

orgn.exe

Is DLL

Packer

Anti Debug

Anti VM

Signed

XOR

MalFamily: Ispy


MalScore: 100

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	835.00 KB (855040 bytes)
Compile time:	2019-08-15 19:25:29
MD5:	b93c7f4dc1e9b7db8cea5c6a6d83b641
SHA1:	f73b7a0ffb07708f50677add9fe2d24c6ea19b53
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2019-10-02 16:36:05

URL(s) file hosting

<http://alwetengroup.com/orgn.exe>

Antivirus Report

Report date	Detection Ratio	Permalink
2019-10-02 00:49:11	34/67	

Import library

mscoree.dll

14

Behaviors detected by system signatures

Harvests information related to installed mail clients

- file: C:\Users\Seven01\AppData\Local\Microsoft\Windows Live Mail*.oeaccount



```
- file: C:\Users\Seven01\AppData\Local\Microsoft\Windows Live Mail\*.*
```

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7d19c9e894f20d4780a31c9a9f17da11
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\192e64c97bf3a54488a039619c763627
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\00471e98b7a362469ed97e3915fd4111
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\32a3dc9c400a4b448b60ab7fe553a392
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\818ecc2f310b344f807e8af5dc013189
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\HTTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\IMAP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\43e0bb79f0f2d84db98ff4f730d23d24
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7760e21103136b47946c9c80fa097f15
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP User

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\6a50d9bd87f9a8478751861a1591a6c2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\86ed2903a4a11cfb57e524153480001
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\10b0e4d6eb1de34dabd532a0806a0fec
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c0000000000046
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ddb0922fc50b8d42be5a821ede840761
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\IMAP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\SMTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\HTTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c0000000000046
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\SMTP User
- key:
HKEY_CURRENT_USER\Identities\{141B4688-D8D4-4AD1-B583-99828374C040}\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts
- key: HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts
- key: HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts
- key:
HKEY_CURRENT_USER\Identities\{141B4688-D8D4-4AD1-B583-99828374C040}\Software\Microsoft\Internet Account Manager\Accounts

Harvests information related to installed instant messenger clients

- key: HKEY_CURRENT_USER\Software\Google\Google Talk\Accounts

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

Exhibits behavior characteristic of iSpy Keylogger

Steals private information from local Internet browsers

- file: C:\Users\Seven01\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

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

- Spam: services.exe (480) called API GetSystemTimeAsFileTime 2416825 times

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

- Injection: RegAsm.exe(2972) -> vbc.exe(2140)

Anomalous .NET characteristics

- anomalous_version: Assembly version is set to 0

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.59, characteristics:
IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size:
0x000cc400, virtual_size: 0x000cc274

Dynamic (imported) function loading detected

- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionEx
- DynamicLoader: KERNEL32.dll/CreateEventExW
- DynamicLoader: KERNEL32.dll/CreateSemaphoreExW
- DynamicLoader: KERNEL32.dll/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/CreateThreadpoolTimer
- DynamicLoader: KERNEL32.dll/SetThreadpoolTimer
- DynamicLoader: KERNEL32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: KERNEL32.dll/CloseThreadpoolTimer
- DynamicLoader: KERNEL32.dll/CreateThreadpoolWait
- DynamicLoader: KERNEL32.dll/SetThreadpoolWait
- DynamicLoader: KERNEL32.dll/CloseThreadpoolWait
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: KERNEL32.dll/GetCurrentProcessorNumber
- DynamicLoader: KERNEL32.dll/GetLogicalProcessorInformation
- DynamicLoader: KERNEL32.dll/CreateSymbolicLinkW
- DynamicLoader: KERNEL32.dll/SetDefaultDllDirectories
- DynamicLoader: KERNEL32.dll/EnumSystemLocalesEx
- DynamicLoader: KERNEL32.dll/CompareStringEx
- DynamicLoader: KERNEL32.dll/GetDateFormatEx
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/GetTimeFormatEx
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/IsValidLocaleName
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: KERNEL32.dll/GetCurrentPackageId
- DynamicLoader: KERNEL32.dll/GetTickCount64
- DynamicLoader: KERNEL32.dll/GetFileInformationByHandleExW
- DynamicLoader: KERNEL32.dll/SetFileInformationByHandleW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: MSCOREE.DLL/
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: mscoreei.dll/RegisterShimImplCallback
- DynamicLoader: mscoreei.dll/RegisterShimImplCleanupCallback
- DynamicLoader: mscoreei.dll/SetShellShimInstance
- DynamicLoader: mscoreei.dll/OnShimDllMainCalled
- DynamicLoader: mscoreei.dll/_CorExeMain_RetAddr
- DynamicLoader: mscoreei.dll/_CorExeMain
- DynamicLoader: SHLWAPI.dll/UrllsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW



- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionEx
- DynamicLoader: KERNEL32.dll/CreateEventExW
- DynamicLoader: KERNEL32.dll/CreateSemaphoreExW
- DynamicLoader: KERNEL32.dll/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/CreateThreadpoolTimer
- DynamicLoader: KERNEL32.dll/SetThreadpoolTimer
- DynamicLoader: KERNEL32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: KERNEL32.dll/CloseThreadpoolTimer
- DynamicLoader: KERNEL32.dll/CreateThreadpoolWait
- DynamicLoader: KERNEL32.dll/SetThreadpoolWait
- DynamicLoader: KERNEL32.dll/CloseThreadpoolWait
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: KERNEL32.dll/GetCurrentProcessorNumber
- DynamicLoader: KERNEL32.dll/GetLogicalProcessorInformation
- DynamicLoader: KERNEL32.dll/CreateSymbolicLinkW
- DynamicLoader: KERNEL32.dll/SetDefaultDllDirectories
- DynamicLoader: KERNEL32.dll/EnumSystemLocalesEx
- DynamicLoader: KERNEL32.dll/CompareStringEx
- DynamicLoader: KERNEL32.dll/GetDateFormatEx
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/GetTimeFormatEx
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/IsValidLocaleName
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: KERNEL32.dll/GetCurrentPackageId
- DynamicLoader: KERNEL32.dll/GetTickCount64
- DynamicLoader: KERNEL32.dll/GetFileInformationByHandleExW
- DynamicLoader: KERNEL32.dll/SetFileInformationByHandleW
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: clr.dll/SetRuntimeInfo
- DynamicLoader: clr.dll/_CorExeMain
- DynamicLoader: MSCOREE.DLL/CreateConfigStream
- DynamicLoader: mscoreei.dll/CreateConfigStream_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream
- DynamicLoader: KERNEL32.dll/GetNumaHighestNodeNumber
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/AddSIDToBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/CreateBoundaryDescriptorW
- DynamicLoader: KERNEL32.dll/CreatePrivateNamespaceW
- DynamicLoader: KERNEL32.dll/OpenPrivateNamespaceW



- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/DeleteBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/WerRegisterRuntimeExceptionModule
- DynamicLoader: KERNEL32.dll/RaiseException
- DynamicLoader: MSCOREE.DLL/
- DynamicLoader: mscoreei.dll/
- DynamicLoader: KERNELBASE.dll/SetSystemFileCacheSize
- DynamicLoader: ntdll.dll/NtSetSystemInformation
- DynamicLoader: KERNELBASE.dll/PrivIsDllSynchronizationHeld
- DynamicLoader: KERNEL32.dll/AddDllDirectory
- DynamicLoader: KERNEL32.dll/SortGetHandle
- DynamicLoader: KERNEL32.dll/SortCloseHandle
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: gdiplus.dll/GdiplusStartup
- DynamicLoader: KERNEL32.dll/IsProcessorFeaturePresent
- DynamicLoader: USER32.dll/GetWindowInfo
- DynamicLoader: USER32.dll/GetAncestor
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/EnumDisplayDevicesA
- DynamicLoader: GDI32.dll/ExtTextOutW
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: gdiplus.dll/GdiLoadImageFromStream
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: WindowsCodecs.dll/DllGetClassObject
- DynamicLoader: KERNEL32.dll/WerRegisterMemoryBlock
- DynamicLoader: gdiplus.dll/GdiImageForceValidation
- DynamicLoader: gdiplus.dll/GdiGetImageType
- DynamicLoader: gdiplus.dll/GdiGetImageRawFormat
- DynamicLoader: gdiplus.dll/GdiGetImageWidth
- DynamicLoader: gdiplus.dll/GdiGetImageHeight
- DynamicLoader: gdiplus.dll/GdiBitmapGetPixel
- DynamicLoader: gdiplus.dll/GdiDisposeImage
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/GetUserPreferredUILanguages
- DynamicLoader: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/SetThreadErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW



- DynamicLoader: KERNEL32.dll/VirtualAlloc
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: KERNEL32.dll/WideCharToMultiByte
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextW
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptDecrypt
- DynamicLoader: ADVAPI32.dll/CryptDeriveKey
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/CryptDestroyKey
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: apphelp.dll/ApphelpCheckRunAppEx
- DynamicLoader: apphelp.dll/ApphelpQueryModuleDataEx
- DynamicLoader: apphelp.dll/ApphelpParseModuleData
- DynamicLoader: apphelp.dll/ApphelpCreateAppcompatData
- DynamicLoader: apphelp.dll/SdbInitDatabaseEx
- DynamicLoader: apphelp.dll/SdbReleaseDatabase
- DynamicLoader: apphelp.dll/SdbUnpackAppCompatData
- DynamicLoader: apphelp.dll/SdbQueryContext
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.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: ADVAPI32.dll/EventUnregister
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionEx
- DynamicLoader: KERNEL32.dll/CreateEventExW
- DynamicLoader: KERNEL32.dll/CreateSemaphoreExW
- DynamicLoader: KERNEL32.dll/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/CreateThreadpoolTimer
- DynamicLoader: KERNEL32.dll/SetThreadpoolTimer
- DynamicLoader: KERNEL32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: KERNEL32.dll/CloseThreadpoolTimer
- DynamicLoader: KERNEL32.dll/CreateThreadpoolWait
- DynamicLoader: KERNEL32.dll/SetThreadpoolWait
- DynamicLoader: KERNEL32.dll/CloseThreadpoolWait
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: KERNEL32.dll/GetCurrentProcessorNumber
- DynamicLoader: KERNEL32.dll/GetLogicalProcessorInformation
- DynamicLoader: KERNEL32.dll/CreateSymbolicLinkW
- DynamicLoader: KERNEL32.dll/SetDefaultDllDirectories
- DynamicLoader: KERNEL32.dll/EnumSystemLocalesEx
- DynamicLoader: KERNEL32.dll/CompareStringEx
- DynamicLoader: KERNEL32.dll/GetDateFormatEx

- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/GetTimeFormatEx
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/IsValidLocaleName
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: KERNEL32.dll/GetCurrentPackageld
- DynamicLoader: KERNEL32.dll/GetTickCount64
- DynamicLoader: KERNEL32.dll/GetFileInformationByHandleExW
- DynamicLoader: KERNEL32.dll/SetFileInformationByHandleW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: MSCOREE.DLL/
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: mscoreei.dll/RegisterShimImplCallback
- DynamicLoader: mscoreei.dll/RegisterShimImplCleanupCallback
- DynamicLoader: mscoreei.dll/SetShellShimInstance
- DynamicLoader: mscoreei.dll/OnShimDllMainCalled
- DynamicLoader: mscoreei.dll/_CorExeMain_RetAddr
- DynamicLoader: mscoreei.dll/_CorExeMain
- DynamicLoader: SHLWAPI.dll/UrllsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionEx
- DynamicLoader: KERNEL32.dll/CreateEventExW
- DynamicLoader: KERNEL32.dll/CreateSemaphoreExW
- DynamicLoader: KERNEL32.dll/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/CreateThreadpoolTimer
- DynamicLoader: KERNEL32.dll/SetThreadpoolTimer
- DynamicLoader: KERNEL32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: KERNEL32.dll/CloseThreadpoolTimer
- DynamicLoader: KERNEL32.dll/CreateThreadpoolWait
- DynamicLoader: KERNEL32.dll/SetThreadpoolWait
- DynamicLoader: KERNEL32.dll/CloseThreadpoolWait
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: KERNEL32.dll/GetCurrentProcessorNumber
- DynamicLoader: KERNEL32.dll/GetLogicalProcessorInformation
- DynamicLoader: KERNEL32.dll/CreateSymbolicLinkW
- DynamicLoader: KERNEL32.dll/SetDefaultDllDirectories
- DynamicLoader: KERNEL32.dll/EnumSystemLocalesEx
- DynamicLoader: KERNEL32.dll/CompareStringEx
- DynamicLoader: KERNEL32.dll/GetDateFormatEx
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/GetTimeFormatEx
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/IsValidLocaleName
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: KERNEL32.dll/GetCurrentPackageld
- DynamicLoader: KERNEL32.dll/GetTickCount64
- DynamicLoader: KERNEL32.dll/GetFileInformationByHandleExW
- DynamicLoader: KERNEL32.dll/SetFileInformationByHandleW
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: clr.dll/SetRuntimeInfo
- DynamicLoader: clr.dll/_CorExeMain
- DynamicLoader: MSCOREE.DLL/CreateConfigStream
- DynamicLoader: mscoreei.dll/CreateConfigStream_RetAddr



- DynamicLoader: mscoreei.dll/CreateConfigStream
- DynamicLoader: KERNEL32.dll/GetNumaHighestNodeNumber
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/AddSIDToBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/CreateBoundaryDescriptorW
- DynamicLoader: KERNEL32.dll/CreatePrivateNamespaceW
- DynamicLoader: KERNEL32.dll/OpenPrivateNamespaceW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/DeleteBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/WerRegisterRuntimeExceptionModule
- DynamicLoader: KERNEL32.dll/RaiseException
- DynamicLoader: MSCOREE.DLL/
- DynamicLoader: mscoreei.dll/
- DynamicLoader: KERNELBASE.dll/SetSystemFileCacheSize
- DynamicLoader: ntdll.dll/NtSetSystemInformation
- DynamicLoader: KERNELBASE.dll/PrivIsDllSynchronizationHeld
- DynamicLoader: KERNEL32.dll/AddDllDirectory
- DynamicLoader: KERNEL32.dll/SortGetHandle
- DynamicLoader: KERNEL32.dll/SortCloseHandle
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: UxTheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariable
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariableW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: 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/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/LoadLibrary
- DynamicLoader: KERNEL32.dll/LoadLibraryW
- DynamicLoader: KERNEL32.dll/EnumResourceTypes
- DynamicLoader: KERNEL32.dll/EnumResourceTypesW
- DynamicLoader: KERNEL32.dll/EnumResourceNames
- DynamicLoader: KERNEL32.dll/EnumResourceNamesW
- DynamicLoader: KERNEL32.dll/GetModuleFileName
- DynamicLoader: KERNEL32.dll/GetModuleFileNameW
- DynamicLoader: KERNEL32.dll/FindResource
- DynamicLoader: KERNEL32.dll/FindResourceW
- DynamicLoader: KERNEL32.dll/SizeofResource
- DynamicLoader: KERNEL32.dll/SizeofResourceW
- DynamicLoader: KERNEL32.dll/LoadResource
- DynamicLoader: KERNEL32.dll/LockResource
- DynamicLoader: KERNEL32.dll/LockResourceW
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetUserPreferredUILanguages
- DynamicLoader: KERNEL32.dll/FreeLibrary
- DynamicLoader: KERNEL32.dll/FreeLibraryW
- DynamicLoader: nlssorting.dll/SortGetHandle
- DynamicLoader: nlssorting.dll/SortCloseHandle
- DynamicLoader: CRYPTSP.dll/CryptGetDefaultProviderW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: KERNEL32.dll/ReleaseMutex
- DynamicLoader: KERNEL32.dll/CreateMutex
- DynamicLoader: KERNEL32.dll/CreateMutexW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetTempPath
- DynamicLoader: KERNEL32.dll/GetTempPathW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetComputerName
- DynamicLoader: KERNEL32.dll/GetComputerNameW
- DynamicLoader: KERNEL32.dll/CreateEvent
- DynamicLoader: KERNEL32.dll/CreateEventW
- DynamicLoader: KERNEL32.dll/SetEvent
- 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/_RpcExtInitializeExtensionPoint
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: ole32.dll/IIDFromString
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: KERNEL32.dll/ResolveDelayLoadedAPI
- DynamicLoader: ole32.dll/CoCreateFreeThreadedMarshaler
- DynamicLoader: ole32.dll/CoGetObjectContext
- DynamicLoader: KERNEL32.dll/LoadLibrary
- DynamicLoader: KERNEL32.dll/LoadLibraryA
- DynamicLoader: KERNEL32.dll/WideCharToMultiByte
- DynamicLoader: KERNEL32.dll/GetProcAddress
- DynamicLoader: wminet_utils.dll/ResetSecurity
- DynamicLoader: wminet_utils.dll/SetSecurity
- DynamicLoader: wminet_utils.dll/BlessWbemServices
- DynamicLoader: wminet_utils.dll/BlessWbemServicesObject
- DynamicLoader: wminet_utils.dll/GetPropertyHandle
- DynamicLoader: wminet_utils.dll/WritePropertyValue
- DynamicLoader: wminet_utils.dll/Clone
- DynamicLoader: wminet_utils.dll/VerifyClientKey
- DynamicLoader: wminet_utils.dll/GetQualifierSet
- DynamicLoader: wminet_utils.dll/Get
- DynamicLoader: wminet_utils.dll/Put
- DynamicLoader: wminet_utils.dll/Delete
- DynamicLoader: wminet_utils.dll/GetNames
- DynamicLoader: wminet_utils.dll/BeginEnumeration
- DynamicLoader: wminet_utils.dll/Next
- DynamicLoader: wminet_utils.dll/EndEnumeration
- DynamicLoader: wminet_utils.dll/GetPropertyQualifierSet
- DynamicLoader: wminet_utils.dll/Clone
- DynamicLoader: wminet_utils.dll/GetObjectText
- DynamicLoader: wminet_utils.dll/SpawnDerivedClass
- DynamicLoader: wminet_utils.dll/SpawnInstance
- DynamicLoader: wminet_utils.dll/CompareTo
- DynamicLoader: wminet_utils.dll/GetPropertyOrigin
- DynamicLoader: wminet_utils.dll/InheritsFrom
- DynamicLoader: wminet_utils.dll/GetMethod
- DynamicLoader: wminet_utils.dll/PutMethod
- DynamicLoader: wminet_utils.dll/DeleteMethod
- DynamicLoader: wminet_utils.dll/BeginMethodEnumeration
- DynamicLoader: wminet_utils.dll/NextMethod
- DynamicLoader: wminet_utils.dll/EndMethodEnumeration
- DynamicLoader: wminet_utils.dll/GetMethodQualifierSet
- DynamicLoader: wminet_utils.dll/GetMethodOrigin
- DynamicLoader: wminet_utils.dll/QualifierSet_Get
- DynamicLoader: wminet_utils.dll/QualifierSet_Put
- DynamicLoader: wminet_utils.dll/QualifierSet_Delete
- DynamicLoader: wminet_utils.dll/QualifierSet_GetNames
- DynamicLoader: wminet_utils.dll/QualifierSet_BeginEnumeration
- DynamicLoader: wminet_utils.dll/QualifierSet_Next
- DynamicLoader: wminet_utils.dll/QualifierSet_EndEnumeration
- DynamicLoader: wminet_utils.dll/GetCurrentApartmentType
- DynamicLoader: wminet_utils.dll/GetDemultiplexedStub
- DynamicLoader: wminet_utils.dll/CreateInstanceEnumWmi
- DynamicLoader: wminet_utils.dll/CreateClassEnumWmi



- DynamicLoader: wminet_utils.dll/ExecQueryWmi
- DynamicLoader: wminet_utils.dll/ExecNotificationQueryWmi
- DynamicLoader: wminet_utils.dll/PutInstanceWmi
- DynamicLoader: wminet_utils.dll/PutClassWmi
- DynamicLoader: wminet_utils.dll/CloneEnumWbemClassObject
- DynamicLoader: wminet_utils.dll/ConnectServerWmi
- DynamicLoader: KERNEL32.dll/GetThreadPreferredUILanguages
- DynamicLoader: KERNEL32.dll/SetThreadPreferredUILanguages
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetSystemDefaultLocaleName
- DynamicLoader: OLEAUT32.dll/SysStringLen
- DynamicLoader: KERNEL32.dll/RtlZeroMemory
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/GetErrorInfo
- DynamicLoader: OLEAUT32.dll/SysStringByteLen
- DynamicLoader: OLEAUT32.dll/SysFreeString
- DynamicLoader: KERNEL32.dll/SetThreadErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: KERNEL32.dll/GetFileType
- DynamicLoader: KERNEL32.dll/WriteFile
- DynamicLoader: KERNEL32.dll/GetModuleHandle
- DynamicLoader: KERNEL32.dll/GetModuleHandleW
- DynamicLoader: KERNEL32.dll/GetProcAddress
- DynamicLoader: USER32.dll/DefWindowProcW
- DynamicLoader: GDI32.dll/GetStockObject
- DynamicLoader: USER32.dll/RegisterClass
- DynamicLoader: USER32.dll/RegisterClassW
- DynamicLoader: USER32.dll/CreateWindowEx
- DynamicLoader: USER32.dll/CreateWindowExW
- DynamicLoader: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/GetWindowLong
- DynamicLoader: USER32.dll/GetWindowLongW
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentThread
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: KERNEL32.dll/GetCurrentThreadId
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/CallWindowProc
- DynamicLoader: USER32.dll/CallWindowProcW
- DynamicLoader: USER32.dll/RegisterWindowMessage
- DynamicLoader: USER32.dll/RegisterWindowMessageW
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: ADVAPI32.dll/EventRegister



- DynamicLoader: KERNEL32.dll/CompareStringOrdinal
- DynamicLoader: KERNEL32.dll/ResolveLocaleName
- DynamicLoader: KERNEL32.dll/GetTempFileName
- DynamicLoader: KERNEL32.dll/GetTempFileNameW
- DynamicLoader: SHELL32.dll/SHGetFolderPath
- DynamicLoader: SHELL32.dll/SHGetFolderPathW
- DynamicLoader: KERNEL32.dll/CreateProcess
- DynamicLoader: KERNEL32.dll/CreateProcessW
- DynamicLoader: KERNEL32.dll/GetThreadContext
- DynamicLoader: KERNEL32.dll/ReadProcessMemory
- DynamicLoader: ntdll.dll/NtUnmapViewOfSection
- DynamicLoader: KERNEL32.dll/VirtualAllocEx
- DynamicLoader: KERNEL32.dll/WriteProcessMemory
- DynamicLoader: KERNEL32.dll/SetThreadContext
- DynamicLoader: KERNEL32.dll/ResumeThread
- DynamicLoader: KERNEL32.dll/ReadFile
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: KERNEL32.dll/DeleteFile
- DynamicLoader: KERNEL32.dll/DeleteFileW
- 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: authZ.dll/AuthzInitializeContextFromToken
- DynamicLoader: authZ.dll/AuthzInitializeObjectAccessAuditEvent2
- DynamicLoader: authZ.dll/AuthzAccessCheck
- DynamicLoader: authZ.dll/AuthzFreeAuditEvent
- DynamicLoader: authZ.dll/AuthzFreeContext
- DynamicLoader: authZ.dll/AuthzInitializeResourceManager
- DynamicLoader: authZ.dll/AuthzFreeResourceManager
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcBindingCreateW
- DynamicLoader: RPCRT4.dll/RpcBindingBind
- DynamicLoader: RPCRT4.dll/I_RpcMapWin32Status
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: ADVAPI32.dll/EventWrite
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: ADVAPI32.dll/EventEnabled
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: kernel32.dll/RegSetValueExW
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: kernel32.dll/RegQueryValueExW
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: wmisvc.dll/IsImproperShutdownDetected
- DynamicLoader: Wevtapi.dll/EvtRender
- DynamicLoader: Wevtapi.dll/EvtNext
- DynamicLoader: Wevtapi.dll/EvtClose
- DynamicLoader: Wevtapi.dll/EvtQuery
- DynamicLoader: Wevtapi.dll/EvtCreateRenderContext
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeW
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/RpcBindingSetOption
- DynamicLoader: RPCRT4.dll/RpcStringFreeW
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: kernel32.dll/ResolveDelayLoadedAPI
- DynamicLoader: ole32.dll/CoCreateFreeThreadedMarshaler
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CreateStreamOnHGlobal
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: KERNELBASE.dll/InitializeAcl
- DynamicLoader: KERNELBASE.dll/AddAce
- DynamicLoader: kernel32.dll/OpenProcessToken
- DynamicLoader: KERNELBASE.dll/GetTokenInformation
- DynamicLoader: KERNELBASE.dll/DuplicateTokenEx
- DynamicLoader: KERNELBASE.dll/AdjustTokenPrivileges
- DynamicLoader: kernel32.dll/SetThreadToken
- DynamicLoader: KERNELBASE.dll/CheckTokenMembership
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: KERNELBASE.dll/AllocateAndInitializeSid
- DynamicLoader: ole32.dll/CLSIDFromString
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- 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/CoRevertToSelf
- DynamicLoader: SspiCli.dll/LogonUserExExW
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetCallContext
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: ole32.dll/CoImpersonateClient
- DynamicLoader: ole32.dll/CoSwitchCallContext
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: kernel32.dll/ResolveDelayLoadedAPI
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/SetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/LocaleNameToLCID
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/LCIDToLocaleName
- DynamicLoader: kernel32.dll/GetSystemDefaultLocaleName
- DynamicLoader: FastProx.dll/DllGetClassObject
- DynamicLoader: FastProx.dll/DllCanUnloadNow
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: kernel32.dll/RegQueryValueExW
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: ADVAPI32.dll/EventWrite
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: ADVAPI32.dll/EventEnabled
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: WMI.DLL/WmiQueryAllDataW
- DynamicLoader: WMI.DLL/WmiQuerySingleInstanceW
- DynamicLoader: WMI.DLL/WmiSetSingleItemW
- DynamicLoader: WMI.DLL/WmiSetSingleInstanceW
- DynamicLoader: WMI.DLL/WmiExecuteMethodW
- DynamicLoader: WMI.DLL/WmiNotificationRegistrationW
- DynamicLoader: WMI.DLL/WmiMofEnumerateResourcesW
- DynamicLoader: WMI.DLL/WmiFileHandleToInstanceNameW
- DynamicLoader: WMI.DLL/WmiDevInstToInstanceNameW
- DynamicLoader: WMI.DLL/WmiQueryGuidInformation
- DynamicLoader: WMI.DLL/WmiOpenBlock
- DynamicLoader: WMI.DLL/WmiCloseBlock
- DynamicLoader: WMI.DLL/WmiFreeBuffer
- DynamicLoader: WMI.DLL/WmiEnumerateGuids
- DynamicLoader: IPHLPAPI.DLL/GetAdaptersAddresses
- DynamicLoader: IPHLPAPI.DLL/GetIpForwardTable2
- DynamicLoader: IPHLPAPI.DLL/ConvertLengthToIpv4Mask
- DynamicLoader: IPHLPAPI.DLL/FreeMibTable
- DynamicLoader: IPHLPAPI.DLL/GetAdapterIndex
- DynamicLoader: IPHLPAPI.DLL/GetAdapterIndex



- DynamicLoader: IPHLPAPI.DLL/GetAdapterIndex
- DynamicLoader: IPHLPAPI.DLL/GetAdapterIndex
- DynamicLoader: IPHLPAPI.DLL/GetAdapterIndex
- DynamicLoader: IPHLPAPI.DLL/GetAdapterIndex
- DynamicLoader: IPHLPAPI.DLL/GetAdapterIndex
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: DNSAPI.dll/DnsQueryConfigAllocEx
- DynamicLoader: IPHLPAPI.DLL/GetCurrentThreadCompartmentId
- DynamicLoader: RPCRT4.dll/NdrClientCall3
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeW
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcStringFreeW
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: DNSAPI.dll/DnsFreeConfigStructure
- DynamicLoader: DNSAPI.dll/DnsQueryConfigDword
- DynamicLoader: IPHLPAPI.DLL/GetAdapterIndex
- DynamicLoader: IPHLPAPI.DLL/GetAdapterIndex
- DynamicLoader: IPHLPAPI.DLL/GetAdapterIndex
- DynamicLoader: IPHLPAPI.DLL/GetAdapterIndex
- DynamicLoader: IPHLPAPI.DLL/GetAdapterIndex
- DynamicLoader: COMCTL32.dll/InitCommonControlsEx
- DynamicLoader: SHELL32.dll/SHGetSpecialFolderPathW
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextA
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptGetHashParam
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/CredReadA
- DynamicLoader: ADVAPI32.dll/CredFree
- DynamicLoader: ADVAPI32.dll/CredDeleteA
- DynamicLoader: ADVAPI32.dll/CredEnumerateA
- DynamicLoader: ADVAPI32.dll/CredEnumerateW
- DynamicLoader: pstorec.dll/PStoreCreateInstance
- DynamicLoader: vaultcli.dll/VaultOpenVault
- DynamicLoader: vaultcli.dll/VaultCloseVault
- DynamicLoader: vaultcli.dll/VaultEnumerateItems
- DynamicLoader: vaultcli.dll/VaultFree
- DynamicLoader: vaultcli.dll/VaultGetInformation
- DynamicLoader: vaultcli.dll/VaultGetItem
- DynamicLoader: psapi.dll/GetModuleBaseNameW
- DynamicLoader: psapi.dll/EnumProcessModules
- DynamicLoader: psapi.dll/GetModuleFileNameExW
- DynamicLoader: psapi.dll/EnumProcesses
- DynamicLoader: psapi.dll/GetModuleInformation
- DynamicLoader: kernel32.dll/QueryFullProcessImageNameW
- DynamicLoader: kernel32.dll/GetProcessTimes
- DynamicLoader: COMCTL32.dll/InitCommonControlsEx
- DynamicLoader: SHELL32.dll/SHGetSpecialFolderPathA
- DynamicLoader: pstorec.dll/PStoreCreateInstance
- DynamicLoader: crypt32.dll/CryptUnprotectData
- DynamicLoader: ADVAPI32.dll/CredReadA



- DynamicLoader: ADVAPI32.dll/CredFree
- DynamicLoader: ADVAPI32.dll/CredDeleteA
- DynamicLoader: ADVAPI32.dll/CredEnumerateA
- DynamicLoader: ADVAPI32.dll/CredEnumerateW
- DynamicLoader: ADVAPI32.dll/CredReadA
- DynamicLoader: ADVAPI32.dll/CredFree
- DynamicLoader: ADVAPI32.dll/CredDeleteA
- DynamicLoader: ADVAPI32.dll/CredEnumerateA
- DynamicLoader: ADVAPI32.dll/CredEnumerateW
- DynamicLoader: crypt32.dll/CryptUnprotectData
- DynamicLoader: ADVAPI32.dll/CredReadA
- DynamicLoader: ADVAPI32.dll/CredFree
- DynamicLoader: ADVAPI32.dll/CredDeleteA
- DynamicLoader: ADVAPI32.dll/CredEnumerateA
- DynamicLoader: ADVAPI32.dll/CredEnumerateW

A process attempted to delay the analysis task.

- Process: RegAsm.exe tried to sleep 596 seconds, actually delayed analysis time by 0 seconds

Guard pages use detected - possible anti-debugging.

Creates RWX memory

SetUnhandledExceptionFilter detected (possible anti-debug)