

## O.exe

Is DLL

Packer

Anti Debug

Anti VM

Signed

XOR

**MalFamily: Ispy**

**MalScore: 100**

<b>File type:</b>	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
<b>File size:</b>	1409.50 KB (1443328 bytes)
<b>Compile time:</b>	2006-06-15 09:47:09
<b>MD5:</b>	1361a18bda5df2080018ebe752879fb9
<b>SHA1:</b>	2847a530395d1b34cbbbb878a4bcb6617630b30b
<b>Import hash:</b>	f34d5f2d4577ed6d9ceec516c1f5a744
<b>Submitted:</b>	2019-09-15 18:45:04

### URL(s) file hosting

<http://172.93.187.131/O.exe>

### Antivirus Report

Report date	Detection Ratio	Permalink
2019-09-15 16:11:43	14/66	

### Import library

mscoree.dll

**17**

## Behaviors detected by system signatures

Collects information to fingerprint the system

Creates a copy of itself



- copy: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Smartscreen.exe

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

Retrieves Windows ProductID, probably to fingerprint the sandbox

Installs itself for autorun at Windows startup

- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Smartscreen.Ink  
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Smartscreen.exe  
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Smartscreen.exe:Zone.Identifier  
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Smartscreen.exe  
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Smartscreen.Ink

Exhibits behavior characteristic of iSpy Keylogger

Executed a process and injected code into it, probably while unpacking

- Injection: Smartscreen.exe(924) -> Smartscreen.exe(1384)

Uses Windows utilities for basic functionality

- command: cmd.exe /C type nul > "C:\Users\Seven01\AppData\Local\Temp\O.exe:Zone.Identifier"  
- command: cmd.exe /C type nul > "C:\Users\Seven01\AppData\Local\Temp\O.exe:Zone.Identifier"  
- command: cmd.exe /c copy "C:\Users\Seven01\AppData\Local\Temp\O.exe"  
"C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Smartscreen.exe"  
- command: cmd.exe /c copy "C:\Users\Seven01\AppData\Local\Temp\O.exe"  
"C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Smartscreen.exe"  
- command: cmd.exe /c, "C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Smartscreen.exe"  
- command: cmd.exe /C type nul > "C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Smartscreen.exe:Zone.Identifier"  
- command: cmd.exe /C type nul > "C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Smartscreen.exe:Zone.Identifier"

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Smartscreen.exe

A process created a hidden window

- Process: O.exe -> cmd.exe  
- Process: O.exe -> cmd.exe  
- Process: O.exe -> cmd.exe  
- Process: Smartscreen.exe -> cmd.exe

Reads data out of its own binary image

- self\_read: process: Smartscreen.exe, pid: 924, offset: 0x00000000, length: 0x00032000

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: ADVAPI32.dll/RegQueryValueExW



- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- 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/UrllsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- 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/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- 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: KERNELBASE.dll/SetSystemFileCacheSize
- DynamicLoader: ntdll.dll/NtSetSystemInformation
- DynamicLoader: KERNELBASE.dll/PrivIsDllSynchronizationHeld
- DynamicLoader: KERNEL32.dll/AddDllDirectory
- DynamicLoader: KERNEL32.dll/SortGetHandle



- DynamicLoader: KERNEL32.dll/SortCloseHandle
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap\_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetUserPreferredUILanguages
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: KERNEL32.dll/CompareStringOrdinal
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/SetThreadErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: clr.dll/CreateAssemblyNameObject
- DynamicLoader: clr.dll/CreateAssemblyNameObjectW
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: ole32.dll/CoGetObjectContext
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- 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: clr.dll/CreateAssemblyEnum
- DynamicLoader: clr.dll/CreateAssemblyEnumW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/ResolveLocaleName
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetCurrentProcessId
- DynamicLoader: KERNEL32.dll/GetCurrentProcessIdW



- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValue
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivilegesW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/OpenProcess
- DynamicLoader: KERNEL32.dll/OpenProcessW
- DynamicLoader: psapi.dll/EnumProcessModules
- DynamicLoader: psapi.dll/EnumProcessModulesW
- DynamicLoader: psapi.dll/GetModuleInformation
- DynamicLoader: psapi.dll/GetModuleInformationW
- DynamicLoader: psapi.dll/GetModuleBaseName
- DynamicLoader: psapi.dll/GetModuleBaseNameW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: psapi.dll/GetModuleFileNameEx
- DynamicLoader: psapi.dll/GetModuleFileNameExW
- DynamicLoader: KERNEL32.dll/ExpandEnvironmentStrings
- DynamicLoader: KERNEL32.dll/ExpandEnvironmentStringsW
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- 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: ole32.dll/CoUninitialize
- DynamicLoader: ole32.dll/CoRevokeInitializeSpy
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: nlsorting.dll/SortGetHandle
- DynamicLoader: nlsorting.dll/SortCloseHandle
- DynamicLoader: gdiplus.dll/GdiplusStartup
- DynamicLoader: KERNEL32.dll/IsProcessorFeaturePresent
- DynamicLoader: USER32.dll/GetWindowInfo
- DynamicLoader: USER32.dll/GetAncestor
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/EnumDisplayDevicesA
- DynamicLoader: GDI32.dll/ExtTextOutW
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: gdiplus.dll/GdiplLoadImageFromStream
- DynamicLoader: WindowsCodecs.dll/DllGetClassObject
- DynamicLoader: KERNEL32.dll/WerRegisterMemoryBlock
- DynamicLoader: gdiplus.dll/GdiplImageForceValidation
- DynamicLoader: gdiplus.dll/GdiplGetImageType
- DynamicLoader: gdiplus.dll/GdiplGetImageRawFormat
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptImportKey



- DynamicLoader: CRYPTSP.dll/CryptExportKey
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: gdiplus.dll/GdipGetImageWidth
- DynamicLoader: gdiplus.dll/GdipGetImageHeight
- DynamicLoader: gdiplus.dll/GdipGetImageEncodersSize
- DynamicLoader: gdiplus.dll/GdipGetImageEncoders
- DynamicLoader: gdiplus.dll/GdipSaveImageToStream
- DynamicLoader: gdiplus.dll/GdipCreateBitmapFromStream
- DynamicLoader: gdiplus.dll/GdipBitmapLockBits
- DynamicLoader: gdiplus.dll/GdipBitmapUnlockBits
- DynamicLoader: gdiplus.dll/GdipDisposeImage
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: KERNEL32.dll/GetFileType
- DynamicLoader: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: KERNEL32.dll/DeleteFile
- DynamicLoader: KERNEL32.dll/DeleteFileW
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: comctl32.dll/
- DynamicLoader: KERNEL32.dll/CreateActCtxW
- DynamicLoader: KERNEL32.dll/AddRefActCtx
- DynamicLoader: KERNEL32.dll/ReleaseActCtx
- DynamicLoader: KERNEL32.dll/ActivateActCtx
- DynamicLoader: KERNEL32.dll/DeactivateActCtx
- DynamicLoader: KERNEL32.dll/GetCurrentActCtx
- DynamicLoader: KERNEL32.dll/QueryActCtxW
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: kernel32.dll/SetThreadUILanguage
- DynamicLoader: kernel32.dll/CopyFileExW
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: kernel32.dll/SetConsoleInputExeNameW
- DynamicLoader: kernel32.dll/SetThreadUILanguage
- DynamicLoader: kernel32.dll/CopyFileExW
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: kernel32.dll/SetConsoleInputExeNameW
- DynamicLoader: kernel32.dll/SetThreadUILanguage
- DynamicLoader: kernel32.dll/CopyFileExW
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: kernel32.dll/SetConsoleInputExeNameW
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- 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: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- 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/GetCurrentPackageld
- 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/UrllsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- 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/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- 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: KERNELBASE.dll/SetSystemFileCacheSize
- DynamicLoader: ntdll.dll/NtSetSystemInformation
- DynamicLoader: KERNELBASE.dll/PrivIsDlISynchronizationHeld
- DynamicLoader: KERNEL32.dll/AddDllDirectory
- DynamicLoader: KERNEL32.dll/SortGetHandle
- DynamicLoader: KERNEL32.dll/SortCloseHandle
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap



- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap\_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetUserPreferredUILanguages
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: KERNEL32.dll/CompareStringOrdinal
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/SetThreadErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: clr.dll/CreateAssemblyNameObject
- DynamicLoader: clr.dll/CreateAssemblyNameObjectW
- DynamicLoader: ole32.dll/CoGetObjectContext
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- 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: clr.dll/CreateAssemblyEnum
- DynamicLoader: clr.dll/CreateAssemblyEnumW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/ResolveLocaleName
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetCurrentProcessId
- DynamicLoader: KERNEL32.dll/GetCurrentProcessIdW
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValue
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivilegesW

- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/OpenProcess
- DynamicLoader: KERNEL32.dll/OpenProcessW
- DynamicLoader: psapi.dll/EnumProcessModules
- DynamicLoader: psapi.dll/EnumProcessModulesW
- DynamicLoader: psapi.dll/GetModuleInformation
- DynamicLoader: psapi.dll/GetModuleInformationW
- DynamicLoader: psapi.dll/GetModuleBaseName
- DynamicLoader: psapi.dll/GetModuleBaseNameW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: psapi.dll/GetModuleFileNameEx
- DynamicLoader: psapi.dll/GetModuleFileNameExW
- DynamicLoader: KERNEL32.dll/ExpandEnvironmentStrings
- DynamicLoader: KERNEL32.dll/ExpandEnvironmentStringsW
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- 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: ole32.dll/CoUninitialize
- DynamicLoader: ole32.dll/CoRevokeInitializeSpy
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: nlsorting.dll/SortGetHandle
- DynamicLoader: nlsorting.dll/SortCloseHandle
- DynamicLoader: gdiplus.dll/GdiplusStartup
- DynamicLoader: KERNEL32.dll/IsProcessorFeaturePresent
- DynamicLoader: USER32.dll/GetWindowInfo
- DynamicLoader: USER32.dll/GetAncestor
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/EnumDisplayDevicesA
- DynamicLoader: GDI32.dll/ExtTextOutW
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: gdiplus.dll/GdiplLoadImageFromStream
- DynamicLoader: WindowsCodecs.dll/DllGetClassObject
- DynamicLoader: KERNEL32.dll/WerRegisterMemoryBlock
- DynamicLoader: gdiplus.dll/GdiplImageForceValidation
- DynamicLoader: gdiplus.dll/GdiplGetImageType
- DynamicLoader: gdiplus.dll/GdiplGetImageRawFormat
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptExportKey
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: gdiplus.dll/GdiplGetImageWidth
- DynamicLoader: gdiplus.dll/GdiplGetImageHeight



- DynamicLoader: gdiplus.dll/GdipGetImageEncodersSize
- DynamicLoader: gdiplus.dll/GdipGetImageEncoders
- DynamicLoader: gdiplus.dll/GdipSaveImageToStream
- DynamicLoader: gdiplus.dll/GdipCreateBitmapFromStream
- DynamicLoader: gdiplus.dll/GdipBitmapLockBits
- DynamicLoader: gdiplus.dll/GdipBitmapUnlockBits
- DynamicLoader: gdiplus.dll/GdipDisposeImage
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: KERNEL32.dll/GetFileType
- DynamicLoader: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: KERNEL32.dll/ReadFile
- DynamicLoader: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: sxs.dll/SxsLookupClrGuid
- DynamicLoader: KERNEL32.dll/ReleaseActCtx
- DynamicLoader: ole32.dll/CoGetClassObject
- 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: wshom.ocx/DllGetClassObject
- DynamicLoader: wshom.ocx/DllCanUnloadNow
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: OLEAUT32.dll/DllGetClassObject
- DynamicLoader: OLEAUT32.dll/DllCanUnloadNow
- DynamicLoader: sxs.dll/SxsOleAut32RedirectTypeLibrary
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: ADVAPI32.dll/RegQueryValueW
- DynamicLoader: sxs.dll/SxsOleAut32MapConfiguredClsidToReferenceClsid
- DynamicLoader: ole32.dll/IIDFromString
- DynamicLoader: sxs.dll/SxsOleAut32MapIIDToProxyStubCLSID
- DynamicLoader: sxs.dll/SxsOleAut32MapIIDToTLBPath
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: OLEAUT32.dll/BSTR\_UserSize
- DynamicLoader: OLEAUT32.dll/BSTR\_UserMarshal
- DynamicLoader: OLEAUT32.dll/BSTR\_UserUnmarshal
- DynamicLoader: OLEAUT32.dll/BSTR\_UserFree
- DynamicLoader: OLEAUT32.dll/VARIANT\_UserSize
- DynamicLoader: OLEAUT32.dll/VARIANT\_UserMarshal
- DynamicLoader: OLEAUT32.dll/VARIANT\_UserUnmarshal
- DynamicLoader: OLEAUT32.dll/VARIANT\_UserFree
- DynamicLoader: OLEAUT32.dll/LPSAFEARRAY\_UserSize
- DynamicLoader: OLEAUT32.dll/LPSAFEARRAY\_UserMarshal
- DynamicLoader: OLEAUT32.dll/LPSAFEARRAY\_UserUnmarshal
- DynamicLoader: OLEAUT32.dll/LPSAFEARRAY\_UserFree
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemFree



- DynamicLoader: ADVAPI32.dll/RegQueryValueW
- DynamicLoader: PROPSYS.dll/PSPropertyBag\_WriteStr
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: PROPSYS.dll/PSPropertyBag\_ReadBSTR
- DynamicLoader: LINKINFO.dll/CreateLinkInfoW
- DynamicLoader: USER32.dll/IsCharAlphaW
- DynamicLoader: USER32.dll/CharPrevW
- DynamicLoader: ntshrui.dll/GetNetResourceFromLocalPathW
- DynamicLoader: srvcli.dll/NetShareEnum
- DynamicLoader: cscapi.dll/CscNetApiGetInterface
- DynamicLoader: slc.dll/SLGetWindowsInformationDWORD
- DynamicLoader: SHLWAPI.dll/PathRemoveFileSpecW
- DynamicLoader: LINKINFO.dll/DestroyLinkInfo
- DynamicLoader: ADVAPI32.dll/ConvertSidToStringSidW
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: ADVAPI32.dll/CryptAcquireContext
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextW
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/CryptGetProvParam
- DynamicLoader: CRYPTSP.dll/CryptGetProvParam
- DynamicLoader: CRYPTSP.dll/CryptGetDefaultProviderW
- DynamicLoader: ADVAPI32.dll/CryptContextAddRef
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptContextAddRef
- DynamicLoader: ADVAPI32.dll/CryptContextAddRef
- DynamicLoader: ADVAPI32.dll/CryptDuplicateKey
- DynamicLoader: CRYPTSP.dll/CryptDuplicateKey
- DynamicLoader: ADVAPI32.dll/CryptSetKeyParam
- DynamicLoader: CRYPTSP.dll/CryptSetKeyParam
- DynamicLoader: ADVAPI32.dll/CryptDecrypt
- DynamicLoader: CRYPTSP.dll/CryptDecrypt
- DynamicLoader: ADVAPI32.dll/CryptDestroyKey
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: KERNEL32.dll/GetCurrentDirectory
- DynamicLoader: KERNEL32.dll/GetCurrentDirectoryW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ADVAPI32.dll/CreateProcessAsUser
- DynamicLoader: ADVAPI32.dll/CreateProcessAsUserA
- DynamicLoader: KERNEL32.dll/WideCharToMultiByte
- DynamicLoader: KERNEL32.dll/GetThreadContext
- DynamicLoader: KERNEL32.dll/ReadProcessMemory
- DynamicLoader: KERNEL32.dll/VirtualAllocEx
- DynamicLoader: KERNEL32.dll/WriteProcessMemory
- DynamicLoader: KERNEL32.dll/SetThreadContext
- DynamicLoader: KERNEL32.dll/ResumeThread
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: netutils.dll/NetApiBufferFree
- DynamicLoader: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: comctl32.dll/
- DynamicLoader: KERNEL32.dll/CreateActCtxW
- DynamicLoader: KERNEL32.dll/AddRefActCtx
- DynamicLoader: KERNEL32.dll/ReleaseActCtx
- DynamicLoader: KERNEL32.dll/ActivateActCtx
- DynamicLoader: KERNEL32.dll/DeactivateActCtx
- DynamicLoader: KERNEL32.dll/GetCurrentActCtx
- DynamicLoader: KERNEL32.dll/QueryActCtxW
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/EventUnregister



- DynamicLoader: kernel32.dll/SetThreadUILanguage
- DynamicLoader: kernel32.dll/CopyFileExW
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: kernel32.dll/SetConsoleInputExeNameW
- 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: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- 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/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue



- DynamicLoader: KERNEL32.dll/FIsSetValue
- 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/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- 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: KERNELBASE.dll/SetSystemFileCacheSize
- DynamicLoader: ntdll.dll/NtSetSystemInformation
- DynamicLoader: KERNELBASE.dll/PrivIsDllSynchronizationHeld
- DynamicLoader: KERNEL32.dll/AddDllDirectory
- DynamicLoader: KERNEL32.dll/SortGetHandle
- DynamicLoader: KERNEL32.dll/SortCloseHandle
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetUserPreferredUILanguages
- DynamicLoader: nlssorting.dll/SortGetHandle
- DynamicLoader: nlssorting.dll/SortCloseHandle
- DynamicLoader: ADVAPI32.dll/ConvertSidToStringSidW
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/SetThreadErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap\_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: KERNEL32.dll/GetTimeZoneInformation
- DynamicLoader: KERNEL32.dll/GetDynamicTimeZoneInformation
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: KERNEL32.dll/GetFileMUIPath
- DynamicLoader: KERNEL32.dll/LoadLibraryEx





- DynamicLoader: KERNEL32.dll/LoadLibraryExW
- DynamicLoader: KERNEL32.dll/FreeLibrary
- DynamicLoader: KERNEL32.dll/FreeLibraryW
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: KERNEL32.dll/GetModuleHandle
- DynamicLoader: KERNEL32.dll/GetModuleHandleW
- DynamicLoader: KERNEL32.dll/GetProcAddress
- DynamicLoader: KERNEL32.dll/WideCharToMultiByte
- DynamicLoader: USER32.dll/DefWindowProcW
- DynamicLoader: GDI32.dll/GetStockObject
- DynamicLoader: USER32.dll/RegisterClass
- DynamicLoader: USER32.dll/RegisterClassW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: USER32.dll/CreateWindowEx
- DynamicLoader: USER32.dll/CreateWindowExW
- DynamicLoader: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/GetWindowLong
- DynamicLoader: USER32.dll/GetWindowLongW
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentThread
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: KERNEL32.dll/GetCurrentThreadId
- DynamicLoader: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/CallWindowProc
- DynamicLoader: USER32.dll/CallWindowProcW
- DynamicLoader: USER32.dll/RegisterWindowMessage
- DynamicLoader: USER32.dll/RegisterWindowMessageW
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: CRYPTSP.dll/CryptGetDefaultProviderW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: ole32.dll/CreateBindCtx
- DynamicLoader: ole32.dll/CoGetObjectContext
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- 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/\_RpcExtInitializeExtensionPoint
- DynamicLoader: ole32.dll/MkParseDisplayName
- 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: ole32.dll/BindMoniker
- DynamicLoader: SXS.DLL/SxsOleAut32RedirectTypeLibrary
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: ADVAPI32.dll/RegQueryValueW
- DynamicLoader: SXS.DLL/SxsOleAut32MapConfiguredClsidToReferenceClsid
- DynamicLoader: SXS.DLL/SxsLookupClrGuid
- DynamicLoader: KERNEL32.dll/ReleaseActCtx
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: mscoreei.dll/\_CorDllMain\_RetAddr
- DynamicLoader: mscoreei.dll/\_CorDllMain
- DynamicLoader: MSCOREE.DLL/GetTokenForVTableEntry
- DynamicLoader: MSCOREE.DLL/SetTargetForVTableEntry
- DynamicLoader: MSCOREE.DLL/GetTargetForVTableEntry
- DynamicLoader: mscoreei.dll/GetTokenForVTableEntry\_RetAddr
- DynamicLoader: mscoreei.dll/GetTokenForVTableEntry
- DynamicLoader: mscoreei.dll/SetTargetForVTableEntry\_RetAddr
- DynamicLoader: mscoreei.dll/SetTargetForVTableEntry
- DynamicLoader: mscoreei.dll/GetTargetForVTableEntry\_RetAddr
- DynamicLoader: mscoreei.dll/GetTargetForVTableEntry
- DynamicLoader: KERNEL32.dll/GetLastError
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/CreateEvent
- DynamicLoader: KERNEL32.dll/CreateEventW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/SetEvent
- DynamicLoader: ole32.dll/CoWaitForMultipleHandles
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: ole32.dll/IIDFromString
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: KERNEL32.dll/LoadLibrary
- DynamicLoader: KERNEL32.dll/LoadLibraryA
- 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: 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: OLEAUT32.dll/SysStringLen
- DynamicLoader: KERNEL32.dll/RtlZeroMemory
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: KERNEL32.dll/RegOpenKeyExW
- 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: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ole32.dll/CLSIDFromString
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- 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: wbemcore.dll/Reinitialize
- 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: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: SspiCli.dll/LogonUserExExW
- 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: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- 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

A process attempted to delay the analysis task.

- Process: Smartscreen.exe tried to sleep 335 seconds, actually delayed analysis time by 0 seconds

Guard pages use detected - possible anti-debugging.



## Creates RWX memory

Executed a command line with /C or /R argument to terminate command shell on completion which can be used to hide execution

```
- command: cmd.exe /C type nul > "C:\Users\Seven01\AppData\Local\Temp\O.exe:Zone.Identifier"  
- command: cmd.exe /c copy "C:\Users\Seven01\AppData\Local\Temp\O.exe"  
"C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start  
Menu\Programs\Startup\Smartscreen.exe"  
- command: cmd.exe /c, "C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start  
Menu\Programs\Startup\Smartscreen.exe"  
- command: cmd.exe /C type nul > "C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start  
Menu\Programs\Startup\Smartscreen.exe:Zone.Identifier"
```

SetUnhandledExceptionFilter detected (possible anti-debug)