

dafa.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:	349.00 KB (357376 bytes)
Compile time:	2019-09-19 23:43:43
MD5:	620239d356bc0af1c8dd8846a2613424
SHA1:	0d3d341acc603593c8e060220e5e5046f987c065
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2019-09-28 16:30:06

URL(s) file hosting

<http://www.sindicato1ucm.cl/wp-content/dafa.exe>

<http://sindicato1ucm.cl/wp-content/dafa.exe>

Antivirus Report

Report date	Detection Ratio	Permalink
2019-09-20 16:13:08	17/71	

Import library

mscoree.dll

24

Behaviors detected by system signatures

Attempts to create or modify system certificates



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

- Injection: dafa.exe(2772) -> dafa.exe(2328)

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\ProgramData\images.exe:Zone.Identifier

Code injection with CreateRemoteThread in a remote process

- Injection: images.exe(2260) -> cmd.exe(2356)

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

- Spam: services.exe (480) called API GetSystemTimeAsFileTime 3297499 times
- Spam: lsass.exe (496) called API NtClose 121824 times
- Spam: WmiPrvSE.exe (1392) called API GetSystemTimeAsFileTime 26872 times

Installs itself for autorun at Windows startup

- file: C:\Windows\Tasks\Adobe Flash Player Updater.job
- file: C:\Windows\Tasks\Adobe Flash Player Updater.job

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Roaming\GcjiTF.exe

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\GcjiTF.exe
- copy: C:\ProgramData\images.exe

Uses Windows utilities for basic functionality

- command: schtasks.exe /Create /TN "Updates\GcjiTF" /XML
"C:\Users\Seven01\AppData\Local\Temp\tmpB665.tmp"
- command: schtasks.exe /Create /TN "Updates\GcjiTF" /XML
"C:\Users\Seven01\AppData\Local\Temp\tmpFF94.tmp"

A scripting utility was executed

- command: powershell Add-MpPreference -ExclusionPath C:\

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.45, characteristics:
IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size:
0x00056800, virtual_size: 0x000566e4

Drops a binary and executes it

- binary: C:\ProgramData\images.exe

A process created a hidden window

- Process: dafa.exe -> schtasks.exe
- Process: images.exe -> schtasks.exe
- Process: images.exe -> C:\Windows\System32\cmd.exe

Creates RWX memory

Anomalous file deletion behavior detected (10+)

- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\tmpB665.tmp
- DeletedFile:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.2772.32565625
- DeletedFile:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.2772.32565625

- DeletedFile: C:\Users\Seven01\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2772.32565812
- DeletedFile: C:\ProgramData\images.exe:Zone.Identifier
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\c5imzpk3.gop.ps1
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\wyzupo3m.uh4.psm1
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\tmpFF94.tmp
- DeletedFile: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.2624.32586203
- DeletedFile: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.2624.32586203
- DeletedFile: C:\Users\Seven01\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2624.32586218
- DeletedFile: C:\Windows\Temp\CabE499.tmp
- DeletedFile: C:\Windows\Temp\TarE49A.tmp
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\l1luzjsp.oih.ps1
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\olx0tcd1.3xm.psm1

Guard pages use detected - possible anti-debugging.

A process attempted to delay the analysis task.

- Process: svchost.exe tried to sleep 300 seconds, actually delayed analysis time by 0 seconds
- Process: images.exe tried to sleep 353 seconds, actually delayed analysis time by 0 seconds

Loads a driver

- 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: 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/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionAndSpinCount
- DynamicLoader: KERNEL32.dll/IsProcessorFeaturePresent
- DynamicLoader: msvcr7.dll/_set_error_mode
- DynamicLoader: msvcr7.dll/?set_terminate@@YAP6AXXZP6AXXZ@Z
- DynamicLoader: msvcr7.dll/_get_terminate
- DynamicLoader: KERNEL32.dll/FindActCtxSectionStringW
- DynamicLoader: KERNEL32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: mscorwks.dll/SetLoadedByMscoree
- DynamicLoader: mscorwks.dll/_CorExeMain
- DynamicLoader: mscorwks.dll/GetCLRFunction
- DynamicLoader: ADVAPI32.dll/RegisterTraceGuidsW
- DynamicLoader: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: ADVAPI32.dll/GetTraceLoggerHandle
- DynamicLoader: ADVAPI32.dll/GetTraceEnableLevel
- DynamicLoader: ADVAPI32.dll/GetTraceEnableFlags
- DynamicLoader: ADVAPI32.dll/TraceEvent
- DynamicLoader: MSCOREE.DLL/IEE
- DynamicLoader: mscoreei.dll/IEE_RetAddr
- DynamicLoader: mscoreei.dll/IEE
- DynamicLoader: mscorwks.dll/IEE
- DynamicLoader: MSCOREE.DLL/GetStartupFlags
- DynamicLoader: mscoreei.dll/GetStartupFlags_RetAddr
- DynamicLoader: mscoreei.dll/GetStartupFlags
- DynamicLoader: MSCOREE.DLL/GetHostConfigurationFile
- DynamicLoader: mscoreei.dll/GetHostConfigurationFile_RetAddr
- DynamicLoader: mscoreei.dll/GetHostConfigurationFile
- DynamicLoader: mscoreei.dll/GetCORVersion_RetAddr
- DynamicLoader: mscoreei.dll/GetCORVersion
- DynamicLoader: MSCOREE.DLL/GetCORSystemDirectory
- DynamicLoader: mscoreei.dll/GetCORSystemDirectory_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream
- DynamicLoader: ntdll.dll/RtlUnwind
- DynamicLoader: KERNEL32.dll/IsWow64Process



- 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/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/AddVectoredContinueHandler
- DynamicLoader: KERNEL32.dll/RemoveVectoredContinueHandler
- DynamicLoader: ADVAPI32.dll/ConvertSidToStringSidW
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/GetWriteWatch
- DynamicLoader: KERNEL32.dll/ResetWriteWatch
- DynamicLoader: KERNEL32.dll/CreateMemoryResourceNotification
- DynamicLoader: KERNEL32.dll/QueryMemoryResourceNotification
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: KERNEL32.dll/QueryActCtxW
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextA
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptGetHashParam
- DynamicLoader: ADVAPI32.dll/CryptImportKey
- DynamicLoader: ADVAPI32.dll/CryptExportKey
- DynamicLoader: ADVAPI32.dll/CryptGenKey
- DynamicLoader: ADVAPI32.dll/CryptGetKeyParam
- DynamicLoader: ADVAPI32.dll/CryptDestroyKey
- DynamicLoader: ADVAPI32.dll/CryptVerifySignatureA
- DynamicLoader: ADVAPI32.dll/CryptSignHashA
- DynamicLoader: ADVAPI32.dll/CryptGetProvParam
- DynamicLoader: ADVAPI32.dll/CryptGetUserKey
- DynamicLoader: ADVAPI32.dll/CryptEnumProvidersA
- DynamicLoader: MSCOREE.DLL/GetMetaDataInternalInterface
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface_RetAddr
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface
- DynamicLoader: mscorwks.dll/GetMetaDataInternalInterface
- DynamicLoader: mscorjit.dll/getJit
- DynamicLoader: KERNEL32.dll/IsWow64Process
- DynamicLoader: uxtheme.dll/IsAppThemed
- DynamicLoader: uxtheme.dll/IsAppThemedW



- DynamicLoader: KERNEL32.dll/CreateActCtx
- DynamicLoader: KERNEL32.dll/CreateActCtxA
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: USER32.dll/RegisterWindowMessage
- DynamicLoader: USER32.dll/RegisterWindowMessageW
- DynamicLoader: KERNEL32.dll/GetUserDefaultUILanguage
- DynamicLoader: KERNEL32.dll/SetErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: mscoreei.dll/LoadLibraryShim_RetAddr
- DynamicLoader: mscoreei.dll/LoadLibraryShim
- DynamicLoader: culture.dll/ConvertLangIdToCultureName
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptGetProvParam
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptSetKeyParam
- DynamicLoader: CRYPTSP.dll/CryptDecrypt
- DynamicLoader: CRYPTSP.dll/CryptEncrypt
- DynamicLoader: KERNEL32.dll/GlobalMemoryStatusEx
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: KERNEL32.dll/VirtualProtect
- DynamicLoader: shfolder.dll/SHGetFolderPath
- DynamicLoader: shfolder.dll/SHGetFolderPathW
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivilegesW
- DynamicLoader: ADVAPI32.dll/SetNamedSecurityInfoW
- DynamicLoader: ADVAPI32.dll/SetNamedSecurityInfoWW
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: KERNEL32.dll/CopyFile
- DynamicLoader: KERNEL32.dll/CopyFileW
- DynamicLoader: ADVAPI32.dll/GetUserName
- DynamicLoader: ADVAPI32.dll/GetUserNameW
- DynamicLoader: KERNEL32.dll/SetFileAttributes
- DynamicLoader: KERNEL32.dll/SetFileAttributesW
- DynamicLoader: ADVAPI32.dll/LsaClose
- DynamicLoader: ADVAPI32.dll/LsaFreeMemory
- DynamicLoader: ADVAPI32.dll/LsaOpenPolicy
- DynamicLoader: ADVAPI32.dll/LsaOpenPolicyW
- DynamicLoader: ADVAPI32.dll/LsaLookupNames2
- DynamicLoader: ADVAPI32.dll/LsaLookupNames2W
- DynamicLoader: KERNEL32.dll/Istrlen
- DynamicLoader: KERNEL32.dll/IstrlenW
- DynamicLoader: MSCOREE.DLL/ND_RU1
- DynamicLoader: mscoreei.dll/ND_RU1_RetAddr
- DynamicLoader: mscoreei.dll/ND_RU1
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentProcessW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/GetTokenInformationW
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: KERNEL32.dll/LocalAllocW



- DynamicLoader: MSCOREE.DLL/ND_R14
- DynamicLoader: mscoreei.dll/ND_R14_RetAddr
- DynamicLoader: mscoreei.dll/ND_R14
- DynamicLoader: ADVAPI32.dll/LsaLookupSids
- DynamicLoader: ADVAPI32.dll/LsaLookupSidsW
- DynamicLoader: KERNEL32.dll/GetTempPath
- DynamicLoader: KERNEL32.dll/GetTempPathW
- DynamicLoader: KERNEL32.dll/GetTempFileName
- DynamicLoader: KERNEL32.dll/GetTempFileNameW
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: KERNEL32.dll/GetFileType
- DynamicLoader: KERNEL32.dll/WriteFile
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: KERNEL32.dll/RtlMoveMemory
- DynamicLoader: KERNEL32.dll/RtlMoveMemoryW
- 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/CloseHandle
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: ole32.dll/CoWaitForMultipleHandles
- 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: KERNEL32.dll/DeleteFile
- DynamicLoader: KERNEL32.dll/DeleteFileW
- DynamicLoader: KERNEL32.dll/CreateProcess
- DynamicLoader: KERNEL32.dll/CreateProcessW
- 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/LookupPrivilegeValue
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivilegesW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: PSAPI.DLL/EnumProcesses
- DynamicLoader: PSAPI.DLL/EnumProcessesW



- 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: 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: ole32.dll/CoTaskMemAlloc
- DynamicLoader: tschannel.dll/DllGetClassObject
- DynamicLoader: tschannel.dll/DllCanUnloadNow
- DynamicLoader: SHELL32.dll/SHChangeNotify
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: RasApi32.dll/RasEnumConnectionsW
- DynamicLoader: RasApi32.dll/RasConnectionNotificationW
- DynamicLoader: WTSAPI32.dll/WTSQueryUserToken
- 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_RpcExtlInitializeExtensionPoint
- 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: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: WINTRUST.dll/WinVerifyTrust
- DynamicLoader: msdmo.dll/DMOEnum
- DynamicLoader: msdmo.dll/DMOGetTypes
- DynamicLoader: msdmo.dll/DMOGetName
- DynamicLoader: avicap32.dll/capGetDriverDescriptionW
- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CreateBindCtx
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetApartmentType
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoGetMalloc
- DynamicLoader: comctl32.dll/
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: ole32.dll/CoRevokeInitializeSpy



- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: kernel32.dll/FIsAlloc
- DynamicLoader: kernel32.dll/FIsGetValue
- DynamicLoader: kernel32.dll/FIsSetValue
- DynamicLoader: kernel32.dll/FIsFree
- DynamicLoader: kernel32.dll/IsProcessorFeaturePresent
- DynamicLoader: kernel32.dll/IsWow64Process
- 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/CorBindToRuntimeEx_RetAddr
- DynamicLoader: mscoreei.dll/CorBindToRuntimeEx
- 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/DllGetClassObjectInternal
- 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: mscoree.dll/_CorExeMain
- DynamicLoader: mscoree.dll/_CorImageUnloading
- DynamicLoader: mscoree.dll/_CorValidatelmage
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: mscoree.dll/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: OLEAUT32.dll/SysStringByteLen
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/LocaleNameToLCID
- 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: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- 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: ADVAPI32.dll/RegCloseKey
- DynamicLoader: kernel32.dll/GetUserDefaultLocaleName
- DynamicLoader: kernel32.dll/LCIDToLocaleName
- DynamicLoader: kernel32.dll/GetUserPreferredUILanguages
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguages
- DynamicLoader: nlssorting.dll/SortGetHandle
- DynamicLoader: nlssorting.dll/SortCloseHandle
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventSetInformation



- 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/_RpcExtInitializeExtensionPoint
- DynamicLoader: clr.dll/CreateAssemblyEnum
- DynamicLoader: clr.dll/CreateAssemblyEnumW
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/ResolveLocaleName
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: ntdll.dll/NtQueryInformationThread
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: kernel32.dll/CreateWaitableTimerExW
- DynamicLoader: kernel32.dll/SetWaitableTimerEx
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: kernel32.dll/GetCurrentProcessId
- DynamicLoader: kernel32.dll/GetCurrentProcessIdW
- DynamicLoader: ADVAPI32.dll/EventRegister
- 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: VERSION.dll/GetFileVersionInfoSize
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW



- DynamicLoader: VERSION.dll/GetFileVersionInfo
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValue
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: kernel32.dll/LCMapStringEx
- DynamicLoader: VERSION.dll/VerLanguageName
- DynamicLoader: VERSION.dll/VerLanguageNameW
- DynamicLoader: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: kernel32.dll/GetExitCodeProcess
- DynamicLoader: kernel32.dll/GetExitCodeProcessW
- DynamicLoader: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: USER32.dll/EnumWindows
- DynamicLoader: USER32.dll/EnumWindowsW
- DynamicLoader: USER32.dll/GetWindowThreadProcessId
- DynamicLoader: USER32.dll/GetWindowThreadProcessIdW
- DynamicLoader: USER32.dll/GetWindow
- DynamicLoader: USER32.dll/IsWindowVisible
- DynamicLoader: USER32.dll/IsWindowVisibleW
- DynamicLoader: kernel32.dll/CreateFile
- DynamicLoader: kernel32.dll/CreateFileW
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/GetFileType
- DynamicLoader: wintrust.dll/WTGetSignatureInfo
- DynamicLoader: wintrust.dll/WTGetSignatureInfoA
- DynamicLoader: wintrust.dll/_WTGetSignatureInfo@24
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtQuerySystemInformationW
- DynamicLoader: wintrust.dll/WinVerifyTrust
- DynamicLoader: wintrust.dll/WinVerifyTrustW
- DynamicLoader: wintrust.dll/WintrustCertificateTrust
- DynamicLoader: wintrust.dll/SoftpubAuthenticode
- DynamicLoader: wintrust.dll/SoftpubInitialize
- DynamicLoader: wintrust.dll/SoftpubLoadMessage
- DynamicLoader: wintrust.dll/SoftpubLoadSignature
- DynamicLoader: wintrust.dll/SoftpubCheckCert
- DynamicLoader: wintrust.dll/SoftpubCleanup
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: kernel32.dll/WerSetFlags
- DynamicLoader: MSISIP.DLL/DllCanUnloadNow
- DynamicLoader: MSISIP.DLL/MsiSIPsMyTypeOfFile
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: kernel32.dll/SetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/SetThreadPreferredUILanguagesW
- DynamicLoader: wshext.dll/DllCanUnloadNow
- DynamicLoader: wshext.dll/IsFileSupportedName
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguagesW
- DynamicLoader: kernel32.dll/GetUserDefaultLocaleName
- DynamicLoader: kernel32.dll/GetUserDefaultLocaleNameW
- DynamicLoader: pwrshsip.dll/DllCanUnloadNow
- DynamicLoader: pwrshsip.dll/PsIsMyFileType
- DynamicLoader: pwrshsip.dll/PsPutSignature
- DynamicLoader: pwrshsip.dll/PsGetSignature
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetEnvironmentVariable
- DynamicLoader: kernel32.dll/GetEnvironmentVariableW



- DynamicLoader: wintrust.dll/WTHelperProvDataFromStateData
- DynamicLoader: wintrust.dll/WTHelperProvDataFromStateDataW
- DynamicLoader: wintrust.dll/WTHelperGetProvSignerFromChain
- DynamicLoader: wintrust.dll/WTHelperGetProvSignerFromChainW
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: kernel32.dll/GetConsoleCP
- DynamicLoader: kernel32.dll/GetConsoleCPW
- DynamicLoader: kernel32.dll/CreateFile
- DynamicLoader: kernel32.dll/CreateFileW
- DynamicLoader: kernel32.dll/GetCurrentConsoleFontEx
- DynamicLoader: kernel32.dll/GetCurrentConsoleFontExW
- DynamicLoader: kernel32.dll/CreateDirectory
- DynamicLoader: kernel32.dll/CreateDirectoryW
- DynamicLoader: kernel32.dll/GetConsoleScreenBufferInfo
- DynamicLoader: kernel32.dll/GetConsoleScreenBufferInfoW
- DynamicLoader: kernel32.dll/GetConsoleMode
- DynamicLoader: kernel32.dll/GetConsoleModeW
- DynamicLoader: kernel32.dll/SetConsoleMode
- DynamicLoader: kernel32.dll/SetConsoleModeW
- DynamicLoader: kernel32.dll/SetConsoleCtrlHandler
- DynamicLoader: kernel32.dll/SetConsoleCtrlHandlerW
- DynamicLoader: kernel32.dll/GetStdHandle
- DynamicLoader: kernel32.dll/GetConsoleMode
- DynamicLoader: kernel32.dll/GetCurrentProcess
- DynamicLoader: kernel32.dll/GetCurrentProcessW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: kernel32.dll/LocalFree
- 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/GetConsoleTitle
- DynamicLoader: kernel32.dll/GetConsoleTitleW
- DynamicLoader: kernel32.dll/SetConsoleTitle
- DynamicLoader: kernel32.dll/SetConsoleTitleW
- DynamicLoader: kernel32.dll/GetProcessTimes
- DynamicLoader: kernel32.dll/GetProcessTimesW
- DynamicLoader: kernel32.dll/GetDynamicTimeZoneInformation
- 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: ADVAPI32.dll/CreateWellKnownSid
- DynamicLoader: kernel32.dll/CreateNamedPipe
- DynamicLoader: kernel32.dll/CreateNamedPipeW
- DynamicLoader: kernel32.dll/GetFileType
- DynamicLoader: kernel32.dll/CreateEvent
- DynamicLoader: kernel32.dll/CreateEventW
- DynamicLoader: kernel32.dll/ConnectNamedPipe
- DynamicLoader: kernel32.dll/SetEnvironmentVariable
- DynamicLoader: kernel32.dll/SetEnvironmentVariableW
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- 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: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: kernel32.dll/ExpandEnvironmentStrings
- DynamicLoader: kernel32.dll/ExpandEnvironmentStringsW
- DynamicLoader: kernel32.dll/GetModuleHandle
- DynamicLoader: kernel32.dll/GetModuleHandleW
- DynamicLoader: kernel32.dll/GetProcAddress
- DynamicLoader: kernel32.dll/WideCharToMultiByte
- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetTimeZoneInformation
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKey
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyEx
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: secur32.dll/GetUserNameEx
- DynamicLoader: secur32.dll/GetUserNameExW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: ADVAPI32.dll/GetUserName
- DynamicLoader: ADVAPI32.dll/GetUserNameW
- DynamicLoader: kernel32.dll/EnumCalendarInfoExEx
- DynamicLoader: kernel32.dll/GetCalendarInfoEx
- DynamicLoader: kernel32.dll/EnumSystemLocalesEx
- DynamicLoader: kernel32.dll/EnumTimeFormatsEx
- DynamicLoader: kernel32.dll/ReleaseMutex
- DynamicLoader: ADVAPI32.dll/RegisterEventSource
- DynamicLoader: ADVAPI32.dll/RegisterEventSourceW
- DynamicLoader: ADVAPI32.dll/DeregisterEventSource
- DynamicLoader: ADVAPI32.dll/ReportEvent
- DynamicLoader: ADVAPI32.dll/ReportEventW
- DynamicLoader: kernel32.dll/GetLogicalDrives
- DynamicLoader: kernel32.dll/GetDriveType
- DynamicLoader: kernel32.dll/GetDriveTypeW
- DynamicLoader: kernel32.dll/GetVolumeInformation
- DynamicLoader: kernel32.dll/GetVolumeInformationW
- DynamicLoader: SHLWAPI.dll/PathIsNetworkPath
- DynamicLoader: SHLWAPI.dll/PathIsNetworkPathW
- DynamicLoader: shell32.dll/
- DynamicLoader: kernel32.dll/GetFileAttributes
- DynamicLoader: kernel32.dll/GetFileAttributesW
- DynamicLoader: kernel32.dll/GetCurrentDirectory
- DynamicLoader: kernel32.dll/GetCurrentDirectoryW
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetSystemDirectory
- DynamicLoader: kernel32.dll/GetSystemDirectoryW
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: kernel32.dll/GetTempPath



- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ncrypt.dll/BCryptOpenAlgorithmProvider
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: ncrypt.dll/BCryptGetProperty
- DynamicLoader: ncrypt.dll/BCryptCreateHash
- DynamicLoader: ncrypt.dll/BCryptHashData
- DynamicLoader: pwrshsip.dll/PsVerifyHash
- DynamicLoader: ncrypt.dll/BCryptFinishHash
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptSetHashParam
- DynamicLoader: CRYPTSP.dll/CryptVerifySignatureA
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: ncrypt.dll/BCryptDestroyHash
- DynamicLoader: USERENV.dll/GetUserProfileDirectoryW
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: sechost.dll/ConvertStringSidToSidW
- DynamicLoader: USERENV.dll/RegisterGPNotification
- DynamicLoader: GPAPI.dll/RegisterGPNotificationInternal
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: sechost.dll/QueryServiceConfigW
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: cryptnet.dll/I_CryptNetGetConnectivity
- DynamicLoader: SensApi.dll/IsNetworkAlive
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/NdrClientCall2
- DynamicLoader: cryptnet.dll/CryptRetrieveObjectByUrlW
- DynamicLoader: SHLWAPI.dll/UrlGetPartW
- DynamicLoader: WINHTTP.dll/WinHttpOpen
- DynamicLoader: WINHTTP.dll/WinHttpSetTimeouts
- DynamicLoader: WINHTTP.dll/WinHttpSetOption
- DynamicLoader: WINHTTP.dll/WinHttpCrackUrl
- DynamicLoader: SHLWAPI.dll/StrCmpNW
- DynamicLoader: WINHTTP.dll/WinHttpConnect
- DynamicLoader: WINHTTP.dll/WinHttpOpenRequest
- DynamicLoader: WINHTTP.dll/WinHttpGetDefaultProxyConfiguration
- DynamicLoader: WINHTTP.dll/WinHttpGetIEProxyConfigForCurrentUser
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: profapi.dll/
- 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/WinHttpQueryDataAvailable
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WINHTTP.dll/WinHttpReadData
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WINHTTP.dll/WinHttpCloseHandle
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceConfigA
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeA
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingA
- DynamicLoader: RPCRT4.dll/RpcEpResolveBinding
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/RpcStringFreeA
- DynamicLoader: RPCRT4.dll/NdrClientCall2
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: CRYPTSP.dll/CryptGetKeyParam
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: cryptnet.dll/DllCanUnloadNow
- DynamicLoader: cryptnet.dll/CertDllVerifyRevocation
- DynamicLoader: ADVAPI32.dll/SaferiSearchMatchingHashRules
- DynamicLoader: wintrust.dll/WTHelperGetProvCertFromChain
- DynamicLoader: wintrust.dll/WTHelperGetProvCertFromChainW
- DynamicLoader: CRYPT32.dll/CertFreeCertificateContext
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContext
- DynamicLoader: CRYPT32.dll/CertGetCertificateContextProperty
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContext
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContextW
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: ADVAPI32.dll/EventUnregister
- 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: CRYPT32.dll/CertFreeCertificateContext
- DynamicLoader: diasymreader.dll/DllGetClassObject
- DynamicLoader: kernel32.dll/GetLastError
- DynamicLoader: kernel32.dll/LocalAlloc
- DynamicLoader: kernel32.dll/GetConsoleOutputCP
- DynamicLoader: kernel32.dll/GetConsoleOutputCPW
- DynamicLoader: GDI32.dll/TranslateCharsetInfo
- DynamicLoader: GDI32.dll/TranslateCharsetInfoW
- DynamicLoader: kernel32.dll/SetConsoleTextAttribute
- DynamicLoader: kernel32.dll/SetConsoleTextAttributeW
- DynamicLoader: kernel32.dll/WriteConsole
- DynamicLoader: kernel32.dll/WriteConsoleW
- DynamicLoader: kernel32.dll/GetModuleFileName
- DynamicLoader: kernel32.dll/GetModuleFileNameW
- DynamicLoader: kernel32.dll/GetFileAttributesEx
- DynamicLoader: kernel32.dll/GetFileAttributesExW
- DynamicLoader: kernel32.dll/GetFileSize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: mscoree.dll/CorExitProcess



- DynamicLoader: mscoreei.dll/CorExitProcess_RetAddr
- DynamicLoader: mscoreei.dll/CorExitProcess
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: clr.dll/_CorDllMain
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- 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/GetCurrentPkgageld
- 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/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionAndSpinCount
- DynamicLoader: KERNEL32.dll/IsProcessorFeaturePresent
- DynamicLoader: msvcrtdll/_set_error_mode
- DynamicLoader: msvcrtdll/?set_terminate@@YAP6AXXZP6AXXZ@Z
- DynamicLoader: msvcrtdll/_get_terminate
- DynamicLoader: KERNEL32.dll/FindActCtxSectionStringW
- DynamicLoader: KERNEL32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: mscorwks.dll/SetLoadedByMscoree
- DynamicLoader: mscorwks.dll/_CorExeMain
- DynamicLoader: mscorwks.dll/GetCLRFunction
- DynamicLoader: ADVAPI32.dll/RegisterTraceGuidsW
- DynamicLoader: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: ADVAPI32.dll/GetTraceLoggerHandle
- DynamicLoader: ADVAPI32.dll/GetTraceEnableLevel
- DynamicLoader: ADVAPI32.dll/GetTraceEnableFlags
- DynamicLoader: ADVAPI32.dll/TraceEvent
- DynamicLoader: MSCOREE.DLL/IEE
- DynamicLoader: mscoreei.dll/IEE_RetAddr
- DynamicLoader: mscoreei.dll/IEE
- DynamicLoader: mscorwks.dll/IEE
- DynamicLoader: MSCOREE.DLL/GetStartupFlags
- DynamicLoader: mscoreei.dll/GetStartupFlags_RetAddr
- DynamicLoader: mscoreei.dll/GetStartupFlags
- DynamicLoader: MSCOREE.DLL/GetHostConfigurationFile
- DynamicLoader: mscoreei.dll/GetHostConfigurationFile_RetAddr
- DynamicLoader: mscoreei.dll/GetHostConfigurationFile
- DynamicLoader: mscoreei.dll/GetCORVersion_RetAddr
- DynamicLoader: mscoreei.dll/GetCORVersion
- DynamicLoader: MSCOREE.DLL/GetCORSystemDirectory
- DynamicLoader: mscoreei.dll/GetCORSystemDirectory_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream
- DynamicLoader: ntdll.dll/RtlUnwind
- DynamicLoader: KERNEL32.dll/IsWow64Process
- 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/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/AddVectoredContinueHandler
- DynamicLoader: KERNEL32.dll/RemoveVectoredContinueHandler
- DynamicLoader: ADVAPI32.dll/ConvertSidToStringSidW



- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/GetWriteWatch
- DynamicLoader: KERNEL32.dll/ResetWriteWatch
- DynamicLoader: KERNEL32.dll/CreateMemoryResourceNotification
- DynamicLoader: KERNEL32.dll/QueryMemoryResourceNotification
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: KERNEL32.dll/QueryActCtxW
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextA
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptGetHashParam
- DynamicLoader: ADVAPI32.dll/CryptImportKey
- DynamicLoader: ADVAPI32.dll/CryptExportKey
- DynamicLoader: ADVAPI32.dll/CryptGenKey
- DynamicLoader: ADVAPI32.dll/CryptGetKeyParam
- DynamicLoader: ADVAPI32.dll/CryptDestroyKey
- DynamicLoader: ADVAPI32.dll/CryptVerifySignatureA
- DynamicLoader: ADVAPI32.dll/CryptSignHashA
- DynamicLoader: ADVAPI32.dll/CryptGetProvParam
- DynamicLoader: ADVAPI32.dll/CryptGetUserKey
- DynamicLoader: ADVAPI32.dll/CryptEnumProvidersA
- DynamicLoader: MSCOREE.DLL/GetMetaDataInternalInterface
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface_RetAddr
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface
- DynamicLoader: mscorwks.dll/GetMetaDataInternalInterface
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: mscorjit.dll/getJit
- DynamicLoader: KERNEL32.dll/IsWow64Process
- DynamicLoader: uxtheme.dll/IsAppThemed
- DynamicLoader: uxtheme.dll/IsAppThemedW
- DynamicLoader: KERNEL32.dll/CreateActCtx
- DynamicLoader: KERNEL32.dll/CreateActCtxA
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: USER32.dll/RegisterWindowMessage
- DynamicLoader: USER32.dll/RegisterWindowMessageW
- DynamicLoader: KERNEL32.dll/GetUserDefaultUILanguage
- DynamicLoader: KERNEL32.dll/SetErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: mscoreei.dll/LoadLibraryShim_RetAddr
- DynamicLoader: mscoreei.dll/LoadLibraryShim
- DynamicLoader: culture.dll/ConvertLangIdToCultureName
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptGetProvParam
- DynamicLoader: CRYPTSP.dll/CryptGenRandom



- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptSetKeyParam
- DynamicLoader: CRYPTSP.dll/CryptDecrypt
- DynamicLoader: CRYPTSP.dll/CryptEncrypt
- DynamicLoader: KERNEL32.dll/GlobalMemoryStatusEx
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: KERNEL32.dll/VirtualProtect
- DynamicLoader: shfolder.dll/SHGetFolderPath
- DynamicLoader: shfolder.dll/SHGetFolderPathW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentProcessW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/GetTokenInformationW
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: KERNEL32.dll/LocalAllocW
- DynamicLoader: KERNEL32.dll/lstrlen
- DynamicLoader: KERNEL32.dll/lstrlenW
- DynamicLoader: MSCOREE.DLL/ND_R14
- DynamicLoader: mscoreei.dll/ND_R14_RetAddr
- DynamicLoader: mscoreei.dll/ND_R14
- DynamicLoader: MSCOREE.DLL/ND_RU1
- DynamicLoader: mscoreei.dll/ND_RU1_RetAddr
- DynamicLoader: mscoreei.dll/ND_RU1
- DynamicLoader: ADVAPI32.dll/LsaClose
- DynamicLoader: ADVAPI32.dll/LsaFreeMemory
- DynamicLoader: ADVAPI32.dll/LsaOpenPolicy
- DynamicLoader: ADVAPI32.dll/LsaOpenPolicyW
- DynamicLoader: ADVAPI32.dll/LsaLookupSids
- DynamicLoader: ADVAPI32.dll/LsaLookupSidsW
- DynamicLoader: KERNEL32.dll/GetTempPath
- DynamicLoader: KERNEL32.dll/GetTempPathW
- DynamicLoader: KERNEL32.dll/GetTempFileName
- DynamicLoader: KERNEL32.dll/GetTempFileNameW
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: KERNEL32.dll/GetFileType
- DynamicLoader: KERNEL32.dll/WriteFile
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: KERNEL32.dll/RtlMoveMemory
- DynamicLoader: KERNEL32.dll/RtlMoveMemoryW
- 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: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: ole32.dll/CoWaitForMultipleHandles
- 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: KERNEL32.dll/DeleteFile
- DynamicLoader: KERNEL32.dll/DeleteFileW
- DynamicLoader: KERNEL32.dll/CreateProcess
- DynamicLoader: KERNEL32.dll/CreateProcessW
- 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/LookupPrivilegeValue
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivilegesW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: PSAPI.DLL/EnumProcesses
- DynamicLoader: PSAPI.DLL/EnumProcessesW
- 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/FIsAlloc
- DynamicLoader: kernel32.dll/FIsGetValue
- DynamicLoader: kernel32.dll/FIsSetValue
- DynamicLoader: kernel32.dll/FIsFree
- DynamicLoader: kernel32.dll/IsProcessorFeaturePresent
- DynamicLoader: kernel32.dll/IsWow64Process
- 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: schannel.dll/SpUserModelInitialize
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: WS2_32.dll/WSASend
- DynamicLoader: WS2_32.dll/WSARecv
- DynamicLoader: secur32.dll/FreeContextBuffer
- DynamicLoader: ncrypt.dll/SslOpenProvider



- DynamicLoader: ncrypt.dll/GetSChannelInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: ncrypt.dll/SslIncrementProviderReferenceCount
- DynamicLoader: ncrypt.dll/SslImportKey
- DynamicLoader: bcryptprimitives.dll/GetCipherInterface
- DynamicLoader: ncrypt.dll/SslLookupCipherSuiteInfo
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ncrypt.dll/BCryptOpenAlgorithmProvider
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: ncrypt.dll/BCryptGetProperty
- DynamicLoader: ncrypt.dll/BCryptCreateHash
- DynamicLoader: ncrypt.dll/BCryptHashData
- DynamicLoader: ncrypt.dll/BCryptFinishHash
- DynamicLoader: ncrypt.dll/BCryptDestroyHash
- DynamicLoader: CRYPT32.dll/CertGetCertificateChain
- DynamicLoader: USERENV.dll/GetUserProfileDirectoryW
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: sechost.dll/ConvertStringSidToSidW
- DynamicLoader: USERENV.dll/RegisterGPNotification
- DynamicLoader: GPAPI.dll/RegisterGPNotificationInternal
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: sechost.dll/QueryServiceConfigW
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptVerifySignatureA
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: cryptnet.dll/I_CryptNetGetConnectivity
- DynamicLoader: SensApi.dll/IsNetworkAlive
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/NdrClientCall2
- DynamicLoader: cryptnet.dll/CryptRetrieveObjectByUrlW
- DynamicLoader: SHLWAPI.dll/UrlGetPartW
- DynamicLoader: WINHTTP.dll/WinHttpOpen
- DynamicLoader: WINHTTP.dll/WinHttpSetTimeouts
- DynamicLoader: WINHTTP.dll/WinHttpSetOption
- DynamicLoader: WINHTTP.dll/WinHttpCrackUrl
- DynamicLoader: WINHTTP.dll/WinHttpConnect
- DynamicLoader: WINHTTP.dll/WinHttpOpenRequest
- DynamicLoader: WINHTTP.dll/WinHttpGetDefaultProxyConfiguration
- DynamicLoader: WINHTTP.dll/WinHttpGetIEProxyConfigForCurrentUser
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ADVAPI32.dll/RegDeleteTreeA
- DynamicLoader: ADVAPI32.dll/RegDeleteTreeW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: NSI.dll/NsiAllocateAndGetTable
- DynamicLoader: CFGMGR32.dll/CM_Open_Class_Key_ExW
- DynamicLoader: IPHLPAPI.DLL/ConvertInterfaceGuidToLuid
- DynamicLoader: IPHLPAPI.DLL/GetIfEntry2
- DynamicLoader: IPHLPAPI.DLL/GetIpForwardTable2
- DynamicLoader: IPHLPAPI.DLL/GetIpNetEntry2
- DynamicLoader: IPHLPAPI.DLL/FreeMibTable
- DynamicLoader: ole32.dll/CoTaskMemFree



- DynamicLoader: NSI.dll/NsiFreeTable
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: WINHTTP.dll/WinHttpGetProxyForUrl
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: profapi.dll/
- DynamicLoader: ADVAPI32.dll/RegDeleteTreeA
- DynamicLoader: ADVAPI32.dll/RegDeleteTreeW
- DynamicLoader: WINHTTP.dll/WinHttpSendRequest
- DynamicLoader: WINHTTP.dll/WinHttpReceiveResponse
- DynamicLoader: WINHTTP.dll/WinHttpQueryHeaders
- DynamicLoader: WINHTTP.dll/WinHttpQueryDataAvailable
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WINHTTP.dll/WinHttpReadData
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WINHTTP.dll/WinHttpCloseHandle
- DynamicLoader: setupapi.dll/SetupIterateCabinetW
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: Cabinet.dll/
- DynamicLoader: Cabinet.dll/
- DynamicLoader: Cabinet.dll/
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceConfigA
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeA
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingA
- DynamicLoader: RPCRT4.dll/RpcEpResolveBinding
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: RPCRT4.dll/RpcStringFreeA
- DynamicLoader: RPCRT4.dll/NdrClientCall2
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: CRYPTSP.dll/CryptGetKeyParam
- DynamicLoader: CRYPT32.dll/CertVerifyCertificateChainPolicy
- DynamicLoader: CRYPT32.dll/CertFreeCertificateChain
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContext
- DynamicLoader: CRYPT32.dll/CertFreeCertificateContext
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- 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: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: WINTRUST.dll/WinVerifyTrust
- DynamicLoader: msdmo.dll/DMOEnum
- DynamicLoader: msdmo.dll/DMOGetTypes
- DynamicLoader: msdmo.dll/DMOGetName



- DynamicLoader: avicap32.dll/capGetDriverDescriptionW
- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: ntdll.dll/RtlNtStatusToDosError
- DynamicLoader: ntdll.dll/RtlSetLastWin32Error
- 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/CorBindToRuntimeEx_RetAddr
- DynamicLoader: mscoreei.dll/CorBindToRuntimeEx
- 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/DllGetClassObjectInternal
- 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: mscoree.dll/_CorExeMain
- DynamicLoader: mscoree.dll/_CorImageUnloading
- DynamicLoader: mscoree.dll/_CorValidateImage
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: mscoree.dll/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: OLEAUT32.dll/SysStringByteLen
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/LocaleNameToLCID
- 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: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- 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/RegCloseKey
- DynamicLoader: kernel32.dll/GetUserDefaultLocaleName
- DynamicLoader: kernel32.dll/LCIDToLocaleName
- DynamicLoader: kernel32.dll/GetUserPreferredUILanguages
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguages
- DynamicLoader: nlssorting.dll/SortGetHandle
- DynamicLoader: nlssorting.dll/SortCloseHandle
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx



- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- 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: ntdll.dll/NtQueryInformationThread
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: kernel32.dll/CreateWaitableTimerExW
- DynamicLoader: kernel32.dll/SetWaitableTimerEx
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: VERSION.dll/GetFileVersionInfoSize
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfo
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValue
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: kernel32.dll/LCMapStringEx
- DynamicLoader: VERSION.dll/VerLanguageName
- DynamicLoader: VERSION.dll/VerLanguageNameW
- 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/CreateFile
- DynamicLoader: kernel32.dll/CreateFileW
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/GetFileType
- DynamicLoader: wintrust.dll/WTGetSignatureInfo



- DynamicLoader: wintrust.dll/WTGetSignatureInfoA
- DynamicLoader: wintrust.dll/_WTGetSignatureInfo@24
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: wintrust.dll/WinVerifyTrust
- DynamicLoader: wintrust.dll/WinVerifyTrustW
- DynamicLoader: wintrust.dll/WintrustCertificateTrust
- DynamicLoader: wintrust.dll/SoftpubAuthenticCode
- DynamicLoader: wintrust.dll/SoftpubInitialize
- DynamicLoader: wintrust.dll/SoftpubLoadMessage
- DynamicLoader: wintrust.dll/SoftpubLoadSignature
- DynamicLoader: wintrust.dll/SoftpubCheckCert
- DynamicLoader: wintrust.dll/SoftpubCleanup
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: MSISIP.DLL/DllCanUnloadNow
- DynamicLoader: MSISIP.DLL/MsiSIPsMyTypeOfFile
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: wshext.dll/DllCanUnloadNow
- DynamicLoader: wshext.dll/IsFileSupportedName
- DynamicLoader: pwrshsip.dll/DllCanUnloadNow
- DynamicLoader: pwrshsip.dll/PsIsMyFileType
- DynamicLoader: pwrshsip.dll/PsPutSignature
- DynamicLoader: pwrshsip.dll/PsGetSignature
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetEnvironmentVariable
- DynamicLoader: kernel32.dll/GetEnvironmentVariableW
- DynamicLoader: wintrust.dll/WTHelperProvDataFromStateData
- DynamicLoader: wintrust.dll/WTHelperProvDataFromStateDataW
- DynamicLoader: wintrust.dll/WTHelperGetProvSignerFromChain
- DynamicLoader: wintrust.dll/WTHelperGetProvSignerFromChainW
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ole32.dll/CoTaskMemFree
- 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: psapi.dll/GetModuleFileNameEx
- DynamicLoader: psapi.dll/GetModuleFileNameExW
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: kernel32.dll/GetExitCodeProcess
- DynamicLoader: kernel32.dll/GetExitCodeProcessW
- DynamicLoader: USER32.dll/EnumWindows
- DynamicLoader: USER32.dll/EnumWindowsW
- DynamicLoader: USER32.dll/GetWindowThreadProcessId
- DynamicLoader: USER32.dll/GetWindowThreadProcessIdW
- DynamicLoader: USER32.dll/GetWindow
- DynamicLoader: USER32.dll/IsWindowVisible



- DynamicLoader: USER32.dll/IsWindowVisibleW
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtQuerySystemInformationW
- DynamicLoader: kernel32.dll/WerSetFlags
- DynamicLoader: kernel32.dll/SetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/SetThreadPreferredUILanguagesW
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguagesW
- DynamicLoader: kernel32.dll/GetUserDefaultLocaleName
- DynamicLoader: kernel32.dll/GetUserDefaultLocaleNameW
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: kernel32.dll/GetConsoleCP
- DynamicLoader: kernel32.dll/GetConsoleCPW
- DynamicLoader: kernel32.dll/CreateFile
- DynamicLoader: kernel32.dll/CreateFileW
- DynamicLoader: kernel32.dll/GetCurrentConsoleFontEx
- DynamicLoader: kernel32.dll/GetCurrentConsoleFontExW
- DynamicLoader: kernel32.dll/GetConsoleScreenBufferInfo
- DynamicLoader: kernel32.dll/GetConsoleScreenBufferInfoW
- DynamicLoader: kernel32.dll/GetConsoleMode
- DynamicLoader: kernel32.dll/GetConsoleModeW
- DynamicLoader: kernel32.dll/SetConsoleMode
- DynamicLoader: kernel32.dll/SetConsoleModeW
- DynamicLoader: kernel32.dll/GetCurrentProcess
- DynamicLoader: kernel32.dll/GetCurrentProcessW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: kernel32.dll/LocalFree
- 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/SetConsoleCtrlHandler
- DynamicLoader: kernel32.dll/SetConsoleCtrlHandlerW
- DynamicLoader: kernel32.dll/GetStdHandle
- DynamicLoader: kernel32.dll/GetConsoleMode
- DynamicLoader: kernel32.dll/GetConsoleTitle
- DynamicLoader: kernel32.dll/GetConsoleTitleW
- DynamicLoader: kernel32.dll/SetConsoleTitle
- DynamicLoader: kernel32.dll/SetConsoleTitleW
- DynamicLoader: kernel32.dll/GetProcessTimes
- DynamicLoader: kernel32.dll/GetProcessTimesW
- DynamicLoader: kernel32.dll/GetDynamicTimeZoneInformation
- 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: ADVAPI32.dll/CreateWellKnownSid
- DynamicLoader: kernel32.dll/CreateNamedPipe
- DynamicLoader: kernel32.dll/CreateNamedPipeW
- DynamicLoader: kernel32.dll/GetFileType
- DynamicLoader: kernel32.dll/CreateEvent
- DynamicLoader: kernel32.dll/CreateEventW
- DynamicLoader: kernel32.dll/ConnectNamedPipe
- DynamicLoader: kernel32.dll/SetEnvironmentVariable
- DynamicLoader: kernel32.dll/SetEnvironmentVariableW
- DynamicLoader: kernel32.dll/GetNativeSystemInfo



- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- 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: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: kernel32.dll/ExpandEnvironmentStrings
- DynamicLoader: kernel32.dll/ExpandEnvironmentStringsW
- DynamicLoader: kernel32.dll/GetModuleHandle
- DynamicLoader: kernel32.dll/GetModuleHandleW
- DynamicLoader: kernel32.dll/GetProcAddress
- DynamicLoader: kernel32.dll/WideCharToMultiByte
- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetTimeZoneInformation
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKey
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyEx
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: secur32.dll/GetUserNameEx
- DynamicLoader: secur32.dll/GetUserNameExW
- DynamicLoader: ADVAPI32.dll/GetUserName
- DynamicLoader: ADVAPI32.dll/GetUserNameW
- DynamicLoader: kernel32.dll/EnumCalendarInfoExEx
- DynamicLoader: kernel32.dll/GetCalendarInfoEx
- DynamicLoader: kernel32.dll/EnumSystemLocalesEx
- DynamicLoader: kernel32.dll/EnumTimeFormatsEx
- DynamicLoader: kernel32.dll/ReleaseMutex
- DynamicLoader: ADVAPI32.dll/RegisterEventSource
- DynamicLoader: ADVAPI32.dll/RegisterEventSourceW
- DynamicLoader: ADVAPI32.dll/DeregisterEventSource
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: ADVAPI32.dll/ReportEvent
- DynamicLoader: ADVAPI32.dll/ReportEventW
- DynamicLoader: kernel32.dll/GetLogicalDrives
- DynamicLoader: kernel32.dll/GetDriveType
- DynamicLoader: kernel32.dll/GetDriveTypeW
- DynamicLoader: kernel32.dll/GetVolumeInformation
- DynamicLoader: kernel32.dll/GetVolumeInformationW
- DynamicLoader: SHLWAPI.dll/PathIsNetworkPath
- DynamicLoader: SHLWAPI.dll/PathIsNetworkPathW
- DynamicLoader: shell32.dll/
- DynamicLoader: kernel32.dll/GetFileAttributes
- DynamicLoader: kernel32.dll/GetFileAttributesW
- DynamicLoader: kernel32.dll/GetCurrentDirectory
- DynamicLoader: kernel32.dll/GetCurrentDirectoryW
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetSystemDirectory
- DynamicLoader: kernel32.dll/GetSystemDirectoryW

- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: ole32.dll/CoInitialize
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ncrypt.dll/BCryptOpenAlgorithmProvider
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: ncrypt.dll/BCryptGetProperty
- DynamicLoader: ncrypt.dll/BCryptCreateHash
- DynamicLoader: ncrypt.dll/BCryptHashData
- DynamicLoader: pwrshsip.dll/PsVerifyHash
- DynamicLoader: ncrypt.dll/BCryptFinishHash
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptSetHashParam
- DynamicLoader: CRYPTSP.dll/CryptVerifySignatureA
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: ncrypt.dll/BCryptDestroyHash
- DynamicLoader: USERENV.dll/GetUserProfileDirectoryW
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: sechost.dll/ConvertStringSidToSidW
- DynamicLoader: USERENV.dll/RegisterGPNotification
- DynamicLoader: GPAPI.dll/RegisterGPNotificationInternal
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: sechost.dll/QueryServiceConfigW
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: cryptnet.dll/I_CryptNetGetConnectivity
- DynamicLoader: SensApi.dll/IsNetworkAlive
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/NdrClientCall2
- DynamicLoader: cryptnet.dll/CryptRetrieveObjectByUrlW
- DynamicLoader: SHLWAPI.dll/UrlGetPartW
- DynamicLoader: WINHTTP.dll/WinHttpOpen
- DynamicLoader: WINHTTP.dll/WinHttpSetTimeouts
- DynamicLoader: WINHTTP.dll/WinHttpSetOption
- DynamicLoader: WINHTTP.dll/WinHttpCrackUrl
- DynamicLoader: SHLWAPI.dll/StrCmpNW
- DynamicLoader: WINHTTP.dll/WinHttpConnect
- DynamicLoader: WINHTTP.dll/WinHttpOpenRequest
- DynamicLoader: WINHTTP.dll/WinHttpGetDefaultProxyConfiguration
- DynamicLoader: WINHTTP.dll/WinHttpGetIEProxyConfigForCurrentUser
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: profapi.dll/
- 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/WinHttpQueryDataAvailable
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WINHTTP.dll/WinHttpReadData
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WINHTTP.dll/WinHttpCloseHandle
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceConfigA
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeA
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingA
- DynamicLoader: RPCRT4.dll/RpcEpResolveBinding
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/RpcStringFreeA
- DynamicLoader: RPCRT4.dll/NdrClientCall2
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: CRYPTSP.dll/CryptGetKeyParam
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: cryptnet.dll/DllCanUnloadNow
- DynamicLoader: cryptnet.dll/CertDllVerifyRevocation
- DynamicLoader: ADVAPI32.dll/SaferiSearchMatchingHashRules
- DynamicLoader: wintrust.dll/WTHelperGetProvCertFromChain
- DynamicLoader: wintrust.dll/WTHelperGetProvCertFromChainW
- DynamicLoader: CRYPT32.dll/CertFreeCertificateContext
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContext
- DynamicLoader: CRYPT32.dll/CertGetCertificateContextProperty
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContext
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContextW
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: ADVAPI32.dll/EventUnregister
- 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: CRYPT32.dll/CertFreeCertificateContext
- DynamicLoader: diasymreader.dll/DllGetClassObject
- DynamicLoader: kernel32.dll/GetLastError
- DynamicLoader: kernel32.dll/LocalAlloc
- DynamicLoader: kernel32.dll/GetConsoleOutputCP
- DynamicLoader: kernel32.dll/GetConsoleOutputCPW
- DynamicLoader: GDI32.dll/TranslateCharsetInfo
- DynamicLoader: GDI32.dll/TranslateCharsetInfoW
- DynamicLoader: kernel32.dll/SetConsoleTextAttribute
- DynamicLoader: kernel32.dll/SetConsoleTextAttributeW
- DynamicLoader: kernel32.dll/WriteConsole
- DynamicLoader: kernel32.dll/WriteConsoleW
- DynamicLoader: kernel32.dll/GetModuleFileName
- DynamicLoader: kernel32.dll/GetModuleFileNameW
- DynamicLoader: kernel32.dll/GetFileAttributesEx
- DynamicLoader: kernel32.dll/GetFileAttributesExW
- DynamicLoader: kernel32.dll/GetFileSize



- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: mscoree.dll/CorExitProcess
- DynamicLoader: mscoreei.dll/CorExitProcess_RetAddr
- DynamicLoader: mscoreei.dll/CorExitProcess
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: clr.dll/_CorDllMain
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: kernel32.dll/SetThreadUILanguage
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: kernel32.dll/CopyFileExW
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: kernel32.dll/SetConsoleInputExeNameW
- 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: CRYPTBASE.dll/SystemFunction036
- 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: PSAPI.DLL/EnumProcesses
- DynamicLoader: PSAPI.DLL/EnumProcessModules
- DynamicLoader: PSAPI.DLL/GetModuleBaseNameW
- DynamicLoader: iphlpapi.dll/GetAdaptersAddresses
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: RPCRT4.dll/RpcServerUnregisterIf
- 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: 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: ikeext.dll/IkeServiceMain
- DynamicLoader: ikeext.dll/SvchostPushServiceGlobals



- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ncrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: ADVAPI32.dll/RegNotifyChangeKeyValue
- DynamicLoader: ncrypt.dll/BCryptOpenAlgorithmProvider
- DynamicLoader: bcryptprimitives.dll/GetCipherInterface
- DynamicLoader: ncrypt.dll/BCryptSetProperty
- DynamicLoader: bcryptprimitives.dll/GetCipherInterface
- DynamicLoader: bcryptprimitives.dll/GetCipherInterface
- DynamicLoader: bcryptprimitives.dll/GetSecretAgreementInterface
- DynamicLoader: bcryptprimitives.dll/GetSecretAgreementInterface
- DynamicLoader: bcryptprimitives.dll/GetSecretAgreementInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: ncrypt.dll/BCryptGenRandom
- DynamicLoader: bcryptprimitives.dll/GetRngInterface
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcBindingCreateW
- DynamicLoader: RPCRT4.dll/RpcBindingBind
- DynamicLoader: RPCRT4.dll/I_RpcMapWin32Status
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: ADVAPI32.dll/AuditQuerySystemPolicy
- DynamicLoader: ADVAPI32.dll/AuditFree
- DynamicLoader: IPHLPAPI.DLL/GetAdaptersAddresses
- DynamicLoader: IPHLPAPI.DLL/NotifyIpInterfaceChange
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: vpnikeapi.dll/GetIDPayload
- DynamicLoader: vpnikeapi.dll/FreeIDPayloadBuffer
- DynamicLoader: AUTHZ.dll/AuthzInitializeResourceManager
- DynamicLoader: ADVAPI32.dll/OpenThreadToken
- DynamicLoader: sechost.dll/ConvertStringSecurityDescriptorToSecurityDescriptorW
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- 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: 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: 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: 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: SspiCli.dll/LsaRegisterLogonProcess
- DynamicLoader: SspiCli.dll/LsaLookupAuthenticationPackage
- DynamicLoader: SspiCli.dll/LsaCallAuthenticationPackage
- DynamicLoader: SspiCli.dll/LsaDeregisterLogonProcess
- DynamicLoader: SspiCli.dll/LsaRegisterPolicyChangeNotification
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: netutils.dll/NetpwPathType
- DynamicLoader: SspiCli.dll/LsaUnregisterPolicyChangeNotification
- 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/FIsGetValue
- 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: 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: sechost.dll/LookupAccountSidLocalW
- 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: 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/RegSetValueExW
- 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: kernel32.dll/OpenProcessToken
- DynamicLoader: KERNELBASE.dll/GetTokenInformation
- DynamicLoader: KERNELBASE.dll/DuplicateTokenEx
- DynamicLoader: KERNELBASE.dll/AdjustTokenPrivileges
- DynamicLoader: KERNELBASE.dll/AllocateAndInitializeSid
- DynamicLoader: KERNELBASE.dll/CheckTokenMembership
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: kernel32.dll/SetThreadToken
- DynamicLoader: ole32.dll/CLSIDFromString
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: wbemcore.dll/Reinitialize
- 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: wbemcore.dll/Reinitialize
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: ole32.dll/CoImpersonateClient
- DynamicLoader: ole32.dll/CoRevertToSelf
- 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: wbemcore.dll/Reinitialize
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- 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: aelupsvc.dll/ServiceMain
- DynamicLoader: aelupsvc.dll/SvchostPushServiceGlobals
- DynamicLoader: apphelp.dll/ApphelpCheckRunAppEx
- DynamicLoader: apphelp.dll/ApphelpCheckRunAppEx
- 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/

At least one IP Address, Domain, or File Name was found in a crypto call

- ioc: inetsim.org0

Expresses interest in specific running processes

- process: explorer.exe



Repeatedly searches for a not-found process, may want to run with startbrowser=1 option

Attempts to connect to a dead IP:Port (3 unique times)

- IP: 192.168.56.1:443
- IP: 192.168.56.1:80
- IP: 192.168.56.1:5201

SetUnhandledExceptionFilter detected (possible anti-debug)