoader: shell32.dll/ShellExecuteExW
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_Size_ExW
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_ExW
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: ADVAPI32.dll/GetUserName
- DynamicLoader: ADVAPI32.dll/GetUserNameW
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivilegesW
- DynamicLoader: ADVAPI32.dll/GetNamedSecurityInfoW
- DynamicLoader: ADVAPI32.dll/GetSecurityDescriptorLength
- DynamicLoader: ADVAPI32.dll/LsaClose
- DynamicLoader: ADVAPI32.dll/LsaFreeMemory
- DynamicLoader: ADVAPI32.dll/LsaOpenPolicy
- DynamicLoader: ADVAPI32.dll/LsaLookupNames2
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ADVAPI32.dll/SetNamedSecurityInfoW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ole32.dll/CoWaitForMultipleHandles
- DynamicLoader: nlssorting.dll/SortGetHandle
- DynamicLoader: nlssorting.dll/SortCloseHandle
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: KERNEL32.dll/CreateEvent
- DynamicLoader: KERNEL32.dll/CreateEventW
- DynamicLoader: ole32.dll/CoGetObjectContext
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKey
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegSetValueEx
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: ole32.dll/NdrOleInitializeExtension
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface

- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: USER32.dll/RegisterWindowMessage
- DynamicLoader: USER32.dll/RegisterWindowMessageW
- DynamicLoader: KERNEL32.dll/LoadLibrary
- DynamicLoader: KERNEL32.dll/LoadLibraryA
- DynamicLoader: KERNEL32.dll/WideCharToMultiByte
- DynamicLoader: KERNEL32.dll/GetProcAddress
- DynamicLoader: wminet_utils.dll/ResetSecurity
- DynamicLoader: wminet_utils.dll/SetSecurity
- DynamicLoader: wminet_utils.dll/BlessIWbemServices
- DynamicLoader: wminet_utils.dll/BlessIWbemServicesObject
- DynamicLoader: wminet_utils.dll/GetPropertyHandle
- DynamicLoader: wminet_utils.dll/WritePropertyValue
- DynamicLoader: wminet_utils.dll/Clone
- DynamicLoader: wminet_utils.dll/VerifyClientKey
- DynamicLoader: wminet_utils.dll/GetQualifierSet
- DynamicLoader: wminet_utils.dll/Get
- DynamicLoader: wminet_utils.dll/Put
- DynamicLoader: wminet_utils.dll/Delete
- DynamicLoader: wminet_utils.dll/GetNames
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: wminet_utils.dll/BeginEnumeration
- DynamicLoader: wminet_utils.dll/Next
- DynamicLoader: wminet_utils.dll/EndEnumeration
- DynamicLoader: wminet_utils.dll/GetPropertyQualifierSet
- DynamicLoader: wminet_utils.dll/Clone
- DynamicLoader: wminet_utils.dll/GetObjectText
- DynamicLoader: wminet_utils.dll/SpawnDerivedClass
- DynamicLoader: wminet_utils.dll/SpawnInstance
- DynamicLoader: wminet_utils.dll/CompareTo
- DynamicLoader: wminet_utils.dll/GetPropertyOrigin
- DynamicLoader: wminet_utils.dll/InheritsFrom
- DynamicLoader: wminet_utils.dll/GetMethod
- DynamicLoader: wminet_utils.dll/PutMethod
- DynamicLoader: wminet_utils.dll/DeleteMethod
- DynamicLoader: wminet_utils.dll/BeginMethodEnumeration
- DynamicLoader: wminet_utils.dll/NextMethod
- DynamicLoader: wminet_utils.dll/EndMethodEnumeration
- DynamicLoader: wminet_utils.dll/GetMethodQualifierSet
- DynamicLoader: wminet_utils.dll/GetMethodOrigin
- DynamicLoader: wminet_utils.dll/QualifierSet_Get
- DynamicLoader: wminet_utils.dll/QualifierSet_Put
- DynamicLoader: wminet_utils.dll/QualifierSet_Delete
- DynamicLoader: wminet_utils.dll/QualifierSet_GetNames
- DynamicLoader: wminet_utils.dll/QualifierSet_BeginEnumeration
- DynamicLoader: wminet_utils.dll/QualifierSet_Next
- DynamicLoader: wminet_utils.dll/QualifierSet_EndEnumeration
- DynamicLoader: wminet_utils.dll/GetCurrentApartmentType
- DynamicLoader: wminet_utils.dll/GetDemultiplexedStub
- DynamicLoader: wminet_utils.dll/CreateInstanceEnumWmi
- DynamicLoader: wminet_utils.dll/CreateClassEnumWmi
- DynamicLoader: wminet_utils.dll/ExecQueryWmi
- DynamicLoader: wminet_utils.dll/ExecNotificationQueryWmi
- DynamicLoader: wminet_utils.dll/PutInstanceWmi
- DynamicLoader: wminet_utils.dll/PutClassWmi
- DynamicLoader: wminet_utils.dll/CloneEnumWbemClassObject

- DynamicLoader: wminet_utils.dll/ConnectServerWmi
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: ole32.dll/IIDFromString
- DynamicLoader: KERNEL32.dll/GetModuleHandle
- DynamicLoader: KERNEL32.dll/GetModuleHandleW
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: KERNEL32.dll/LoadLibrary
- DynamicLoader: KERNEL32.dll/LoadLibraryW
- DynamicLoader: KERNEL32.dll/ResolveDelayLoadedAPI
- DynamicLoader: ole32.dll/CoCreateFreeThreadedMarshaler
- DynamicLoader: ole32.dll/CoGetObjectContext
- DynamicLoader: USER32.dll/AdjustWindowRectEx
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentThread
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: KERNEL32.dll/GetCurrentThreadId
- DynamicLoader: KERNEL32.dll/GetProcAddress
- DynamicLoader: USER32.dll/DefWindowProcW
- DynamicLoader: GDI32.dll/GetStockObject
- DynamicLoader: USER32.dll/RegisterClass
- DynamicLoader: USER32.dll/RegisterClassW
- DynamicLoader: USER32.dll/CreateWindowEx
- DynamicLoader: USER32.dll/CreateWindowExW
- DynamicLoader: USER32.dll/SetWindowLongPtr
- DynamicLoader: USER32.dll/SetWindowLongPtrW
- DynamicLoader: USER32.dll/GetWindowLongPtr
- DynamicLoader: USER32.dll/GetWindowLongPtrW
- DynamicLoader: USER32.dll/SetWindowLongPtr
- DynamicLoader: USER32.dll/SetWindowLongPtrW
- DynamicLoader: USER32.dll/CallWindowProc
- DynamicLoader: USER32.dll/CallWindowProcW
- DynamicLoader: USER32.dll/GetClientRect
- DynamicLoader: USER32.dll/GetWindowRect
- DynamicLoader: USER32.dll/GetParent
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: USER32.dll/GetProcessWindowStation
- DynamicLoader: USER32.dll/GetUserObjectInformation
- DynamicLoader: USER32.dll/GetUserObjectInformationA
- DynamicLoader: KERNEL32.dll/SetConsoleCtrlHandler
- DynamicLoader: KERNEL32.dll/SetConsoleCtrlHandlerW
- DynamicLoader: KERNEL32.dll/GetModuleHandle
- DynamicLoader: KERNEL32.dll/GetModuleHandleW
- DynamicLoader: USER32.dll/GetClassInfo
- DynamicLoader: USER32.dll/GetClassInfoW
- DynamicLoader: USER32.dll/RegisterClass
- DynamicLoader: USER32.dll/RegisterClassW
- DynamicLoader: USER32.dll/CreateWindowEx
- DynamicLoader: USER32.dll/CreateWindowExW
- DynamicLoader: USER32.dll/DefWindowProc
- DynamicLoader: USER32.dll/DefWindowProcW
- DynamicLoader: KERNEL32.dll/GetStartupInfo
- DynamicLoader: KERNEL32.dll/GetStartupInfoW
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/GetDC
- DynamicLoader: GDI32.dll/GetDeviceCaps
- DynamicLoader: USER32.dll/ReleaseDC
- DynamicLoader: USER32.dll/CreateIconFromResourceEx
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: USER32.dll/GetSystemMenu
- DynamicLoader: USER32.dll/GetWindowPlacement
- DynamicLoader: USER32.dll/EnableMenuItem
- DynamicLoader: USER32.dll/GetClientRect

- DynamicLoader: USER32.dll/GetWindowTextLength
- DynamicLoader: USER32.dll/GetWindowTextLengthW
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/GetWindowText
- DynamicLoader: USER32.dll/GetWindowTextW
- DynamicLoader: USER32.dll/SetWindowPos
- DynamicLoader: USER32.dll/RedrawWindow
- DynamicLoader: USER32.dll/SetClipboardViewer
- DynamicLoader: USER32.dll/SetClipboardViewerW
- DynamicLoader: ole32.dll/OleInitialize
- DynamicLoader: ole32.dll/OleGetClipboard
- DynamicLoader: KERNEL32.dll/GlobalLock
- DynamicLoader: KERNEL32.dll/GlobalUnlock
- DynamicLoader: KERNEL32.dll/GlobalFree
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: USER32.dll/IsWindowVisible
- DynamicLoader: ole32.dll/CoRegisterMessageFilter
- DynamicLoader: USER32.dll/PeekMessage
- DynamicLoader: USER32.dll/PeekMessageW
- DynamicLoader: USER32.dll/WaitMessage
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ADVAPI32.dll/RegEnumValue
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: USER32.dll/IsWindowUnicode
- DynamicLoader: USER32.dll/GetMessageW
- DynamicLoader: USER32.dll/TranslateMessage
- DynamicLoader: USER32.dll/DispatchMessageW
- DynamicLoader: KERNEL32.dll/GetThreadPreferredUILanguages
- DynamicLoader: KERNEL32.dll/SetThreadPreferredUILanguages
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetSystemDefaultLocaleName
- DynamicLoader: fastprox.dll/DllGetClassObject
- DynamicLoader: fastprox.dll/DllCanUnloadNow
- DynamicLoader: OLEAUT32.dll/SysStringLen
- DynamicLoader: KERNEL32.dll/RtlZeroMemory
- DynamicLoader: KERNEL32.dll/RegOpenKeyExW
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: USER32.dll/PostMessage
- DynamicLoader: USER32.dll/PostMessageW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: KERNEL32.dll/CompareStringOrdinal
- DynamicLoader: clr.dll/CreateAssemblyNameObject
- DynamicLoader: clr.dll/CreateAssemblyNameObjectW
- DynamicLoader: clr.dll/CreateAssemblyEnum
- DynamicLoader: clr.dll/CreateAssemblyEnumW
- DynamicLoader: KERNEL32.dll/ResolveLocaleName
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: CRYPTSP.dll/CryptGetDefaultProviderW
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentProcessW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/GetTokenInformationW
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: KERNEL32.dll/LocalAllocW

- DynamicLoader: ADVAPI32.dll/DuplicateTokenEx
- DynamicLoader: ADVAPI32.dll/DuplicateTokenExW
- DynamicLoader: ADVAPI32.dll/CheckTokenMembership
- DynamicLoader: ADVAPI32.dll/CheckTokenMembershipW
- DynamicLoader: KERNEL32.dll/GetComputerName
- DynamicLoader: KERNEL32.dll/GetComputerNameW
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: KERNEL32.dll/GetFileType
- DynamicLoader: KERNEL32.dll/GetFileSize
- DynamicLoader: KERNEL32.dll/ReadFile
- DynamicLoader: KERNEL32.dll/QueryPerformanceFrequency
- DynamicLoader: KERNEL32.dll/QueryPerformanceCounter
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: rasapi32.dll/RasEnumConnections
- DynamicLoader: rasapi32.dll/RasEnumConnectionsW
- DynamicLoader: rtutils.dll/TraceRegisterExA
- DynamicLoader: rtutils.dll/TracePrintfExA
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: WS2_32.dll/WSAStartup
- DynamicLoader: WS2_32.dll/WSASocket
- DynamicLoader: WS2_32.dll/WSASocketW
- DynamicLoader: WS2_32.dll/setsockopt
- DynamicLoader: WS2_32.dll/WSAEventSelect
- DynamicLoader: WS2_32.dll/ioctlsocket
- DynamicLoader: WS2_32.dll/closesocket
- DynamicLoader: WS2_32.dll/ioctlsocket
- DynamicLoader: WS2_32.dll/WSAIoctl
- DynamicLoader: KERNEL32.dll/FormatMessage
- DynamicLoader: KERNEL32.dll/FormatMessageW
- DynamicLoader: WS2_32.dll/WSAEventSelect
- DynamicLoader: rasapi32.dll/RasConnectionNotification
- DynamicLoader: rasapi32.dll/RasConnectionNotificationW
- DynamicLoader: ADVAPI32.dll/RegOpenCurrentUser
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegNotifyChangeKeyValue
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: winhttp.dll/WinHttpOpen
- DynamicLoader: winhttp.dll/WinHttpOpenW
- DynamicLoader: winhttp.dll/WinHttpCloseHandle
- DynamicLoader: winhttp.dll/WinHttpCloseHandleW
- DynamicLoader: sechost.dll/NotifyServiceStatusChangeA
- DynamicLoader: winhttp.dll/WinHttpSetTimeouts
- DynamicLoader: winhttp.dll/WinHttpSetTimeoutsW
- DynamicLoader: winhttp.dll/WinHttpGetIEProxyConfigForCurrentUser
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware

- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: SspiCli.dll/GetUserNameExW
- DynamicLoader: ADVAPI32.dll/GetUserNameW
- DynamicLoader: XmlLite.dll/CreateXmlWriter
- DynamicLoader: XmlLite.dll/CreateXmlWriterOutputWithEncodingName
- DynamicLoader: tschannel.dll/DllGetClassObject
- DynamicLoader: tschannel.dll/DllCanUnloadNow
- DynamicLoader: WTSAPI32.dll/WTSQueryUserToken
- DynamicLoader: USERENV.dll/CreateEnvironmentBlock
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: SSPICLI.DLL/GetUserNameExW
- DynamicLoader: SHELL32.dll/SHChangeNotify
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: USERENV.dll/DestroyEnvironmentBlock
- DynamicLoader: qmgr.dll/ServiceMain
- DynamicLoader: qmgr.dll/SvchostPushServiceGlobals
- DynamicLoader: ADVAPI32.dll/RegisterEventSourceW
- DynamicLoader: ADVAPI32.dll/ReportEventW
- DynamicLoader: ADVAPI32.dll/DeregisterEventSource
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ole32.dll/CoInitializeSecurity
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: wmisvc.dll/ServiceMain
- DynamicLoader: wmisvc.dll/SvchostPushServiceGlobals
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: kernel32.dll/ResolveDelayLoadedAPI
- DynamicLoader: VSSAPI.DLL/CreateWriter
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ADVAPI32.dll/LookupAccountNameW
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: samcli.dll/NetLocalGroupGetMembers
- DynamicLoader: SAMLIB.dll/SamConnect
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeW
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcStringFreeW

- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: SAMLIB.dll/SamOpenDomain
- DynamicLoader: SAMLIB.dll/SamLookupNamesInDomain
- DynamicLoader: SAMLIB.dll/SamOpenAlias
- DynamicLoader: SAMLIB.dll/SamFreeMemory
- DynamicLoader: SAMLIB.dll/SamCloseHandle
- DynamicLoader: SAMLIB.dll/SamGetMembersInAlias
- DynamicLoader: netutils.dll/NetApiBufferFree
- DynamicLoader: SAMLIB.dll/SamEnumerateDomainsInSamServer
- DynamicLoader: SAMLIB.dll/SamLookupDomainInSamServer
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/StringFromCLSID
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: PROPSYS.dll/VariantToPropVariant
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemsvc.dll/DllGetClassObject
- DynamicLoader: wbemsvc.dll/DllCanUnloadNow
- DynamicLoader: authZ.dll/AuthzInitializeContextFromToken
- DynamicLoader: authZ.dll/AuthzInitializeObjectAccessAuditEvent2
- DynamicLoader: authZ.dll/AuthzAccessCheck
- DynamicLoader: authZ.dll/AuthzFreeAuditEvent
- DynamicLoader: authZ.dll/AuthzFreeContext
- DynamicLoader: authZ.dll/AuthzInitializeResourceManager
- DynamicLoader: authZ.dll/AuthzFreeResourceManager
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcBindingCreateW
- DynamicLoader: RPCRT4.dll/RpcBindingBind
- DynamicLoader: RPCRT4.dll/I_RpcMapWin32Status
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: ADVAPI32.dll/EventWrite
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: ADVAPI32.dll/EventEnabled
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: kernel32.dll/RegSetValueExW
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: kernel32.dll/RegQueryValueExW
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: wmisvc.dll/IsImproperShutdownDetected
- DynamicLoader: Wevtapi.dll/EvtRender
- DynamicLoader: Wevtapi.dll/EvtNext
- DynamicLoader: Wevtapi.dll/EvtClose
- DynamicLoader: Wevtapi.dll/EvtQuery
- DynamicLoader: Wevtapi.dll/EvtCreateRenderContext
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeW
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/RpcBindingSetOption
- DynamicLoader: RPCRT4.dll/RpcStringFreeW
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: kernel32.dll/ResolveDelayLoadedAPI
- DynamicLoader: ole32.dll/CoCreateFreeThreadedMarshaler
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CreateStreamOnHGlobal
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext

- DynamicLoader: KERNELBASE.dll/InitializeAcl
- DynamicLoader: KERNELBASE.dll/AddAce
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: kernel32.dll/OpenProcessToken
- DynamicLoader: KERNELBASE.dll/GetTokenInformation
- DynamicLoader: KERNELBASE.dll/DuplicateTokenEx
- DynamicLoader: KERNELBASE.dll/AdjustTokenPrivileges
- DynamicLoader: KERNELBASE.dll/AllocateAndInitializeSid
- DynamicLoader: KERNELBASE.dll/CheckTokenMembership
- DynamicLoader: kernel32.dll/SetThreadToken
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: ole32.dll/CLSIDFromString
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: authZ.dll/AuthzInitializeContextFromToken
- DynamicLoader: authZ.dll/AuthzInitializeResourceManager
- DynamicLoader: authZ.dll/AuthzInitializeContextFromSid
- DynamicLoader: authZ.dll/AuthzInitializeContextFromToken
- DynamicLoader: authZ.dll/AuthzAccessCheck
- DynamicLoader: authZ.dll/AuthzFreeContext
- DynamicLoader: authZ.dll/AuthzFreeResourceManager
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetCallContext
- DynamicLoader: ole32.dll/CoRevertToSelf
- DynamicLoader: SspiCli.dll/LogonUserExExW
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: ole32.dll/CoImpersonateClient
- DynamicLoader: ole32.dll/CoSwitchCallContext
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: kernel32.dll/ResolveDelayLoadedAPI
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/SetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/LocaleNameToLCID
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/LCIDToLocaleName
- DynamicLoader: kernel32.dll/GetSystemDefaultLocaleName
- DynamicLoader: FastProx.dll/DllGetClassObject
- DynamicLoader: FastProx.dll/DllCanUnloadNow
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: kernel32.dll/RegQueryValueExW
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: ADVAPI32.dll/EventWrite
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: ADVAPI32.dll/EventEnabled

- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: WMI.DLL/WmiQueryAllDataW
- DynamicLoader: WMI.DLL/WmiQuerySingleInstanceW
- DynamicLoader: WMI.DLL/WmiSetSingleItemW
- DynamicLoader: WMI.DLL/WmiSetSingleInstanceW
- DynamicLoader: WMI.DLL/WmiExecuteMethodW
- DynamicLoader: WMI.DLL/WmiNotificationRegistrationW
- DynamicLoader: WMI.DLL/WmiMofEnumerateResourcesW
- DynamicLoader: WMI.DLL/WmiFileHandleToInstanceNameW
- DynamicLoader: WMI.DLL/WmiDevInstToInstanceNameW
- DynamicLoader: WMI.DLL/WmiQueryGuidInformation
- DynamicLoader: WMI.DLL/WmiOpenBlock
- DynamicLoader: WMI.DLL/WmiCloseBlock
- DynamicLoader: WMI.DLL/WmiFreeBuffer
- DynamicLoader: WMI.DLL/WmiEnumerateGuids
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: DEVOBJ.dll/DevObjCreateDeviceInfoList
- DynamicLoader: DEVOBJ.dll/DevObjGetClassDevs
- DynamicLoader: DEVOBJ.dll/DevObjEnumDeviceInterfaces
- DynamicLoader: DEVOBJ.dll/DevObjGetDeviceInterfaceDetail
- DynamicLoader: CFGMGR32.dll/CM_Connect_MachineA
- DynamicLoader: CFGMGR32.dll/CM_Disconnect_Machine
- DynamicLoader: CFGMGR32.dll/CM_Locate_DevNodeW
- DynamicLoader: CFGMGR32.dll/CM_Get_DevNode_Registry_PropertyW
- DynamicLoader: CFGMGR32.dll/CM_Get_Child
- DynamicLoader: CFGMGR32.dll/CM_Get_Sibling
- DynamicLoader: CFGMGR32.dll/CM_Get_DevNode_Status
- DynamicLoader: CFGMGR32.dll/CM_Get_First_Log_Conf
- DynamicLoader: CFGMGR32.dll/CM_Get_Next_Res_Des
- DynamicLoader: CFGMGR32.dll/CM_Get_Res_Des_Data
- DynamicLoader: CFGMGR32.dll/CM_Get_Res_Des_Data_Size
- DynamicLoader: CFGMGR32.dll/CM_Free_Log_Conf_Handle
- DynamicLoader: CFGMGR32.dll/CM_Free_Res_Des_Handle
- DynamicLoader: CFGMGR32.dll/CM_Get_Device_IDA
- DynamicLoader: CFGMGR32.dll/CM_Get_Device_ID_Size
- DynamicLoader: CFGMGR32.dll/CM_Get_Parent
- DynamicLoader: ole32.dll/CLSIDFromString
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: DEVOBJ.dll/DevObjDestroyDeviceInfoList
- DynamicLoader: DEVOBJ.dll/DevObjEnumDeviceInfo
- DynamicLoader: SETUPAPI.dll/CM_Open_DevNode_Key_Ex
- DynamicLoader: DEVOBJ.dll/DevObjGetDeviceProperty
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/MonitorFromWindow
- DynamicLoader: USER32.dll/MonitorFromRect
- DynamicLoader: USER32.dll/MonitorFromPoint
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/EnumDisplayDevicesW
- DynamicLoader: USER32.dll/GetMonitorInfoW
- DynamicLoader: dxgi.dll/DXGIReportAdapterConfiguration
- DynamicLoader: SETUPAPI.dll/SetupDiGetClassDevsW
- DynamicLoader: SETUPAPI.dll/SetupDiEnumDeviceInterfaces
- DynamicLoader: SETUPAPI.dll/SetupDiGetDeviceInterfaceDetailW
- DynamicLoader: SETUPAPI.dll/SetupDiDestroyDeviceInfoList
- DynamicLoader: GDI32.dll/D3DKMTOpenAdapterFromDeviceName

- DynamicLoader: GDI32.dll/D3DKMTQueryAdapterInfo
- DynamicLoader: GDI32.dll/D3DKMTGetDisplayModeList
- DynamicLoader: GDI32.dll/D3DKMTCloseAdapter
- DynamicLoader: WINTRUST.dll/WinVerifyTrust
- DynamicLoader: WINBRAND.dll/BrandingLoadString
- DynamicLoader: SECURITY.DLL/InitSecurityInterfaceW
- DynamicLoader: CRYPTSP.dll/SystemFunction035
- DynamicLoader: schannel.DLL/SpUserModeInitialize
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: ntdll.dll/RtlInitUnicodeString
- DynamicLoader: ntdll.dll/RtlFreeUnicodeString
- DynamicLoader: ntdll.dll/NtSetSystemEnvironmentValue
- DynamicLoader: ntdll.dll/NtQuerySystemEnvironmentValue
- DynamicLoader: ntdll.dll/NtCreateFile
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtQueryDirectoryObject
- DynamicLoader: ntdll.dll/NtQueryObject
- DynamicLoader: ntdll.dll/NtOpenDirectoryObject
- DynamicLoader: ntdll.dll/NtQueryInformationProcess
- DynamicLoader: ntdll.dll/NtQueryInformationToken
- DynamicLoader: ntdll.dll/NtOpenFile
- DynamicLoader: ntdll.dll/NtClose
- DynamicLoader: ntdll.dll/NtFsControlFile
- DynamicLoader: ntdll.dll/NtQueryVolumeInformationFile
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: NETAPI32.DLL/NetGroupEnum
- DynamicLoader: NETAPI32.DLL/NetGroupGetInfo
- DynamicLoader: NETAPI32.DLL/NetGroupSetInfo
- DynamicLoader: NETAPI32.DLL/NetLocalGroupGetInfo
- DynamicLoader: NETAPI32.DLL/NetLocalGroupSetInfo
- DynamicLoader: NETAPI32.DLL/NetGroupGetUsers
- DynamicLoader: NETAPI32.DLL/NetLocalGroupGetMembers
- DynamicLoader: NETAPI32.DLL/NetLocalGroupEnum
- DynamicLoader: NETAPI32.DLL/NetShareEnum
- DynamicLoader: NETAPI32.DLL/NetShareGetInfo
- DynamicLoader: NETAPI32.DLL/NetShareAdd
- DynamicLoader: NETAPI32.DLL/NetShareEnumSticky
- DynamicLoader: NETAPI32.DLL/NetShareSetInfo
- DynamicLoader: NETAPI32.DLL/NetShareDel
- DynamicLoader: NETAPI32.DLL/NetShareDelSticky
- DynamicLoader: NETAPI32.DLL/NetShareCheck
- DynamicLoader: NETAPI32.DLL/NetUserEnum
- DynamicLoader: NETAPI32.DLL/NetUserGetInfo
- DynamicLoader: NETAPI32.DLL/NetUserSetInfo
- DynamicLoader: NETAPI32.DLL/NetGroupEnum
- DynamicLoader: NETAPI32.DLL/NetApiBufferFree
- DynamicLoader: NETAPI32.DLL/NetQueryDisplayInformation
- DynamicLoader: NETAPI32.DLL/NetServerSetInfo
- DynamicLoader: NETAPI32.DLL/NetServerGetInfo
- DynamicLoader: NETAPI32.DLL/NetGetDCName
- DynamicLoader: NETAPI32.DLL/NetWkstaGetInfo
- DynamicLoader: NETAPI32.DLL/NetGetAnyDCName
- DynamicLoader: NETAPI32.DLL/NetServerEnum
- DynamicLoader: NETAPI32.DLL/NetUserModalsGet
- DynamicLoader: NETAPI32.DLL/NetScheduleJobAdd
- DynamicLoader: NETAPI32.DLL/NetScheduleJobDel
- DynamicLoader: NETAPI32.DLL/NetScheduleJobEnum
- DynamicLoader: NETAPI32.DLL/NetScheduleJobGetInfo
- DynamicLoader: NETAPI32.DLL/NetUseGetInfo
- DynamicLoader: NETAPI32.DLL/NetEnumerateTrustedDomains

- DynamicLoader: NETAPI32.DLL/DsGetDcNameW
- DynamicLoader: NETAPI32.DLL/DsRoleGetPrimaryDomainInformation
- DynamicLoader: NETAPI32.DLL/DsRoleFreeMemory
- DynamicLoader: NETAPI32.DLL/NetRenameMachineInDomain
- DynamicLoader: NETAPI32.DLL/NetJoinDomain
- DynamicLoader: NETAPI32.DLL/NetUnjoinDomain
- DynamicLoader: WKSCLI.DLL/NetWkstaGetInfo
- DynamicLoader: cscapi.dll/CscNetApiGetInterface
- DynamicLoader: kernel32.dll/GetDiskFreeSpaceExW
- DynamicLoader: kernel32.dll/GetVolumePathNameW
- DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
- DynamicLoader: kernel32.dll/Thread32First
- DynamicLoader: kernel32.dll/Thread32Next
- DynamicLoader: kernel32.dll/Process32First
- DynamicLoader: kernel32.dll/Process32Next
- DynamicLoader: kernel32.dll/Module32First
- DynamicLoader: kernel32.dll/Module32Next
- DynamicLoader: kernel32.dll/Heap32ListFirst
- DynamicLoader: kernel32.dll/GlobalMemoryStatusEx
- DynamicLoader: kernel32.dll/GetSystemDefaultUILanguage
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextW
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: SHLWAPI.dll/PathIsDirectoryW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegNotifyChangeKeyValue
- DynamicLoader: SspiCli.dll/GetUserNameExW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: ole32.dll/NdrOleInitializeExtension
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: ole32.dll/CLSIDFromOle1Class
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject2
- DynamicLoader: tschannel.dll/DllGetClassObject
- DynamicLoader: tschannel.dll/DllCanUnloadNow
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData

- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: SHLWAPI.dll/PathIsPrefixW
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: XmlLite.dll/CreateXmlReader
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextW
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: SHLWAPI.dll/PathIsDirectoryW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegNotifyChangeKeyValue
- DynamicLoader: SspiCli.dll/GetUserNameExW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: ole32.dll/NdrOleInitializeExtension
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: ole32.dll/CLSIDFromOle1Class
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject2
- DynamicLoader: tschannel.dll/DllGetClassObject
- DynamicLoader: tschannel.dll/DllCanUnloadNow
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: SHLWAPI.dll/PathIsPrefixW
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptHashData

- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: XmlLite.dll/CreateXmlReader
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: RPCRT4.dll/UuidFromStringW
- DynamicLoader: radarrs.dll/WdiDiagnosticModuleMain
- DynamicLoader: radarrs.dll/WdiHandleInstance
- DynamicLoader: radarrs.dll/WdiGetDiagnosticModuleInterfaceVersion
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: GDI32.dll/GetLayout
- DynamicLoader: GDI32.dll/GdiRealizationInfo
- DynamicLoader: GDI32.dll/FontIsLinked
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: GDI32.dll/GetTextFaceAliasW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: GDI32.dll/GetFontAssocStatus
- DynamicLoader: ADVAPI32.dll/RegQueryValueExA
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: GDI32.dll/GetTextFaceAliasW
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: wersvc.dll/ServiceMain
- DynamicLoader: wersvc.dll/SvchostPushServiceGlobals
- DynamicLoader: ADVAPI32.dll/RegGetValueW
- DynamicLoader: sechost.dll/ConvertStringSecurityDescriptorToSecurityDescriptorW
- DynamicLoader: faultrep.dll/WerpInitiateCrashReporting
- DynamicLoader: wer.dll/WerpCreateMachineStore
- DynamicLoader: SHELL32.dll/SHGetFolderPathEx
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: profapi.dll/
- DynamicLoader: USERENV.dll/CreateEnvironmentBlock
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: SspiCli.dll/GetUserNameExW
- DynamicLoader: faultrep.dll/WerpInitiateCrashReporting
- DynamicLoader: faultrep.dll/WerpInitiateCrashReporting
- DynamicLoader: USERENV.dll/DestroyEnvironmentBlock
- DynamicLoader: wer.dll/WerpSvcReportFromMachineQueue
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/DuplicateToken
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/CheckTokenMembership
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: WTSAPI32.dll/WTSQueryUserToken
- DynamicLoader: WINSTA.dll/WinStationQueryInformationW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ADVAPI32.dll/CreateWellKnownSid
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeW

- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcStringFreeW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: ADVAPI32.dll/ImpersonateLoggedOnUser
- DynamicLoader: ADVAPI32.dll/CreateProcessAsUserW
- DynamicLoader: ADVAPI32.dll/RevertToSelf
- DynamicLoader: faultrep.dll/WerpInitiateCrashReporting
- DynamicLoader: wer.dll/WerpCreateMachineStore
- DynamicLoader: USERENV.dll/CreateEnvironmentBlock
- DynamicLoader: USERENV.dll/DestroyEnvironmentBlock
- DynamicLoader: wer.dll/WerpSvcReportFromMachineQueue
- DynamicLoader: IMM32.dll/ImmDisableIME
- DynamicLoader: psapi.dll/GetModuleFileNameExW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: wer.dll/WerpCreateIntegratorReportId
- DynamicLoader: kernel32.dll/FlsAlloc
- DynamicLoader: kernel32.dll/FlsFree
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: kernel32.dll/FlsSetValue
- DynamicLoader: kernel32.dll/InitializeCriticalSectionEx
- DynamicLoader: kernel32.dll/CreateEventExW
- DynamicLoader: kernel32.dll/CreateSemaphoreExW
- DynamicLoader: kernel32.dll/SetThreadStackGuarantee
- DynamicLoader: kernel32.dll/CreateThreadpoolTimer
- DynamicLoader: kernel32.dll/SetThreadpoolTimer
- DynamicLoader: kernel32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: kernel32.dll/CloseThreadpoolTimer
- DynamicLoader: kernel32.dll/CreateThreadpoolWait
- DynamicLoader: kernel32.dll/SetThreadpoolWait
- DynamicLoader: kernel32.dll/CloseThreadpoolWait
- DynamicLoader: kernel32.dll/FlushProcessWriteBuffers
- DynamicLoader: kernel32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: kernel32.dll/GetCurrentProcessorNumber
- DynamicLoader: kernel32.dll/GetLogicalProcessorInformation
- DynamicLoader: kernel32.dll/CreateSymbolicLinkW
- DynamicLoader: kernel32.dll/SetDefaultDllDirectories
- DynamicLoader: kernel32.dll/EnumSystemLocalesEx
- DynamicLoader: kernel32.dll/CompareStringEx
- DynamicLoader: kernel32.dll/GetDateFormatEx
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/GetTimeFormatEx
- DynamicLoader: kernel32.dll/GetUserDefaultLocaleName
- DynamicLoader: kernel32.dll/IsValidLocaleName
- DynamicLoader: kernel32.dll/LCMapStringEx
- DynamicLoader: kernel32.dll/GetCurrentPackageId
- DynamicLoader: kernel32.dll/GetTickCount64
- DynamicLoader: kernel32.dll/GetFileInformationByHandleExW
- DynamicLoader: kernel32.dll/SetFileInformationByHandleW
- DynamicLoader: mscordacwks.dll/OutOfProcessExceptionEventCallback
- DynamicLoader: kernel32.dll/GetProcessIdOfThread
- DynamicLoader: kernel32.dll/GetThreadId
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: wer.dll/WerReportCreate
- DynamicLoader: ADVAPI32.dll/OpenProcessToken

- DynamicLoader: wer.dll/WerpSetIntegratorReportId
- DynamicLoader: wer.dll/WerReportSetParameter
- DynamicLoader: dbgeng.dll/DebugCreate
- DynamicLoader: ntdll.dll/CsrGetProcessId
- DynamicLoader: ntdll.dll/DbgBreakPoint
- DynamicLoader: ntdll.dll/DbgPrint
- DynamicLoader: ntdll.dll/DbgPrompt
- DynamicLoader: ntdll.dll/DbgUiConvertStateChangeStructure
- DynamicLoader: ntdll.dll/DbgUiGetThreadDebugObject
- DynamicLoader: ntdll.dll/DbgUiIssueRemoteBreakin
- DynamicLoader: ntdll.dll/DbgUiSetThreadDebugObject
- DynamicLoader: ntdll.dll/NtAllocateVirtualMemory
- DynamicLoader: ntdll.dll/NtClose
- DynamicLoader: ntdll.dll/NtCreateDebugObject
- DynamicLoader: ntdll.dll/NtCreateFile
- DynamicLoader: ntdll.dll/NtDebugActiveProcess
- DynamicLoader: ntdll.dll/NtDebugContinue
- DynamicLoader: ntdll.dll/NtFreeVirtualMemory
- DynamicLoader: ntdll.dll/NtOpenProcess
- DynamicLoader: ntdll.dll/NtOpenThread
- DynamicLoader: ntdll.dll/NtQueryInformationProcess
- DynamicLoader: ntdll.dll/NtQueryInformationThread
- DynamicLoader: ntdll.dll/NtQueryMutant
- DynamicLoader: ntdll.dll/NtQueryObject
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtRemoveProcessDebug
- DynamicLoader: ntdll.dll/NtResumeThread
- DynamicLoader: ntdll.dll/NtSetInformationDebugObject
- DynamicLoader: ntdll.dll/NtSetInformationProcess
- DynamicLoader: ntdll.dll/NtSystemDebugControl
- DynamicLoader: ntdll.dll/NtWaitForDebugEvent
- DynamicLoader: ntdll.dll/RtlAnsiStringToUnicodeString
- DynamicLoader: ntdll.dll/RtlCreateProcessParameters
- DynamicLoader: ntdll.dll/RtlCreateUserProcess
- DynamicLoader: ntdll.dll/RtlDestroyProcessParameters
- DynamicLoader: ntdll.dll/RtlDosPathNameToNtPathName_U
- DynamicLoader: ntdll.dll/RtlFindMessage
- DynamicLoader: ntdll.dll/RtlFreeHeap
- DynamicLoader: ntdll.dll/RtlFreeUnicodeString
- DynamicLoader: ntdll.dll/RtlGetFunctionTableListHead
- DynamicLoader: ntdll.dll/RtlGetUnloadEventTrace
- DynamicLoader: ntdll.dll/RtlGetUnloadEventTraceEx
- DynamicLoader: ntdll.dll/RtlInitAnsiString
- DynamicLoader: ntdll.dll/RtlInitUnicodeString
- DynamicLoader: ntdll.dll/RtlTryEnterCriticalSection
- DynamicLoader: ntdll.dll/RtlUnicodeStringToAnsiString
- DynamicLoader: ntdll.dll/NtOpenProcessToken
- DynamicLoader: ntdll.dll/NtOpenThreadToken
- DynamicLoader: ntdll.dll/NtQueryInformationToken
- DynamicLoader: kernel32.dll/CloseProfileUserMapping
- DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
- DynamicLoader: kernel32.dll/DebugActiveProcessStop
- DynamicLoader: kernel32.dll/DebugBreak
- DynamicLoader: kernel32.dll/DebugBreakProcess
- DynamicLoader: kernel32.dll/DebugSetProcessKillOnExit
- DynamicLoader: kernel32.dll/Module32First
- DynamicLoader: kernel32.dll/Module32FirstW
- DynamicLoader: kernel32.dll/Module32Next
- DynamicLoader: kernel32.dll/Module32NextW
- DynamicLoader: kernel32.dll/OpenThread
- DynamicLoader: kernel32.dll/Process32First
- DynamicLoader: kernel32.dll/Process32FirstW
- DynamicLoader: kernel32.dll/Process32Next

- DynamicLoader: kernel32.dll/Process32NextW
- DynamicLoader: kernel32.dll/ProcessIdToSessionId
- DynamicLoader: kernel32.dll/SetProcessShutdownParameters
- DynamicLoader: kernel32.dll/Thread32First
- DynamicLoader: kernel32.dll/Thread32Next
- DynamicLoader: kernel32.dll/GetTimeZoneInformation
- DynamicLoader: kernel32.dll/DuplicateHandle
- DynamicLoader: kernel32.dll/Wow64GetThreadSelectorEntry
- DynamicLoader: ADVAPI32.dll/CloseServiceHandle
- DynamicLoader: ADVAPI32.dll/ControlService
- DynamicLoader: ADVAPI32.dll/CreateServiceA
- DynamicLoader: ADVAPI32.dll/CreateServiceW
- DynamicLoader: ADVAPI32.dll/DeleteService
- DynamicLoader: ADVAPI32.dll/EnumServicesStatusExA
- DynamicLoader: ADVAPI32.dll/EnumServicesStatusExW
- DynamicLoader: ADVAPI32.dll/GetEventLogInformation
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenSCManagerA
- DynamicLoader: ADVAPI32.dll/OpenSCManagerW
- DynamicLoader: ADVAPI32.dll/OpenServiceA
- DynamicLoader: ADVAPI32.dll/OpenServiceW
- DynamicLoader: ADVAPI32.dll/StartServiceA
- DynamicLoader: ADVAPI32.dll/StartServiceW
- DynamicLoader: ADVAPI32.dll/GetSidSubAuthority
- DynamicLoader: ADVAPI32.dll/GetSidSubAuthorityCount
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeExW
- DynamicLoader: VERSION.dll/GetFileVersionInfoExW
- DynamicLoader: dbghelp.dll/DebugExtensionInitialize
- DynamicLoader: dbghelp.dll/WinDbgExtensionDllInit
- DynamicLoader: dbghelp.dll/ExtensionApiVersion
- DynamicLoader: dbghelp.dll/CheckVersion
- DynamicLoader: wer.dll/WerpSetDynamicParameter
- DynamicLoader: wer.dll/WerReportAddDump
- DynamicLoader: wer.dll/WerpSetCallBack
- DynamicLoader: wer.dll/WerReportSetUIOption
- DynamicLoader: wer.dll/WerpAddRegisteredDataToReport
- DynamicLoader: wer.dll/WerReportSubmit
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegGetValueW
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/CheckTokenMembership
- DynamicLoader: USER32.dll/GetProcessWindowStation
- DynamicLoader: USER32.dll/GetThreadDesktop
- DynamicLoader: USER32.dll/GetUserObjectInformationW
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: SensApi.dll/IsNetworkAlive
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/CharUpperW
- DynamicLoader: werui.dll/WerUICreate
- DynamicLoader: werui.dll/WerUIStart
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: DUI70.dll/InitProcessPriv

- DynamicLoader: COMCTL32.dll/LoadIconWithScaleDown
- DynamicLoader: ntdll.dll/RtlRunEncodeUnicodeString
- DynamicLoader: ntdll.dll/RtlInitUnicodeString
- DynamicLoader: ntdll.dll/RtlRunDecodeUnicodeString
- DynamicLoader: DUI70.dll/InitThread
- DynamicLoader: DUser.dll/InitGadgets
- DynamicLoader: USER32.dll/RegisterMessagePumpHook
- DynamicLoader: DUI70.dll/?GetClassInfoPtr@CCBase@DirectUI@@SAPEAUIClassInfo@2@XZ
- DynamicLoader: DUI70.dll/?GetFactoryLock@Element@DirectUI@@SAPEAU_RTL_CRITICAL_SECTION@@XZ
- DynamicLoader: DUI70.dll/??0CritSecLock@DirectUI@@QEAA@PEAU_RTL_CRITICAL_SECTION@@@Z
- DynamicLoader: DUI70.dll/?ClassExist@ClassInfoBase@DirectUI@@SA_NPEAPEAUIClassInfo@2@PEBQEBUPropertyInfo@2@IPEAU32@PEAUHINSTANCE__@@PEBG_N@Z
- DynamicLoader: DUI70.dll/??0ClassInfoBase@DirectUI@@QEAA@XZ
- DynamicLoader: DUI70.dll/?Initialize@ClassInfoBase@DirectUI@@QEAAJPEAUHINSTANCE__@@PEBG_NPEBQEBUPropertyInfo@2@I@Z
- DynamicLoader: DUI70.dll/?Register@ClassInfoBase@DirectUI@@QEAAJXZ
- DynamicLoader: DUI70.dll/?IsGlobal@ClassInfoBase@DirectUI@@UEBA_NXZ
- DynamicLoader: DUI70.dll/?GetName@ClassInfoBase@DirectUI@@UEBAPEBGXZ
- DynamicLoader: DUI70.dll/?GetModule@ClassInfoBase@DirectUI@@UEBAPEAUHINSTANCE__@@XZ
- DynamicLoader: DUI70.dll/??1CritSecLock@DirectUI@@QEAA@XZ
- DynamicLoader: DUI70.dll/??0CCBase@DirectUI@@QEAA@KPEBG@Z
- DynamicLoader: DUI70.dll/?Initialize@CCBase@DirectUI@@QEAAJIPEAVElement@2@PEAK@Z
- DynamicLoader: DUser.dll/CreateGadget
- DynamicLoader: DUser.dll/SetGadgetMessageFilter
- DynamicLoader: DUser.dll/SetGadgetStyle
- DynamicLoader: DUI70.dll/?OnPropertyChanging@Element@DirectUI@@UEAA_NPEBUPropertyInfo@2@HPEAVValue@2@1@Z
- DynamicLoader: DUI70.dll/?HandleUiaPropertyChangingListener@Element@DirectUI@@UEAAXPEBUPropertyInfo@2@@Z
- DynamicLoader: DUI70.dll/?HandleUiaPropertyListener@Element@DirectUI@@UEAAXPEBUPropertyInfo@2@HPEAVValue@2@1@Z
- DynamicLoader: DUI70.dll/?DirectionProp@Element@DirectUI@@SAPEBUPropertyInfo@2@XZ
- DynamicLoader: DUI70.dll/?OnPropertyChanged@CCBase@DirectUI@@UEAAXPEBUPropertyInfo@2@HPEAVValue@2@1@Z
- DynamicLoader: DUI70.dll/?SetFontSize@Element@DirectUI@@QEAAJH@Z
- DynamicLoader: DUI70.dll/?SetWidth@Element@DirectUI@@QEAAJH@Z
- DynamicLoader: DUI70.dll/?SetHeight@Element@DirectUI@@QEAAJH@Z
- DynamicLoader: DUI70.dll/?EndDefer@Element@DirectUI@@QEAAXK@Z
- DynamicLoader: DUI70.dll/?OnGroupChanged@Element@DirectUI@@UEAAXH_N@Z
- DynamicLoader: DUser.dll/InvalidateGadget
- DynamicLoader: DUI70.dll/CreateDUIWrapper
- DynamicLoader: SHELL32.dll/ExtractIconExW
- DynamicLoader: COMCTL32.dll/TaskDialogIndirect
- DynamicLoader: COMCTL32.dll/LoadIconWithScaleDown
- DynamicLoader: ntdll.dll/RtlRunEncodeUnicodeString
- DynamicLoader: ntdll.dll/RtlInitUnicodeString
- DynamicLoader: ntdll.dll/RtlRunDecodeUnicodeString
- DynamicLoader: DUser.dll/InitGadgets
- DynamicLoader: uxtheme.dll/IsThemeActive
- DynamicLoader: DUser.dll/CreateGadget
- DynamicLoader: DUser.dll/SetGadgetMessageFilter
- DynamicLoader: DUser.dll/SetGadgetStyle
- DynamicLoader: DUser.dll/SetGadgetRootInfo

- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: uxtheme.dll/IsAppThemed
- DynamicLoader: ole32.dll/CreateStreamOnHGlobal
- DynamicLoader: xmllite.dll/CreateXmlReader
- DynamicLoader: xmllite.dll/CreateXmlReaderInputWithEncodingName
- DynamicLoader: DUser.dll/FindStdColor
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: DUser.dll/SetGadgetParent
- DynamicLoader: DUser.dll/GetDUserModule
- DynamicLoader: xmllite.dll/CreateXmlReader
- DynamicLoader: xmllite.dll/CreateXmlReaderInputWithEncodingName
- DynamicLoader: DUser.dll/AttachWndProcW
- DynamicLoader: COMCTL32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/OpenThemeData
- DynamicLoader: DUser.dll/GetGadgetRect
- DynamicLoader: DUser.dll/GetGadgetRgn
- DynamicLoader: DUser.dll/GetGadgetTicket
- DynamicLoader: COMCTL32.dll/RegisterClassNameW
- DynamicLoader: DUser.dll/SetGadgetRootInfo
- DynamicLoader: DUI70.dll/?GetPICount@ClassInfoBase@DirectUI@@UEBAIXZ
- DynamicLoader: DUI70.dll/?GetByClassIndex@ClassInfoBase@DirectUI@@UEAAPEBUPropertyInfo@2@I@Z
- DynamicLoader: DUser.dll/SetGadgetParent
- DynamicLoader: DUI70.dll/?OnHosted@HWNDHost@DirectUI@@MEAAXPEAVElement@2@@Z
- DynamicLoader: DUser.dll/AttachWndProcW
- DynamicLoader: DUI70.dll/?CreateAccNameLabel@HWNDHost@DirectUI@@IEAAPEAUHWND__@@PEAU3@@Z
- DynamicLoader: COMCTL32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/EnableThemeDialogTexture
- DynamicLoader: DUI70.dll/?OnMessage@HWNDHost@DirectUI@@UEAA_NI_K_JPEA_J@Z
- DynamicLoader: DUI70.dll/?CreateHWND@CCBase@DirectUI@@UEAAPEAUHWND__@@PEAU3@@Z
- DynamicLoader: DUI70.dll/?PostCreate@CCBase@DirectUI@@MEAAXPEAUHWND__@@@Z
- DynamicLoader: DUser.dll/GetGadgetRect
- DynamicLoader: DUser.dll/GetGadgetRgn
- DynamicLoader: DUI70.dll/?IsContentProtected@Element@DirectUI@@UEAA_NXZ
- DynamicLoader: COMCTL32.dll/RegisterClassNameW
- DynamicLoader: DUser.dll/InvalidateGadget
- DynamicLoader: DUser.dll/GetGadgetFocus
- DynamicLoader: GDI32.dll/GetLayout
- DynamicLoader: GDI32.dll/GdiRealizationInfo
- DynamicLoader: GDI32.dll/FontIsLinked
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: GDI32.dll/GetTextFaceAliasW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: GDI32.dll/GetFontAssocStatus
- DynamicLoader: ADVAPI32.dll/RegQueryValueExA
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: GDI32.dll/GetTextFaceAliasW
- DynamicLoader: DUser.dll/SetGadgetFocus
- DynamicLoader: DUser.dll/DUserSendEvent
- DynamicLoader: DUser.dll/SetGadgetRect
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: COMCTL32.dll/SetWindowSubclass
- DynamicLoader: COMCTL32.dll/DefSubclassProc
- DynamicLoader: DUI70.dll/?GetHWND@HWNDHost@DirectUI@@UEAAPEAUHWND__@@XZ
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: uxtheme.dll/BufferedPaintInit

- DynamicLoader: uxtheme.dll/BeginBufferedPaint
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: uxtheme.dll/GetBufferedPaintDC
- DynamicLoader: uxtheme.dll/GetBufferedPaintTargetDC
- DynamicLoader: uxtheme.dll/EndBufferedPaint
- DynamicLoader: DUser.dll/ForwardGadgetMessage
- DynamicLoader: COMCTL32.dll/RegisterClassNameW
- DynamicLoader: xmllite.dll/CreateXmlReader
- DynamicLoader: xmllite.dll/CreateXmlReaderInputWithEncodingName
- DynamicLoader: xmllite.dll/CreateXmlReader
- DynamicLoader: xmllite.dll/CreateXmlReaderInputWithEncodingName
- DynamicLoader: COMCTL32.dll/RegisterClassNameW
- DynamicLoader: DUser.dll/DUserPostEvent
- DynamicLoader: DUser.dll/DisableContainerHwnd
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: uxtheme.dll/BufferedPaintUnInit
- DynamicLoader: werui.dll/WerUIUpdateUIForState
- DynamicLoader: DUser.dll/DeleteHandle
- DynamicLoader: DUser.dll/DetachWndProc
- DynamicLoader: COMCTL32.dll/RemoveWindowSubclass
- DynamicLoader: DUI70.dll/?OnUnHosted@HWNDHost@DirectUI@@MEAAXPEAVElement@2@@Z
- DynamicLoader: DUser.dll/DisableContainerHwnd
- DynamicLoader: DUI70.dll/?MessageCallback@HWNDHost@DirectUI@@UEAAIPEAUtagGMSG@@@Z
- DynamicLoader: DUI70.dll/?HandleUiaDestroyListener@Element@DirectUI@@UEAAXXZ
- DynamicLoader: DUI70.dll/?OnDestroy@HWNDHost@DirectUI@@UEAAXXZ
- DynamicLoader: DUI70.dll/??1CCBase@DirectUI@@UEAA@XZ
- DynamicLoader: USER32.dll/MsgWaitForMultipleObjects
- DynamicLoader: WINHTTP.dll/WinHttpOpen
- DynamicLoader: WINHTTP.dll/WinHttpSetTimeouts
- DynamicLoader: WINHTTP.dll/WinHttpSetOption
- DynamicLoader: WINHTTP.dll/WinHttpConnect
- DynamicLoader: WINHTTP.dll/WinHttpOpenRequest
- DynamicLoader: WINHTTP.dll/WinHttpSetStatusCallback
- DynamicLoader: WINHTTP.dll/WinHttpGetDefaultProxyConfiguration
- DynamicLoader: WINHTTP.dll/WinHttpGetIEProxyConfigForCurrentUser
- DynamicLoader: WINHTTP.dll/WinHttpGetProxyForUrl
- DynamicLoader: WINHTTP.dll/WinHttpSendRequest
- DynamicLoader: WS2_32.dll/GetAddrInfoW
- DynamicLoader: WS2_32.dll/WSASocketW
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/WSAIoctl
- DynamicLoader: WS2_32.dll/FreeAddrInfoW
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/WSARecv
- DynamicLoader: WS2_32.dll/WSASend
- DynamicLoader: WINHTTP.dll/WinHttpReceiveResponse
- DynamicLoader: WINHTTP.dll/WinHttpQueryHeaders
- DynamicLoader: WINHTTP.dll/WinHttpReadData
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WINHTTP.dll/WinHttpCloseHandle
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/IsValidSid
- DynamicLoader: ADVAPI32.dll/GetLengthSid
- DynamicLoader: ADVAPI32.dll/CopySid
- DynamicLoader: SHELL32.dll/SHGetFolderPathW
- DynamicLoader: WS2_32.dll/
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW

- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/RegisterEventSourceW
- DynamicLoader: ADVAPI32.dll/ReportEventW
- DynamicLoader: ADVAPI32.dll/DeregisterEventSource
- DynamicLoader: werui.dll/WerUITerminate
- DynamicLoader: werui.dll/WerUIDelete
- DynamicLoader: DUser.dll/DUserFlushMessages
- DynamicLoader: DUser.dll/DUserFlushDeferredMessages
- DynamicLoader: DUI70.dll/UnInitThread
- DynamicLoader: DUser.dll/DUserFlushMessages
- DynamicLoader: DUser.dll/DUserFlushDeferredMessages
- DynamicLoader: DUser.dll/DeleteHandle
- DynamicLoader: USER32.dll/UnregisterMessagePumpHook
- DynamicLoader: DUI70.dll/UnInitProcessPriv
- DynamicLoader: DUI70.dll/?Release@ClassInfoBase@DirectUI@@UEAAHXZ
- DynamicLoader: DUI70.dll/?GetGlobalIndex@ClassInfoBase@DirectUI@@UEBAIXZ
- DynamicLoader: DUI70.dll/??1ClassInfoBase@DirectUI@@UEAA@XZ
- DynamicLoader: SHLWAPI.dll/PathIsDirectoryW
- DynamicLoader: wer.dll/WerReportCloseHandle
- DynamicLoader: ADVAPI32.dll/DuplicateToken
- DynamicLoader: wer.dll/WerpFreeString
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: IMM32.dll/ImmDisableIME
- DynamicLoader: psapi.dll/GetModuleFileNameExW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: ADVAPI32.dll/I_QueryTagInformation
- DynamicLoader: wer.dll/WerpCreateIntegratorReportId
- DynamicLoader: wer.dll/WerReportCreate
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: wer.dll/WerpSetIntegratorReportId
- DynamicLoader: wer.dll/WerReportSetParameter
- DynamicLoader: dbgeng.dll/DebugCreate
- DynamicLoader: ntdll.dll/CsrGetProcessId
- DynamicLoader: ntdll.dll/DbgBreakPoint
- DynamicLoader: ntdll.dll/DbgPrint
- DynamicLoader: ntdll.dll/DbgPrompt
- DynamicLoader: ntdll.dll/DbgUiConvertStateChangeStructure
- DynamicLoader: ntdll.dll/DbgUiGetThreadDebugObject
- DynamicLoader: ntdll.dll/DbgUiIssueRemoteBreakin
- DynamicLoader: ntdll.dll/DbgUiSetThreadDebugObject
- DynamicLoader: ntdll.dll/NtAllocateVirtualMemory
- DynamicLoader: ntdll.dll/NtClose
- DynamicLoader: ntdll.dll/NtCreateDebugObject
- DynamicLoader: ntdll.dll/NtCreateFile
- DynamicLoader: ntdll.dll/NtDebugActiveProcess
- DynamicLoader: ntdll.dll/NtDebugContinue
- DynamicLoader: ntdll.dll/NtFreeVirtualMemory
- DynamicLoader: ntdll.dll/NtOpenProcess
- DynamicLoader: ntdll.dll/NtOpenThread
- DynamicLoader: ntdll.dll/NtQueryInformationProcess
- DynamicLoader: ntdll.dll/NtQueryInformationThread
- DynamicLoader: ntdll.dll/NtQueryMutant
- DynamicLoader: ntdll.dll/NtQueryObject
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtRemoveProcessDebug

- DynamicLoader: ntdll.dll/NtResumeThread
- DynamicLoader: ntdll.dll/NtSetInformationDebugObject
- DynamicLoader: ntdll.dll/NtSetInformationProcess
- DynamicLoader: ntdll.dll/NtSystemDebugControl
- DynamicLoader: ntdll.dll/NtWaitForDebugEvent
- DynamicLoader: ntdll.dll/RtlAnsiStringToUnicodeString
- DynamicLoader: ntdll.dll/RtlCreateProcessParameters
- DynamicLoader: ntdll.dll/RtlCreateUserProcess
- DynamicLoader: ntdll.dll/RtlDestroyProcessParameters
- DynamicLoader: ntdll.dll/RtlDosPathNameToNtPathName_U
- DynamicLoader: ntdll.dll/RtlFindMessage
- DynamicLoader: ntdll.dll/RtlFreeHeap
- DynamicLoader: ntdll.dll/RtlFreeUnicodeString
- DynamicLoader: ntdll.dll/RtlGetFunctionTableListHead
- DynamicLoader: ntdll.dll/RtlGetUnloadEventTrace
- DynamicLoader: ntdll.dll/RtlGetUnloadEventTraceEx
- DynamicLoader: ntdll.dll/RtlInitAnsiString
- DynamicLoader: ntdll.dll/RtlInitUnicodeString
- DynamicLoader: ntdll.dll/RtlTryEnterCriticalSection
- DynamicLoader: ntdll.dll/RtlUnicodeStringToAnsiString
- DynamicLoader: ntdll.dll/NtOpenProcessToken
- DynamicLoader: ntdll.dll/NtOpenThreadToken
- DynamicLoader: ntdll.dll/NtQueryInformationToken
- DynamicLoader: kernel32.dll/CloseProfileUserMapping
- DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
- DynamicLoader: kernel32.dll/DebugActiveProcessStop
- DynamicLoader: kernel32.dll/DebugBreak
- DynamicLoader: kernel32.dll/DebugBreakProcess
- DynamicLoader: kernel32.dll/DebugSetProcessKillOnExit
- DynamicLoader: kernel32.dll/Module32First
- DynamicLoader: kernel32.dll/Module32FirstW
- DynamicLoader: kernel32.dll/Module32Next
- DynamicLoader: kernel32.dll/Module32NextW
- DynamicLoader: kernel32.dll/OpenThread
- DynamicLoader: kernel32.dll/Process32First
- DynamicLoader: kernel32.dll/Process32FirstW
- DynamicLoader: kernel32.dll/Process32Next
- DynamicLoader: kernel32.dll/Process32NextW
- DynamicLoader: kernel32.dll/ProcessIdToSessionId
- DynamicLoader: kernel32.dll/SetProcessShutdownParameters
- DynamicLoader: kernel32.dll/Thread32First
- DynamicLoader: kernel32.dll/Thread32Next
- DynamicLoader: kernel32.dll/GetTimeZoneInformation
- DynamicLoader: kernel32.dll/DuplicateHandle
- DynamicLoader: kernel32.dll/Wow64GetThreadSelectorEntry
- DynamicLoader: ADVAPI32.dll/CloseServiceHandle
- DynamicLoader: ADVAPI32.dll/ControlService
- DynamicLoader: ADVAPI32.dll/CreateServiceA
- DynamicLoader: ADVAPI32.dll/CreateServiceW
- DynamicLoader: ADVAPI32.dll/DeleteService
- DynamicLoader: ADVAPI32.dll/EnumServicesStatusExA
- DynamicLoader: ADVAPI32.dll/EnumServicesStatusExW
- DynamicLoader: ADVAPI32.dll/GetEventLogInformation
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenSCManagerA
- DynamicLoader: ADVAPI32.dll/OpenSCManagerW
- DynamicLoader: ADVAPI32.dll/OpenServiceA
- DynamicLoader: ADVAPI32.dll/OpenServiceW
- DynamicLoader: ADVAPI32.dll/StartServiceA
- DynamicLoader: ADVAPI32.dll/StartServiceW
- DynamicLoader: ADVAPI32.dll/GetSidSubAuthority

- DynamicLoader: ADVAPI32.dll/GetSidSubAuthorityCount
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeExW
- DynamicLoader: VERSION.dll/GetFileVersionInfoExW
- DynamicLoader: wer.dll/WerReportAddDump
- DynamicLoader: wer.dll/WerpSetCallBack
- DynamicLoader: wer.dll/WerReportSetUIOption
- DynamicLoader: wer.dll/WerpAddRegisteredDataToReport
- DynamicLoader: wer.dll/WerReportSubmit
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegGetValueW
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/CheckTokenMembership
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: USER32.dll/GetProcessWindowStation
- DynamicLoader: USER32.dll/GetThreadDesktop
- DynamicLoader: USER32.dll/GetUserObjectInformationW
- DynamicLoader: SensApi.dll/IsNetworkAlive
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/CharUpperW
- DynamicLoader: wer.dll/WerpAddAppCompatData
- DynamicLoader: apphelp.dll/SdbGetFileAttributes
- DynamicLoader: apphelp.dll/SdbFormatAttribute
- DynamicLoader: apphelp.dll/SdbFreeFileAttributes
- DynamicLoader: apphelp.dll/SdbGetFileAttributes
- DynamicLoader: apphelp.dll/SdbFormatAttribute
- DynamicLoader: apphelp.dll/SdbFreeFileAttributes
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: SHELL32.dll/SHGetFolderPathEx
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: profapi.dll/
- DynamicLoader: ADVAPI32.dll/QueryTraceW
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/IsValidSid
- DynamicLoader: ADVAPI32.dll/GetLengthSid
- DynamicLoader: ADVAPI32.dll/CopySid
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAceEx
- DynamicLoader: ADVAPI32.dll/InitializeSecurityDescriptor
- DynamicLoader: ADVAPI32.dll/SetSecurityDescriptorDacl
- DynamicLoader: ADVAPI32.dll/RegisterEventSourceW
- DynamicLoader: ADVAPI32.dll/ReportEventW
- DynamicLoader: ADVAPI32.dll/DeregisterEventSource
- DynamicLoader: SHLWAPI.dll/PathIsDirectoryW
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: wer.dll/WerpGetStoreLocation
- DynamicLoader: wer.dll/WerpGetStoreType
- DynamicLoader: wer.dll/WerReportCloseHandle
- DynamicLoader: USER32.dll/MsgWaitForMultipleObjects
- DynamicLoader: ADVAPI32.dll/DuplicateToken
- DynamicLoader: wer.dll/WerpFreeString
- DynamicLoader: RPCRT4.dll/RpcBindingFree

- DynamicLoader: IMM32.dll/ImmDisableIME
- DynamicLoader: psapi.dll/GetModuleFileNameExW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: ADVAPI32.dll/I_QueryTagInformation
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ole32.dll/CoInitializeSecurity
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: fntcache.dll/ServiceMain
- DynamicLoader: fntcache.dll/SvchostPushServiceGlobals
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: Secur32.dll/SecpTranslateNameEx
- DynamicLoader: RPCRT4.dll/I_RpcMapWin32Status
- DynamicLoader: logoncli.dll/DsGetDcNameW
- DynamicLoader: ADVAPI32.dll/LsaOpenPolicy
- DynamicLoader: ADVAPI32.dll/LsaQueryInformationPolicy
- DynamicLoader: netutils.dll/NetApiBufferAllocate
- DynamicLoader: ADVAPI32.dll/LsaFreeMemory
- DynamicLoader: ADVAPI32.dll/LsaClose
- DynamicLoader: WS2_32.dll/
- DynamicLoader: netutils.dll/NetpIsDomainNameValid
- DynamicLoader: WLDAP32.dll/
- DynamicLoader: netutils.dll/NetApiBufferFree
- DynamicLoader: WS2_32.dll/
- DynamicLoader: RPCRT4.dll/I_RpcMapWin32Status
- DynamicLoader: netutils.dll/NetpwNameCompare
- DynamicLoader: RPCRT4.dll/RpcAsyncCompleteCall
- DynamicLoader: ADVAPI32.dll/RegGetValueW
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: SHELL32.dll/SHGetFolderPathEx
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: profapi.dll/
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/CheckTokenMembership
- DynamicLoader: USER32.dll/GetProcessWindowStation
- DynamicLoader: USER32.dll/GetThreadDesktop
- DynamicLoader: USER32.dll/GetUserObjectInformationW
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: SensApi.dll/IsNetworkAlive
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/CharUpperW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: werui.dll/WerUICreate

- DynamicLoader: werui.dll/WerUIStart
- DynamicLoader: ADVAPI32.dll/RegisterEventSourceW
- DynamicLoader: ADVAPI32.dll/ReportEventW
- DynamicLoader: ADVAPI32.dll/DeregisterEventSource
- DynamicLoader: werui.dll/WerUITerminate
- DynamicLoader: werui.dll/WerUIDelete
- DynamicLoader: SHLWAPI.dll/PathIsDirectoryW
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: USER32.dll/MsgWaitForMultipleObjects
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ole32.dll/CoInitializeSecurity
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: qmgr.dll/ServiceMain
- DynamicLoader: qmgr.dll/SvchostPushServiceGlobals
- DynamicLoader: aelupsvc.dll/ServiceMain
- DynamicLoader: aelupsvc.dll/SvchostPushServiceGlobals
- DynamicLoader: srvsvc.dll/ServiceMain
- DynamicLoader: srvsvc.dll/SvchostPushServiceGlobals
- DynamicLoader: ADVAPI32.dll/SetEntriesInAclW
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: themeservice.dll/ThemeServiceMain
- DynamicLoader: themeservice.dll/SvchostPushServiceGlobals
- DynamicLoader: sechost.dll/ConvertStringSecurityDescriptorToSecurityDescriptorW
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: schedsvc.dll/ServiceMain
- DynamicLoader: schedsvc.dll/SvchostPushServiceGlobals
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: shsvcs.dll/HardwareDetectionServiceMain
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/LsaOpenPolicy
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/WSASocketW
- DynamicLoader: WS2_32.dll/WSAIoctl
- DynamicLoader: WS2_32.dll/
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: ADVAPI32.dll/LsaQueryInformationPolicy
- DynamicLoader: RPCRT4.dll/RpcBindingCreateW
- DynamicLoader: RPCRT4.dll/RpcBindingBind
- DynamicLoader: sechost.dll/ConvertStringSecurityDescriptorToSecurityDescriptorW
- DynamicLoader: shsvcs.dll/SvchostPushServiceGlobals
- DynamicLoader: RPCRT4.dll/I_RpcMapWin32Status
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: netutils.dll/NetApiBufferAllocate
- DynamicLoader: ADVAPI32.dll/LsaFreeMemory
- DynamicLoader: ADVAPI32.dll/LsaClose
- DynamicLoader: netutils.dll/NetApiBufferFree
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: WINSTA.dll/WinStationOpenServerW

- DynamicLoader: WINSTA.dll/WinStationEnumerateW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: ADVAPI32.dll/CreateWellKnownSid
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeW
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcStringFreeW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: bitsigd.dll/InitializeEx
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: RPCRT4.dll/I_RpcExceptionFilter
- DynamicLoader: SSCORE.DLL/SsCoreInitialize
- DynamicLoader: SSCORE.DLL/SsCoreUninitialize
- DynamicLoader: SSCORE.DLL/SsCoreShareAdd
- DynamicLoader: SSCORE.DLL/SsCoreShareSetInfo
- DynamicLoader: SSCORE.DLL/SsCoreShareDel
- DynamicLoader: SSCORE.DLL/SsCoreShareCleanup
- DynamicLoader: FirewallAPI.DLL/IcfChangeNotificationCreate
- DynamicLoader: FirewallAPI.DLL/IcfChangeNotificationDestroy
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: WINSTA.dll/WinStationFreeMemory
- DynamicLoader: WINSTA.dll/WinStationCloseServer
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: secur32.dll/InitSecurityInterfaceW
- DynamicLoader: CRYPTSP.dll/SystemFunction035
- DynamicLoader: CLUSAPI.DLL/OpenCluster
- DynamicLoader: CLUSAPI.DLL/CloseCluster
- DynamicLoader: CLUSAPI.DLL/OpenClusterGroup
- DynamicLoader: CLUSAPI.DLL/ClusterGroupOpenEnum
- DynamicLoader: CLUSAPI.DLL/ClusterGroupEnum
- DynamicLoader: CLUSAPI.DLL/ClusterGroupCloseEnum
- DynamicLoader: CLUSAPI.DLL/CloseClusterGroup
- DynamicLoader: CLUSAPI.DLL/CreateClusterResource
- DynamicLoader: CLUSAPI.DLL/OpenClusterResource
- DynamicLoader: CLUSAPI.DLL/OnlineClusterResource
- DynamicLoader: CLUSAPI.DLL/OfflineClusterResource
- DynamicLoader: CLUSAPI.DLL/AddClusterResourceDependency
- DynamicLoader: CLUSAPI.DLL/ClusterResourceControl
- DynamicLoader: CLUSAPI.DLL/GetClusterResourceState
- DynamicLoader: CLUSAPI.DLL/ClusterResourceOpenEnum
- DynamicLoader: CLUSAPI.DLL/ClusterResourceEnum
- DynamicLoader: CLUSAPI.DLL/ClusterResourceCloseEnum
- DynamicLoader: CLUSAPI.DLL/CloseClusterResource
- DynamicLoader: CLUSAPI.DLL/DeleteClusterResource
- DynamicLoader: CLUSAPI.DLL/CreateClusterNotifyPort
- DynamicLoader: CLUSAPI.DLL/RegisterClusterNotify
- DynamicLoader: CLUSAPI.DLL/GetClusterNotify
- DynamicLoader: CLUSAPI.DLL/CloseClusterNotifyPort
- DynamicLoader: CLUSAPI.DLL/ClusterRegCloseKey
- DynamicLoader: CLUSAPI.DLL/ClusterRegOpenKey
- DynamicLoader: CLUSAPI.DLL/GetClusterResourceKey
- DynamicLoader: RESUTILS.DLL/ResUtilFindSzProperty
- DynamicLoader: RESUTILS.DLL/ResUtilFindDwordProperty
- DynamicLoader: RESUTILS.DLL/ResUtilEnumResourcesEx
- DynamicLoader: RESUTILS.DLL/ResUtilPropertyListFromParameterBlock
- DynamicLoader: RESUTILS.DLL/ResUtilGetResourceName
- DynamicLoader: RESUTILS.DLL/ResUtilResourceTypesEqual
- DynamicLoader: RESUTILS.DLL/ResUtilGetResourceDependency

- DynamicLoader: RESUTILS.DLL/ResUtilFreeParameterBlock
- DynamicLoader: RESUTILS.DLL/ResUtilGetPropertiesToParameterBlock
- DynamicLoader: RESUTILS.DLL/ResUtilResourcesEqual
- DynamicLoader: ADVAPI32.dll/GetSecurityInfo
- DynamicLoader: ADVAPI32.dll/GetAce
- DynamicLoader: ADVAPI32.dll/GetLengthSid
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAceEx
- DynamicLoader: ADVAPI32.dll/SetSecurityInfo
- DynamicLoader: ADVAPI32.dll/ImpersonateLoggedOnUser
- DynamicLoader: ADVAPI32.dll/RevertToSelf
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptVerifySignatureW
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: UxTheme.dll/
- DynamicLoader: UxTheme.dll/
- DynamicLoader: UxTheme.dll/
- DynamicLoader: UxTheme.dll/
- DynamicLoader: UxTheme.dll/
- DynamicLoader: UxTheme.dll/
- DynamicLoader: UxTheme.dll/
- DynamicLoader: SspiCli.dll/LsaRegisterLogonProcess
- DynamicLoader: SspiCli.dll/LsaLookupAuthenticationPackage
- DynamicLoader: SspiCli.dll/LsaCallAuthenticationPackage
- DynamicLoader: SspiCli.dll/LsaDeregisterLogonProcess
- DynamicLoader: ole32.dll/CoRegisterClassObject
- DynamicLoader: WS2_32.dll/
- DynamicLoader: SspiCli.dll/LsaRegisterPolicyChangeNotification
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: upnp.dll/DllGetClassObject
- DynamicLoader: upnp.dll/DllCanUnloadNow
- DynamicLoader: taskcomp.dll/InitializeAdapter
- DynamicLoader: taskcomp.dll/UpdateJobStatus
- DynamicLoader: ADVAPI32.dll/GetCurrentHwProfileW
- DynamicLoader: netutils.dll/NetpwPathType
- DynamicLoader: apphelp.dll/ApphelpCheckRunAppEx
- DynamicLoader: taskcomp.dll/ShutdownAdapter
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeA
- DynamicLoader: taskcomp.dll/RegisterTaskNotification
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingA
- DynamicLoader: taskcomp.dll/DeleteTaskNotification
- DynamicLoader: taskcomp.dll/SetSdNotification
- DynamicLoader: RPCRT4.dll/RpcStringFreeA
- DynamicLoader: taskcomp.dll/IsRegistering
- DynamicLoader: CFGMGR32.dll/CMP_RegisterNotification
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: sechost.dll/I_ScPnPGetServiceName
- DynamicLoader: sechost.dll/ConvertStringSecurityDescriptorToSecurityDescriptorW

- DynamicLoader: RPCRT4.dll/I_RpcExceptionFilter
- DynamicLoader: sechost.dll/OpenSCManagerA
- DynamicLoader: sechost.dll/OpenServiceA
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: sechost.dll/StartServiceA
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: CFGMGR32.dll/CM_MapCrToWin32Err
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_Size_ExW
- DynamicLoader: SspiCli.dll/LsaUnregisterPolicyChangeNotification
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_ExW
- DynamicLoader: ADVAPI32.dll/LsaOpenPolicy
- DynamicLoader: ADVAPI32.dll/LsaQueryInformationPolicy
- DynamicLoader: ADVAPI32.dll/LsaClose
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ADVAPI32.dll/LsaFreeMemory
- DynamicLoader: ADVAPI32.dll/ImpersonateLoggedOnUser
- DynamicLoader: SETUPAPI.dll/SetupDiCreateDeviceInfoList
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: SETUPAPI.dll/SetupDiOpenDeviceInterfaceW
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/WSASocketW
- DynamicLoader: WS2_32.dll/WSAIoctl
- DynamicLoader: WS2_32.dll/
- DynamicLoader: SETUPAPI.dll/SetupDiGetDeviceInterfaceDetailW
- DynamicLoader: SETUPAPI.dll/SetupDiGetDeviceRegistryPropertyW
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/WSAProviderConfigChange
- DynamicLoader: SETUPAPI.dll/SetupDiDeleteDeviceInterfaceData
- DynamicLoader: SETUPAPI.dll/SetupDiDestroyDeviceInfoList
- DynamicLoader: WS2_32.dll/getaddrinfo
- DynamicLoader: WINTRUST.dll/WinVerifyTrust
- DynamicLoader: CFGMGR32.dll/CMP_UnregisterNotification
- DynamicLoader: SETUPAPI.dll/SetupDiGetDevicePropertyW
- DynamicLoader: SETUPAPI.dll/CM_Get_DevNode_Registry_Property_ExW
- DynamicLoader: SETUPAPI.dll/CM_Get_Parent_Ex
- DynamicLoader: SETUPAPI.dll/CM_Get_DevNode_Custom_PropertyW
- DynamicLoader: WTSAPI32.dll/WTSEnumerateSessionsW
- DynamicLoader: WINSTA.dll/WinStationEnumerateW
- DynamicLoader: WINSTA.dll/WinStationFreeMemory
- DynamicLoader: WTSAPI32.dll/WTSFreeMemory
- DynamicLoader: ADVAPI32.dll/RevertToSelf
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeW
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/RpcBindingSetOption
- DynamicLoader: RPCRT4.dll/RpcStringFreeW
- DynamicLoader: RPCRT4.dll/RpcAsyncInitializeHandle
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: FVEAPI.dll/FveOpenVolumeW
- DynamicLoader: RPCRT4.dll/Ndr64AsyncClientCall
- DynamicLoader: FVEAPI.dll/FveGetStatus
- DynamicLoader: FVEAPI.dll/FveIsVolumeEncryptable
- DynamicLoader: FVEAPI.dll/FveCloseVolume

- DynamicLoader: SETUPAPI.dll/SetupDiGetClassDevsW
- DynamicLoader: wiarpc.dll/WiaEventsInitialize
- DynamicLoader: SETUPAPI.dll/SetupDiEnumDeviceInterfaces
- DynamicLoader: sechost.dll/ConvertStringSecurityDescriptorToSecurityDescriptorW
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: WS2_32.dll/
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ADVAPI32.dll/LogonUserW
- DynamicLoader: SspiCli.dll/LogonUserExExW
- DynamicLoader: WTSAPI32.dll/WTSQueryUserToken
- DynamicLoader: WINSTA.dll/WinStationQueryInformationW
- DynamicLoader: WTSAPI32.dll/WTSEnumerateSessionsW
- DynamicLoader: WTSAPI32.dll/WTSFreeMemory
- DynamicLoader: ADVAPI32.dll/QueryAllTracesW
- DynamicLoader: vssapi.DLL/CreateWriter
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ADVAPI32.dll/LookupAccountNameW
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: SAMCLI.DLL/NetLocalGroupGetMembers
- DynamicLoader: SAMLIB.dll/SamConnect
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeW
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcStringFreeW
- DynamicLoader: ADVAPI32.dll/EnumDependentServicesW
- DynamicLoader: ole32.dll/CoRevokeClassObject
- DynamicLoader: ole32.dll/CoDisconnectContext
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: SAMLIB.dll/SamOpenDomain
- DynamicLoader: SAMLIB.dll/SamLookupNamesInDomain
- DynamicLoader: SAMLIB.dll/SamOpenAlias
- DynamicLoader: SAMLIB.dll/SamFreeMemory
- DynamicLoader: SAMLIB.dll/SamCloseHandle
- DynamicLoader: SAMLIB.dll/SamGetMembersInAlias
- DynamicLoader: netutils.dll/NetApiBufferFree
- DynamicLoader: SAMLIB.dll/SamEnumerateDomainsInSamServer
- DynamicLoader: SAMLIB.dll/SamLookupDomainInSamServer
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/StringFromCLSID
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: PROPSYS.dll/VariantToPropVariant
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_Size_ExW
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_ExW
- DynamicLoader: SHELL32.dll/
- DynamicLoader: PROPSYS.dll/
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegGetValueW
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/

- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: PROPSYS.dll/InitPropVariantFromStringAsVector
- DynamicLoader: PROPSYS.dll/PSCoerceToCanonicalValue
- DynamicLoader: PROPSYS.dll/PropVariantToStringAlloc
- DynamicLoader: ole32.dll/PropVariantClear
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ADVAPI32.dll/OpenThreadToken
- DynamicLoader: ole32.dll/CoRegisterClassObject
- DynamicLoader: IPHLPAPI.DLL/GetAdaptersAddresses
- DynamicLoader: srvsvc.dll/ServiceMain
- DynamicLoader: srvsvc.dll/SvchostPushServiceGlobals
- DynamicLoader: sechost.dll/ConvertStringSecurityDescriptorToSecurityDescriptorW
- DynamicLoader: ADVAPI32.dll/LsaOpenPolicy
- DynamicLoader: ADVAPI32.dll/LsaQueryInformationPolicy
- DynamicLoader: netutils.dll/NetApiBufferAllocate
- DynamicLoader: ADVAPI32.dll/LsaFreeMemory
- DynamicLoader: ADVAPI32.dll/LsaClose
- DynamicLoader: netutils.dll/NetApiBufferFree
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ole32.dll/CLSIDFromOle1Class
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject2
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: thumbcache.dll/DllGetClassObject
- DynamicLoader: thumbcache.dll/DllCanUnloadNow
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: PROPSYS.dll/DllGetClassObject
- DynamicLoader: PROPSYS.dll/DllCanUnloadNow
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: IMM32.dll/ImmDisableIME
- DynamicLoader: psapi.dll/GetModuleFileNameExW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: wer.dll/WerpCreateIntegratorReportId
- DynamicLoader: wer.dll/WerReportCreate

- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: wer.dll/WerpSetIntegratorReportId
- DynamicLoader: wer.dll/WerReportSetParameter
- DynamicLoader: dbgeng.dll/DebugCreate
- DynamicLoader: ntdll.dll/CsrGetProcessId
- DynamicLoader: ntdll.dll/DbgBreakPoint
- DynamicLoader: ntdll.dll/DbgPrint
- DynamicLoader: ntdll.dll/DbgPrompt
- DynamicLoader: ntdll.dll/DbgUiConvertStateChangeStructure
- DynamicLoader: ntdll.dll/DbgUiGetThreadDebugObject
- DynamicLoader: ntdll.dll/DbgUiIssueRemoteBreakin
- DynamicLoader: ntdll.dll/DbgUiSetThreadDebugObject
- DynamicLoader: ntdll.dll/NtAllocateVirtualMemory
- DynamicLoader: ntdll.dll/NtClose
- DynamicLoader: ntdll.dll/NtCreateDebugObject
- DynamicLoader: ntdll.dll/NtCreateFile
- DynamicLoader: ntdll.dll/NtDebugActiveProcess
- DynamicLoader: ntdll.dll/NtDebugContinue
- DynamicLoader: ntdll.dll/NtFreeVirtualMemory
- DynamicLoader: ntdll.dll/NtOpenProcess
- DynamicLoader: ntdll.dll/NtOpenThread
- DynamicLoader: ntdll.dll/NtQueryInformationProcess
- DynamicLoader: ntdll.dll/NtQueryInformationThread
- DynamicLoader: ntdll.dll/NtQueryMutant
- DynamicLoader: ntdll.dll/NtQueryObject
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtRemoveProcessDebug
- DynamicLoader: ntdll.dll/NtResumeThread
- DynamicLoader: ntdll.dll/NtSetInformationDebugObject
- DynamicLoader: ntdll.dll/NtSetInformationProcess
- DynamicLoader: ntdll.dll/NtSystemDebugControl
- DynamicLoader: ntdll.dll/NtWaitForDebugEvent
- DynamicLoader: ntdll.dll/RtlAnsiStringToUnicodeString
- DynamicLoader: ntdll.dll/RtlCreateProcessParameters
- DynamicLoader: ntdll.dll/RtlCreateUserProcess
- DynamicLoader: ntdll.dll/RtlDestroyProcessParameters
- DynamicLoader: ntdll.dll/RtlDosPathNameToNtPathName_U
- DynamicLoader: ntdll.dll/RtlFindMessage
- DynamicLoader: ntdll.dll/RtlFreeHeap
- DynamicLoader: ntdll.dll/RtlFreeUnicodeString
- DynamicLoader: ntdll.dll/RtlGetFunctionTableListHead
- DynamicLoader: ntdll.dll/RtlGetUnloadEventTrace
- DynamicLoader: ntdll.dll/RtlGetUnloadEventTraceEx
- DynamicLoader: ntdll.dll/RtlInitAnsiString
- DynamicLoader: ntdll.dll/RtlInitUnicodeString
- DynamicLoader: ntdll.dll/RtlTryEnterCriticalSection
- DynamicLoader: ntdll.dll/RtlUnicodeStringToAnsiString
- DynamicLoader: ntdll.dll/NtOpenProcessToken
- DynamicLoader: ntdll.dll/NtOpenThreadToken
- DynamicLoader: ntdll.dll/NtQueryInformationToken
- DynamicLoader: kernel32.dll/CloseProfileUserMapping
- DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
- DynamicLoader: kernel32.dll/DebugActiveProcessStop
- DynamicLoader: kernel32.dll/DebugBreak
- DynamicLoader: kernel32.dll/DebugBreakProcess
- DynamicLoader: kernel32.dll/DebugSetProcessKillOnExit
- DynamicLoader: kernel32.dll/Module32First
- DynamicLoader: kernel32.dll/Module32FirstW
- DynamicLoader: kernel32.dll/Module32Next
- DynamicLoader: kernel32.dll/Module32NextW
- DynamicLoader: kernel32.dll/OpenThread
- DynamicLoader: kernel32.dll/Process32First
- DynamicLoader: kernel32.dll/Process32FirstW

- DynamicLoader: kernel32.dll/Process32Next
- DynamicLoader: kernel32.dll/Process32NextW
- DynamicLoader: kernel32.dll/ProcessIdToSessionId
- DynamicLoader: kernel32.dll/SetProcessShutdownParameters
- DynamicLoader: kernel32.dll/Thread32First
- DynamicLoader: kernel32.dll/Thread32Next
- DynamicLoader: kernel32.dll/GetTimeZoneInformation
- DynamicLoader: kernel32.dll/DuplicateHandle
- DynamicLoader: kernel32.dll/Wow64GetThreadSelectorEntry
- DynamicLoader: ADVAPI32.dll/CloseServiceHandle
- DynamicLoader: ADVAPI32.dll/ControlService
- DynamicLoader: ADVAPI32.dll/CreateServiceA
- DynamicLoader: ADVAPI32.dll/CreateServiceW
- DynamicLoader: ADVAPI32.dll/DeleteService
- DynamicLoader: ADVAPI32.dll/EnumServicesStatusExA
- DynamicLoader: ADVAPI32.dll/EnumServicesStatusExW
- DynamicLoader: ADVAPI32.dll/GetEventLogInformation
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenSCManagerA
- DynamicLoader: ADVAPI32.dll/OpenSCManagerW
- DynamicLoader: ADVAPI32.dll/OpenServiceA
- DynamicLoader: ADVAPI32.dll/OpenServiceW
- DynamicLoader: ADVAPI32.dll/StartServiceA
- DynamicLoader: ADVAPI32.dll/StartServiceW
- DynamicLoader: ADVAPI32.dll/GetSidSubAuthority
- DynamicLoader: ADVAPI32.dll/GetSidSubAuthorityCount
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeExW
- DynamicLoader: VERSION.dll/GetFileVersionInfoExW
- DynamicLoader: dbghelp.dll/DebugExtensionInitialize
- DynamicLoader: dbghelp.dll/WinDbgExtensionDllInit
- DynamicLoader: dbghelp.dll/ExtensionApiVersion
- DynamicLoader: dbghelp.dll/CheckVersion
- DynamicLoader: wer.dll/WerpSetDynamicParameter
- DynamicLoader: wer.dll/WerReportAddDump
- DynamicLoader: wer.dll/WerpSetCallBack
- DynamicLoader: wer.dll/WerReportSetUIOption
- DynamicLoader: wer.dll/WerpAddRegisteredDataToReport
- DynamicLoader: wer.dll/WerReportSubmit
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegGetValueW
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/CheckTokenMembership
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: SensApi.dll/IsNetworkAlive
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/CharUpperW
- DynamicLoader: wer.dll/WerpAddAppCompatData
- DynamicLoader: apphelp.dll/SdbGetFileAttributes
- DynamicLoader: apphelp.dll/SdbFormatAttribute
- DynamicLoader: apphelp.dll/SdbFreeFileAttributes
- DynamicLoader: apphelp.dll/SdbGetFileAttributes
- DynamicLoader: apphelp.dll/SdbFormatAttribute
- DynamicLoader: apphelp.dll/SdbFreeFileAttributes

- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: SHELL32.dll/SHGetFolderPathEx
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: profapi.dll/
- DynamicLoader: dbghelp.dll/MiniDumpWriteDump
- DynamicLoader: kernel32.dll/OpenThread
- DynamicLoader: kernel32.dll/Thread32First
- DynamicLoader: kernel32.dll/Thread32Next
- DynamicLoader: kernel32.dll/Module32First
- DynamicLoader: kernel32.dll/Module32Next
- DynamicLoader: kernel32.dll/Module32FirstW
- DynamicLoader: kernel32.dll/Module32NextW
- DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
- DynamicLoader: kernel32.dll/GetLongPathNameA
- DynamicLoader: kernel32.dll/GetLongPathNameW
- DynamicLoader: kernel32.dll/GetProcessTimes
- DynamicLoader: kernel32.dll/GetTimeZoneInformation
- DynamicLoader: ntdll.dll/NtOpenThread
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtQueryInformationProcess
- DynamicLoader: ntdll.dll/NtQueryInformationThread
- DynamicLoader: ntdll.dll/NtQueryObject
- DynamicLoader: ntdll.dll/NtQueryMutant
- DynamicLoader: ntdll.dll/NtSystemDebugControl
- DynamicLoader: ntdll.dll/RtlFreeHeap
- DynamicLoader: ntdll.dll/RtlGetFunctionTableListHead
- DynamicLoader: ntdll.dll/RtlGetUnloadEventTrace
- DynamicLoader: ntdll.dll/RtlGetUnloadEventTraceEx
- DynamicLoader: ntdll.dll/NtOpenProcessToken
- DynamicLoader: ntdll.dll/NtOpenThreadToken
- DynamicLoader: ntdll.dll/NtQueryInformationToken
- DynamicLoader: ntdll.dll/NtClose
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/GetSidSubAuthority
- DynamicLoader: ADVAPI32.dll/GetSidSubAuthorityCount
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExA
- DynamicLoader: ADVAPI32.dll/RegQueryValueExA
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: powrprof.dll/CallNtPowerInformation
- DynamicLoader: psapi.dll/EnumProcessModules
- DynamicLoader: psapi.dll/GetModuleFileNameExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeA
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoA
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueA
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: verifier.dll/VerifierEnumerateResource
- DynamicLoader: ntdll.dll/NtSuspendProcess
- DynamicLoader: ntdll.dll/NtResumeProcess
- DynamicLoader: kernel32.dll/OpenThread
- DynamicLoader: kernel32.dll/Thread32First
- DynamicLoader: kernel32.dll/Thread32Next
- DynamicLoader: kernel32.dll/Module32First
- DynamicLoader: kernel32.dll/Module32Next
- DynamicLoader: kernel32.dll/Module32FirstW

- DynamicLoader: kernel32.dll/Module32NextW
- DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
- DynamicLoader: kernel32.dll/GetLongPathNameA
- DynamicLoader: kernel32.dll/GetLongPathNameW
- DynamicLoader: kernel32.dll/GetProcessTimes
- DynamicLoader: kernel32.dll/GetTimeZoneInformation
- DynamicLoader: ntdll.dll/NtOpenThread
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtQueryInformationProcess
- DynamicLoader: ntdll.dll/NtQueryInformationThread
- DynamicLoader: ntdll.dll/NtQueryObject
- DynamicLoader: ntdll.dll/NtQueryMutant
- DynamicLoader: ntdll.dll/NtSystemDebugControl
- DynamicLoader: ntdll.dll/RtlFreeHeap
- DynamicLoader: ntdll.dll/RtlGetFunctionTableListHead
- DynamicLoader: ntdll.dll/RtlGetUnloadEventTrace
- DynamicLoader: ntdll.dll/RtlGetUnloadEventTraceEx
- DynamicLoader: ntdll.dll/NtOpenProcessToken
- DynamicLoader: ntdll.dll/NtOpenThreadToken
- DynamicLoader: ntdll.dll/NtQueryInformationToken
- DynamicLoader: ntdll.dll/NtClose
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/GetSidSubAuthority
- DynamicLoader: ADVAPI32.dll/GetSidSubAuthorityCount
- DynamicLoader: powrprof.dll/CallNtPowerInformation
- DynamicLoader: psapi.dll/EnumProcessModules
- DynamicLoader: psapi.dll/GetModuleFileNameExW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeA
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoA
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueA
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: ADVAPI32.dll/QueryTraceW
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/IsValidSid
- DynamicLoader: ADVAPI32.dll/GetLengthSid
- DynamicLoader: ADVAPI32.dll/CopySid
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAceEx
- DynamicLoader: ADVAPI32.dll/InitializeSecurityDescriptor
- DynamicLoader: ADVAPI32.dll/SetSecurityDescriptorDacl
- DynamicLoader: ADVAPI32.dll/RegisterEventSourceW
- DynamicLoader: ADVAPI32.dll/ReportEventW
- DynamicLoader: ADVAPI32.dll/DeregisterEventSource
- DynamicLoader: SHLWAPI.dll/PathIsDirectoryW
- DynamicLoader: wer.dll/WerpGetStoreLocation
- DynamicLoader: wer.dll/WerpGetStoreType
- DynamicLoader: wer.dll/WerReportCloseHandle
- DynamicLoader: USER32.dll/MsgWaitForMultipleObjects
- DynamicLoader: ADVAPI32.dll/DuplicateToken
- DynamicLoader: wer.dll/WerpFreeString
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: kernel32.dll/FlsAlloc
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: kernel32.dll/FlsSetValue
- DynamicLoader: kernel32.dll/FlsFree
- DynamicLoader: kernel32.dll/IsProcessorFeaturePresent
- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: ADVAPI32.dll/RegGetValueW
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW

- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: SHELL32.dll/SHGetFolderPathEx
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: profapi.dll/
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/CheckTokenMembership
- DynamicLoader: USER32.dll/GetProcessWindowStation
- DynamicLoader: USER32.dll/GetThreadDesktop
- DynamicLoader: USER32.dll/GetUserObjectInformationW
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: SensApi.dll/IsNetworkAlive
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/CharUpperW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: werui.dll/WerUICreate
- DynamicLoader: werui.dll/WerUIStart
- DynamicLoader: ADVAPI32.dll/RegisterEventSourceW
- DynamicLoader: ADVAPI32.dll/ReportEventW
- DynamicLoader: ADVAPI32.dll/DeregisterEventSource
- DynamicLoader: werui.dll/WerUITerminate
- DynamicLoader: werui.dll/WerUIDelete
- DynamicLoader: SHLWAPI.dll/PathIsDirectoryW
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: USER32.dll/MsgWaitForMultipleObjects
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: sechost.dll/LookupAccountNameLocalW

Starts servers listening on 0.0.0.0:0, :0

Scheduled file move on reboot detected

- File Move on Reboot: Old: C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_svchost.exe_7cd839042cd1de73f48236893e54999c52054_cab_0b26ad6f\Report.wer.tmp -> New: C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_svchost.exe_7cd839042cd1de73f48236893e54999c52054_cab_0b26ad6f\Report.wer
- File Move on Reboot: Old: C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_taskhost.exe_7f86ff522426a3314829b0b4bf7c44a66fbeec_cab_0aa37e52\Report.wer.tmp -> New: C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_taskhost.exe_7f86ff522426a3314829b0b4bf7c44a66fbeec_cab_0aa37e52\Report.wer

Attempts to connect to a dead IP:Port (1 unique times)

- IP: 192.168.56.1:80

At least one process apparently crashed during execution

SetUnhandledExceptionFilter detected (possible anti-debug)