


cswindowsservicerecoveryproperty.exe

Is DLL 

Packer 

Anti Debug 

Anti VM 

Signed 

XOR 

MalFamily: Swisyn

MalScore: 100

File type: PE32 executable (GUI) Intel 80386, for MS Windows

File size: 219.43 KB (224699 bytes)

Compile time: 2011-06-14 21:01:16

MD5: 9e135081c3d16e40ace18aeb8e1afb9d

SHA1: 81199319692bf3f15713908e29d02243e4be5aec


Import hash: 98f67c550a7da65513e63ffd998f6b2e

Submitted: 2019-01-12 13:30:10

URL(s) file hosting

<http://tonghopgia.net/webservices/redirect/cswindowsservicerecoveryproperty.exe>

Antivirus Report

Report date	Detection Ratio	Permalink
2018-12-29 12:42:22	62/70	

Import library

MSVBVM60.DLL

16

Behaviors detected by system signatures

Attempts to modify Explorer settings to prevent hidden files from being displayed

Anomalous binary characteristics

- anomaly: Actual checksum does not match that reported in PE header

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Local\Temp\cswindowsservicerecoveryproperty.exe\xc2\xa0
- file: C:\Windows\system\explorer.exe
- file: C:\Windows\system\spoolsv.exe
- file: C:\Users\Seven01\AppData\Roaming\mrsys.exe
- file: C:\Windows\system\svchost.exe

Installs itself for autorun at Windows startup

- key:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\Explorer
- data: c:\windows\system\explorer.exe RO
- key:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\Svchost
- data: c:\windows\system\svchost.exe RO
- key: HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}
- data: unknown
- key: HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE-E0AC10B4E666}
- data: unknown
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}\StubPath
- data: C:\Users\Seven01\AppData\Roaming\mrsys.exe MR
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE-E0AC10B4E666}\StubPath
- data: C:\Users\Seven01\AppData\Roaming\mrsys.exe MR
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\shell
- data: C:\Windows\explorer.exe, c:\windows\system\explorer.exe

Installs an hook procedure to monitor for mouse events

Sniffs keystrokes

- SetWindowsHookExA: Process: explorer.exe(956)

Uses Windows utilities for basic functionality

- command: at 17:23 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
- command: at 17:36 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
- command: at 17:48 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe

Drops a binary and executes it

- binary: C:\Windows\system\svchost.exe
- binary: C:\Windows\system\explorer.exe
- binary: C:\Users\Seven01\AppData\Local\icsys.icn.exe
- binary: C:\Windows\system\spoolsv.exe

Reads data out of its own binary image

- self_read: process: cswindowsservicerecoveryproperty.exe, pid: 2772, offset: 0x00000000, length: 0x00033ba2
- self_read: process: cswindowsservicerecoveryproperty.exe, pid: 2772, offset: 0x00036da2, length: 0x00000019
- self_read: process: icsys.icn.exe, pid: 1044, offset: 0x00000000, length: 0x0002e000
- self_read: process: icsys.icn.exe, pid: 1044, offset: 0x00033b89, length: 0x00000019
- self_read: process: explorer.exe, pid: 956, offset: 0x00000000, length: 0x0002e000
- self_read: process: explorer.exe, pid: 956, offset: 0x00033b37, length: 0x00000019
- self_read: process: spoolsv.exe, pid: 1384, offset: 0x00000000, length: 0x0002e000

- self_read: process: spoolsv.exe, pid: 1384, offset: 0x00033b58, length: 0x00000019
- self_read: process: svchost.exe, pid: 2300, offset: 0x00033b1a, length: 0x00000015

Expresses interest in specific running processes

- process: svchost.exe
- process: explorer.exe

Dynamic (imported) function loading detected

- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: OLEAUT32.dll/OleLoadPictureEx
- DynamicLoader: OLEAUT32.dll/DispCallFunc
- DynamicLoader: OLEAUT32.dll/LoadTypeLibEx
- DynamicLoader: OLEAUT32.dll/UnRegisterTypeLib
- DynamicLoader: OLEAUT32.dll/CreateTypeLib2
- DynamicLoader: OLEAUT32.dll/VarDateFromUpdate
- DynamicLoader: OLEAUT32.dll/VarUpdateFromDate
- DynamicLoader: OLEAUT32.dll/GetAltMonthNames
- DynamicLoader: OLEAUT32.dll/VarNumFromParseNum
- DynamicLoader: OLEAUT32.dll/VarParseNumFromStr
- DynamicLoader: OLEAUT32.dll/VarDecFromR4
- DynamicLoader: OLEAUT32.dll/VarDecFromR8
- DynamicLoader: OLEAUT32.dll/VarDecFromDate
- DynamicLoader: OLEAUT32.dll/VarDecFromI4
- DynamicLoader: OLEAUT32.dll/VarDecFromCy
- DynamicLoader: OLEAUT32.dll/VarR4FromDec
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromTypeInfo
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromGuids
- DynamicLoader: OLEAUT32.dll/SafeArrayGetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArraySetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArrayGetIID
- DynamicLoader: OLEAUT32.dll/SafeArraySetIID
- DynamicLoader: OLEAUT32.dll/SafeArrayCopyData
- DynamicLoader: OLEAUT32.dll/SafeArrayAllocDescriptorEx
- DynamicLoader: OLEAUT32.dll/SafeArrayCreateEx
- DynamicLoader: OLEAUT32.dll/VarFormat
- DynamicLoader: OLEAUT32.dll/VarFormatDateTime
- DynamicLoader: OLEAUT32.dll/VarFormatNumber
- DynamicLoader: OLEAUT32.dll/VarFormatPercent
- DynamicLoader: OLEAUT32.dll/VarFormatCurrency
- DynamicLoader: OLEAUT32.dll/VarWeekdayName
- DynamicLoader: OLEAUT32.dll/VarMonthName
- DynamicLoader: OLEAUT32.dll/VarAdd
- DynamicLoader: OLEAUT32.dll/VarAnd
- DynamicLoader: OLEAUT32.dll/VarCat
- DynamicLoader: OLEAUT32.dll/VarDiv
- DynamicLoader: OLEAUT32.dll/VarEqv
- DynamicLoader: OLEAUT32.dll/VarIdiv
- DynamicLoader: OLEAUT32.dll/VarImp
- DynamicLoader: OLEAUT32.dll/VarMod
- DynamicLoader: OLEAUT32.dll/VarMul
- DynamicLoader: OLEAUT32.dll/VarOr
- DynamicLoader: OLEAUT32.dll/VarPow
- DynamicLoader: OLEAUT32.dll/VarSub
- DynamicLoader: OLEAUT32.dll/VarXor
- DynamicLoader: OLEAUT32.dll/VarAbs
- DynamicLoader: OLEAUT32.dll/VarFix
- DynamicLoader: OLEAUT32.dll/VarInt
- DynamicLoader: OLEAUT32.dll/VarNeg
- DynamicLoader: OLEAUT32.dll/VarNot
- DynamicLoader: OLEAUT32.dll/VarRound



- DynamicLoader: OLEAUT32.dll/VarCmp
- DynamicLoader: OLEAUT32.dll/VarDecAdd
- DynamicLoader: OLEAUT32.dll/VarDecCmp
- DynamicLoader: OLEAUT32.dll/VarBstrCat
- DynamicLoader: OLEAUT32.dll/VarCyMull4
- DynamicLoader: OLEAUT32.dll/VarBstrCmp
- DynamicLoader: ole32.dll/CoCreateInstanceEx
- DynamicLoader: ole32.dll/CLSIDFromProgIDEx
- DynamicLoader: SXS.DLL/SxsOleAut32MapIIDOrCLSIDToTypeLibrary
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/MonitorFromWindow
- DynamicLoader: USER32.dll/MonitorFromRect
- DynamicLoader: USER32.dll/MonitorFromPoint
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: ole32.dll/CLSIDFromOle1Class
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject2
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: shell32.dll/SHGetSpecialFolderLocation
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CreateBindCtx
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetApartmentType
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetMalloc
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_Size_ExW
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ADVAPI32.dll/OpenThreadToken
- DynamicLoader: shell32.dll/
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_ExW
- DynamicLoader: shell32.dll/SHGetPathFromIDListA
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ADVAPI32.dll/InitializeSecurityDescriptor
- DynamicLoader: ADVAPI32.dll/SetEntriesInAclW
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: ADVAPI32.dll/SetSecurityDescriptorDacl
- DynamicLoader: ADVAPI32.dll/IsTextUnicode
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: kernel32.dll/GetComputerNameA
- DynamicLoader: ADVAPI32.dll/GetUserNameA
- DynamicLoader: kernel32.dll/GetFileAttributesA
- 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: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoRevokeInitializeSpy
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: comctl32.dll/
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: OLEAUT32.dll/OleLoadPictureEx
- DynamicLoader: OLEAUT32.dll/DispCallFunc
- DynamicLoader: OLEAUT32.dll/LoadTypeLibEx
- DynamicLoader: OLEAUT32.dll/UnRegisterTypeLib
- DynamicLoader: OLEAUT32.dll/CreateTypeLib2
- DynamicLoader: OLEAUT32.dll/VarDateFromUpdate
- DynamicLoader: OLEAUT32.dll/VarUpdateFromDate
- DynamicLoader: OLEAUT32.dll/GetAltMonthNames
- DynamicLoader: OLEAUT32.dll/VarNumFromParseNum
- DynamicLoader: OLEAUT32.dll/VarParseNumFromStr
- DynamicLoader: OLEAUT32.dll/VarDecFromR4
- DynamicLoader: OLEAUT32.dll/VarDecFromR8
- DynamicLoader: OLEAUT32.dll/VarDecFromDate
- DynamicLoader: OLEAUT32.dll/VarDecFromI4
- DynamicLoader: OLEAUT32.dll/VarDecFromCy
- DynamicLoader: OLEAUT32.dll/VarR4FromDec
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromTypeInfo
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromGuids
- DynamicLoader: OLEAUT32.dll/SafeArrayGetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArraySetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArrayGetIID
- DynamicLoader: OLEAUT32.dll/SafeArraySetIID
- DynamicLoader: OLEAUT32.dll/SafeArrayCopyData
- DynamicLoader: OLEAUT32.dll/SafeArrayAllocDescriptorEx
- DynamicLoader: OLEAUT32.dll/SafeArrayCreateEx
- DynamicLoader: OLEAUT32.dll/VarFormat
- DynamicLoader: OLEAUT32.dll/VarFormatDateTime
- DynamicLoader: OLEAUT32.dll/VarFormatNumber
- DynamicLoader: OLEAUT32.dll/VarFormatPercent
- DynamicLoader: OLEAUT32.dll/VarFormatCurrency
- DynamicLoader: OLEAUT32.dll/VarWeekdayName
- DynamicLoader: OLEAUT32.dll/VarMonthName
- DynamicLoader: OLEAUT32.dll/VarAdd
- DynamicLoader: OLEAUT32.dll/VarAnd
- DynamicLoader: OLEAUT32.dll/VarCat
- DynamicLoader: OLEAUT32.dll/VarDiv
- DynamicLoader: OLEAUT32.dll/VarEqv
- DynamicLoader: OLEAUT32.dll/VarIdiv
- DynamicLoader: OLEAUT32.dll/VarImp
- DynamicLoader: OLEAUT32.dll/VarMod
- DynamicLoader: OLEAUT32.dll/VarMul
- DynamicLoader: OLEAUT32.dll/VarOr
- DynamicLoader: OLEAUT32.dll/VarPow
- DynamicLoader: OLEAUT32.dll/VarSub
- DynamicLoader: OLEAUT32.dll/VarXor

- DynamicLoader: OLEAUT32.dll/VarAbs
- DynamicLoader: OLEAUT32.dll/VarFix
- DynamicLoader: OLEAUT32.dll/VarInt
- DynamicLoader: OLEAUT32.dll/VarNeg
- DynamicLoader: OLEAUT32.dll/VarNot
- DynamicLoader: OLEAUT32.dll/VarRound
- DynamicLoader: OLEAUT32.dll/VarCmp
- DynamicLoader: OLEAUT32.dll/VarDecAdd
- DynamicLoader: OLEAUT32.dll/VarDecCmp
- DynamicLoader: OLEAUT32.dll/VarBstrCat
- DynamicLoader: OLEAUT32.dll/VarCyMull4
- DynamicLoader: OLEAUT32.dll/VarBstrCmp
- DynamicLoader: ole32.dll/CoCreateInstanceEx
- DynamicLoader: ole32.dll/CLSIDFromProgIDEx
- DynamicLoader: SXS.DLL/SxsOleAut32MapIIDOrCLSIDToTypeLibrary
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/MonitorFromWindow
- DynamicLoader: USER32.dll/MonitorFromRect
- DynamicLoader: USER32.dll/MonitorFromPoint
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: ole32.dll/CLSIDFromOle1Class
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject2
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: shell32.dll/SHGetSpecialFolderLocation
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CreateBindCtx
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetApartmentType
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetMalloc
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ADVAPI32.dll/OpenThreadToken
- DynamicLoader: shell32.dll/
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: shell32.dll/SHGetPathFromIDListA
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_Size_ExW
- DynamicLoader: kernel32.dll/NlsGetCacheUpdateCount
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_ExW
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ADVAPI32.dll/InitializeSecurityDescriptor
- DynamicLoader: ADVAPI32.dll/SetEntriesInAclW
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: ADVAPI32.dll/SetSecurityDescriptorDacl
- DynamicLoader: ADVAPI32.dll/IsTextUnicode
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/



- DynamicLoader: kernel32.dll/GetComputerNameA
- DynamicLoader: ADVAPI32.dll/GetUserNameA
- DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
- DynamicLoader: kernel32.dll/Process32First
- DynamicLoader: kernel32.dll/OpenProcess
- DynamicLoader: Psapi.dll/GetModuleFileNameExA
- DynamicLoader: kernel32.dll/Process32Next
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/GetFileAttributesA
- 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: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoRevokeInitializeSpy
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: comctl32.dll/
- 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: 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: ntdll.dll/RtlVirtualUnwind
- DynamicLoader: KERNEL32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/AddSIDToBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/CreateBoundaryDescriptorW
- DynamicLoader: KERNEL32.dll/CreatePrivateNamespaceW
- DynamicLoader: KERNEL32.dll/OpenPrivateNamespaceW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/DeleteBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/WerRegisterRuntimeExceptionModule
- DynamicLoader: KERNEL32.dll/RaiseException
- DynamicLoader: MSCOREE.DLL/
- DynamicLoader: mscoreei.dll/
- DynamicLoader: KERNEL32.dll/AddDllDirectory
- DynamicLoader: KERNEL32.dll/SortGetHandle
- DynamicLoader: KERNEL32.dll/SortCloseHandle
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: ADVAPI32.dll/OpenSCManager
- DynamicLoader: ADVAPI32.dll/OpenSCManagerW
- DynamicLoader: ADVAPI32.dll/OpenService
- DynamicLoader: ADVAPI32.dll/OpenServiceW
- DynamicLoader: KERNEL32.dll/FormatMessage
- DynamicLoader: KERNEL32.dll/FormatMessageW
- DynamicLoader: ADVAPI32.dll/CloseServiceHandle
- DynamicLoader: ADVAPI32.dll/CloseServiceHandleW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetStdHandle
- DynamicLoader: KERNEL32.dll/WriteFile
- DynamicLoader: KERNEL32.dll/GetConsoleOutputCP
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetUserPreferredUILanguages
- DynamicLoader: KERNEL32.dll/UnmapViewOfFile
- DynamicLoader: KERNEL32.dll/GetFileType
- 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: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: OLEAUT32.dll/OleLoadPictureEx
- DynamicLoader: OLEAUT32.dll/DispCallFunc
- DynamicLoader: OLEAUT32.dll/LoadTypeLibEx
- DynamicLoader: OLEAUT32.dll/UnRegisterTypeLib
- DynamicLoader: OLEAUT32.dll/CreateTypeLib2
- DynamicLoader: OLEAUT32.dll/VarDateFromUpdate
- DynamicLoader: OLEAUT32.dll/VarUpdateFromDate
- DynamicLoader: OLEAUT32.dll/GetAltMonthNames
- DynamicLoader: OLEAUT32.dll/VarNumFromParseNum
- DynamicLoader: OLEAUT32.dll/VarParseNumFromStr
- DynamicLoader: OLEAUT32.dll/VarDecFromR4
- DynamicLoader: OLEAUT32.dll/VarDecFromR8
- DynamicLoader: OLEAUT32.dll/VarDecFromDate
- DynamicLoader: OLEAUT32.dll/VarDecFromI4
- DynamicLoader: OLEAUT32.dll/VarDecFromCy
- DynamicLoader: OLEAUT32.dll/VarR4FromDec
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromTypeInfo
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromGuids
- DynamicLoader: OLEAUT32.dll/SafeArrayGetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArraySetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArrayGetIID
- DynamicLoader: OLEAUT32.dll/SafeArraySetIID
- DynamicLoader: OLEAUT32.dll/SafeArrayCopyData
- DynamicLoader: OLEAUT32.dll/SafeArrayAllocDescriptorEx
- DynamicLoader: OLEAUT32.dll/SafeArrayCreateEx
- DynamicLoader: OLEAUT32.dll/VarFormat
- DynamicLoader: OLEAUT32.dll/VarFormatDateTime
- DynamicLoader: OLEAUT32.dll/VarFormatNumber
- DynamicLoader: OLEAUT32.dll/VarFormatPercent
- DynamicLoader: OLEAUT32.dll/VarFormatCurrency
- DynamicLoader: OLEAUT32.dll/VarWeekdayName
- DynamicLoader: OLEAUT32.dll/VarMonthName
- DynamicLoader: OLEAUT32.dll/VarAdd
- DynamicLoader: OLEAUT32.dll/VarAnd
- DynamicLoader: OLEAUT32.dll/VarCat
- DynamicLoader: OLEAUT32.dll/VarDiv
- DynamicLoader: OLEAUT32.dll/VarEqv
- DynamicLoader: OLEAUT32.dll/VarIdiv
- DynamicLoader: OLEAUT32.dll/VarImp
- DynamicLoader: OLEAUT32.dll/VarMod
- DynamicLoader: OLEAUT32.dll/VarMul
- DynamicLoader: OLEAUT32.dll/VarOr
- DynamicLoader: OLEAUT32.dll/VarPow
- DynamicLoader: OLEAUT32.dll/VarSub
- DynamicLoader: OLEAUT32.dll/VarXor
- DynamicLoader: OLEAUT32.dll/VarAbs
- DynamicLoader: OLEAUT32.dll/VarFix
- DynamicLoader: OLEAUT32.dll/VarInt
- DynamicLoader: OLEAUT32.dll/VarNeg
- DynamicLoader: OLEAUT32.dll/VarNot
- DynamicLoader: OLEAUT32.dll/VarRound
- DynamicLoader: OLEAUT32.dll/VarCmp
- DynamicLoader: OLEAUT32.dll/VarDecAdd
- DynamicLoader: OLEAUT32.dll/VarDecCmp
- DynamicLoader: OLEAUT32.dll/VarBstrCat
- DynamicLoader: OLEAUT32.dll/VarCyMull4



- DynamicLoader: OLEAUT32.dll/VarBstrCmp
- DynamicLoader: ole32.dll/CoCreateInstanceEx
- DynamicLoader: ole32.dll/CLSIDFromProgIDEx
- DynamicLoader: SXS.DLL/SxsOleAut32MapIIDOrCLSIDToTypeLibrary
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/MonitorFromWindow
- DynamicLoader: USER32.dll/MonitorFromRect
- DynamicLoader: USER32.dll/MonitorFromPoint
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: ole32.dll/CLSIDFromOle1Class
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject2
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: shell32.dll/SHGetSpecialFolderLocation
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CreateBindCtx
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetApartmentType
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetMalloc
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_Size_ExW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_ExW
- DynamicLoader: ADVAPI32.dll/OpenThreadToken
- DynamicLoader: shell32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: shell32.dll/SHGetPathFromIDListA
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: comctl32.dll/
- DynamicLoader: kernel32.dll/NlsGetCacheUpdateCount
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ADVAPI32.dll/InitializeSecurityDescriptor
- DynamicLoader: ADVAPI32.dll/SetEntriesInAclW
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: ADVAPI32.dll/SetSecurityDescriptorDacl
- DynamicLoader: ADVAPI32.dll/IsTextUnicode
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: kernel32.dll/GetComputerNameA
- DynamicLoader: ADVAPI32.dll/GetUserNameA
- DynamicLoader: kernel32.dll/GetFileAttributesA
- DynamicLoader: USER32.dll/SetWindowsHookExA
- DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
- DynamicLoader: kernel32.dll/Process32First
- DynamicLoader: kernel32.dll/OpenProcess
- DynamicLoader: Psapi.dll/GetModuleFileNameExA
- DynamicLoader: kernel32.dll/Process32Next
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: ADVAPI32.dll/RegCreateKeyA



- DynamicLoader: ADVAPI32.dll/RegSetValueExA
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: kernel32.dll/WritePrivateProfileStringA
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExA
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExA
- DynamicLoader: ADVAPI32.dll/RegDeleteKeyA
- DynamicLoader: ADVAPI32.dll/RegOpenKeyA
- DynamicLoader: ADVAPI32.dll/RegDeleteValueA
- 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: USER32.dll/GetForegroundWindow
- DynamicLoader: USER32.dll/GetWindowThreadProcessId
- DynamicLoader: kernel32.dll/Thread32First
- DynamicLoader: kernel32.dll/Thread32Next
- DynamicLoader: kernel32.dll/OpenThread
- DynamicLoader: kernel32.dll/ResumeThread
- DynamicLoader: USER32.dll/CallNextHookEx
- DynamicLoader: kernel32.dll/FindFirstFileA
- DynamicLoader: kernel32.dll/DeleteFileA
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: OLEAUT32.dll/OleLoadPictureEx
- DynamicLoader: OLEAUT32.dll/DispCallFunc
- DynamicLoader: OLEAUT32.dll/LoadTypeLibEx
- DynamicLoader: OLEAUT32.dll/UnRegisterTypeLib
- DynamicLoader: OLEAUT32.dll/CreateTypeLib2
- DynamicLoader: OLEAUT32.dll/VarDateFromUpdate
- DynamicLoader: OLEAUT32.dll/VarUpdateFromDate
- DynamicLoader: OLEAUT32.dll/GetAltMonthNames
- DynamicLoader: OLEAUT32.dll/VarNumFromParseNum
- DynamicLoader: OLEAUT32.dll/VarParseNumFromStr
- DynamicLoader: OLEAUT32.dll/VarDecFromR4
- DynamicLoader: OLEAUT32.dll/VarDecFromR8
- DynamicLoader: OLEAUT32.dll/VarDecFromDate
- DynamicLoader: OLEAUT32.dll/VarDecFromI4
- DynamicLoader: OLEAUT32.dll/VarDecFromCy
- DynamicLoader: OLEAUT32.dll/VarR4FromDec
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromTypeInfo
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromGuids
- DynamicLoader: OLEAUT32.dll/SafeArrayGetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArraySetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArrayGetIID
- DynamicLoader: OLEAUT32.dll/SafeArraySetIID
- DynamicLoader: OLEAUT32.dll/SafeArrayCopyData
- DynamicLoader: OLEAUT32.dll/SafeArrayAllocDescriptorEx
- DynamicLoader: OLEAUT32.dll/SafeArrayCreateEx
- DynamicLoader: OLEAUT32.dll/VarFormat
- DynamicLoader: OLEAUT32.dll/VarFormatDateTime
- DynamicLoader: OLEAUT32.dll/VarFormatNumber
- DynamicLoader: OLEAUT32.dll/VarFormatPercent
- DynamicLoader: OLEAUT32.dll/VarFormatCurrency
- DynamicLoader: OLEAUT32.dll/VarWeekdayName
- DynamicLoader: OLEAUT32.dll/VarMonthName

- DynamicLoader: OLEAUT32.dll/VarAdd
- DynamicLoader: OLEAUT32.dll/VarAnd
- DynamicLoader: OLEAUT32.dll/VarCat
- DynamicLoader: OLEAUT32.dll/VarDiv
- DynamicLoader: OLEAUT32.dll/VarEqv
- DynamicLoader: OLEAUT32.dll/VarIdiv
- DynamicLoader: OLEAUT32.dll/VarImp
- DynamicLoader: OLEAUT32.dll/VarMod
- DynamicLoader: OLEAUT32.dll/VarMul
- DynamicLoader: OLEAUT32.dll/VarOr
- DynamicLoader: OLEAUT32.dll/VarPow
- DynamicLoader: OLEAUT32.dll/VarSub
- DynamicLoader: OLEAUT32.dll/VarXor
- DynamicLoader: OLEAUT32.dll/VarAbs
- DynamicLoader: OLEAUT32.dll/VarFix
- DynamicLoader: OLEAUT32.dll/VarInt
- DynamicLoader: OLEAUT32.dll/VarNeg
- DynamicLoader: OLEAUT32.dll/VarNot
- DynamicLoader: OLEAUT32.dll/VarRound
- DynamicLoader: OLEAUT32.dll/VarCmp
- DynamicLoader: OLEAUT32.dll/VarDecAdd
- DynamicLoader: OLEAUT32.dll/VarDecCmp
- DynamicLoader: OLEAUT32.dll/VarBstrCat
- DynamicLoader: OLEAUT32.dll/VarCyMull4
- DynamicLoader: OLEAUT32.dll/VarBstrCmp
- DynamicLoader: ole32.dll/CoCreateInstanceEx
- DynamicLoader: ole32.dll/CLSIDFromProgIDEx
- DynamicLoader: SXS.DLL/SxsOleAut32MapIIDOrCLSIDToTypeLibrary
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/MonitorFromWindow
- DynamicLoader: USER32.dll/MonitorFromRect
- DynamicLoader: USER32.dll/MonitorFromPoint
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: ole32.dll/CLSIDFromOle1Class
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject2
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: shell32.dll/SHGetSpecialFolderLocation
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CreateBindCtx
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetApartmentType
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetMalloc
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_Size_ExW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_ExW
- DynamicLoader: ADVAPI32.dll/OpenThreadToken
- DynamicLoader: shell32.dll/
- DynamicLoader: ole32.dll/CoUninitialize



- DynamicLoader: shell32.dll/SHGetPathFromIDListA
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: kernel32.dll/NlsGetCacheUpdateCount
- DynamicLoader: kernel32.dll/GetFileAttributesA
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoRevokeInitializeSpy
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: OLEAUT32.dll/OleLoadPictureEx
- DynamicLoader: OLEAUT32.dll/DispCallFunc
- DynamicLoader: OLEAUT32.dll/LoadTypeLibEx
- DynamicLoader: OLEAUT32.dll/UnRegisterTypeLib
- DynamicLoader: OLEAUT32.dll/CreateTypeLib2
- DynamicLoader: OLEAUT32.dll/VarDateFromUpdate
- DynamicLoader: OLEAUT32.dll/VarUpdateFromDate
- DynamicLoader: OLEAUT32.dll/GetAltMonthNames
- DynamicLoader: OLEAUT32.dll/VarNumFromParseNum
- DynamicLoader: OLEAUT32.dll/VarParseNumFromStr
- DynamicLoader: OLEAUT32.dll/VarDecFromR4
- DynamicLoader: OLEAUT32.dll/VarDecFromR8
- DynamicLoader: OLEAUT32.dll/VarDecFromDate
- DynamicLoader: OLEAUT32.dll/VarDecFromI4
- DynamicLoader: OLEAUT32.dll/VarDecFromCy
- DynamicLoader: OLEAUT32.dll/VarR4FromDec
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromTypeInfo
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromGuids
- DynamicLoader: OLEAUT32.dll/SafeArrayGetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArraySetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArrayGetIID
- DynamicLoader: OLEAUT32.dll/SafeArraySetIID
- DynamicLoader: OLEAUT32.dll/SafeArrayCopyData
- DynamicLoader: OLEAUT32.dll/SafeArrayAllocDescriptorEx
- DynamicLoader: OLEAUT32.dll/SafeArrayCreateEx
- DynamicLoader: OLEAUT32.dll/VarFormat
- DynamicLoader: OLEAUT32.dll/VarFormatDateTime
- DynamicLoader: OLEAUT32.dll/VarFormatNumber
- DynamicLoader: OLEAUT32.dll/VarFormatPercent
- DynamicLoader: OLEAUT32.dll/VarFormatCurrency
- DynamicLoader: OLEAUT32.dll/VarWeekdayName
- DynamicLoader: OLEAUT32.dll/VarMonthName
- DynamicLoader: OLEAUT32.dll/VarAdd
- DynamicLoader: OLEAUT32.dll/VarAnd
- DynamicLoader: OLEAUT32.dll/VarCat
- DynamicLoader: OLEAUT32.dll/VarDiv
- DynamicLoader: OLEAUT32.dll/VarEqv
- DynamicLoader: OLEAUT32.dll/VarIdiv
- DynamicLoader: OLEAUT32.dll/VarImp
- DynamicLoader: OLEAUT32.dll/VarMod
- DynamicLoader: OLEAUT32.dll/VarMul
- DynamicLoader: OLEAUT32.dll/VarOr
- DynamicLoader: OLEAUT32.dll/VarPow
- DynamicLoader: OLEAUT32.dll/VarSub
- DynamicLoader: OLEAUT32.dll/VarXor
- DynamicLoader: OLEAUT32.dll/VarAbs
- DynamicLoader: OLEAUT32.dll/VarFix
- DynamicLoader: OLEAUT32.dll/VarInt
- DynamicLoader: OLEAUT32.dll/VarNeg

- DynamicLoader: OLEAUT32.dll/VarNot
- DynamicLoader: OLEAUT32.dll/VarRound
- DynamicLoader: OLEAUT32.dll/VarCmp
- DynamicLoader: OLEAUT32.dll/VarDecAdd
- DynamicLoader: OLEAUT32.dll/VarDecCmp
- DynamicLoader: OLEAUT32.dll/VarBstrCat
- DynamicLoader: OLEAUT32.dll/VarCyMull4
- DynamicLoader: OLEAUT32.dll/VarBstrCmp
- DynamicLoader: ole32.dll/CoCreateInstanceEx
- DynamicLoader: ole32.dll/CLSIDFromProgIDEx
- DynamicLoader: SXS.DLL/SxsOleAut32MapIIDOrCLSIDToTypeLibrary
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/MonitorFromWindow
- DynamicLoader: USER32.dll/MonitorFromRect
- DynamicLoader: USER32.dll/MonitorFromPoint
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: ole32.dll/CLSIDFromOle1Class
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject2
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: shell32.dll/SHGetSpecialFolderLocation
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CreateBindCtx
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetApartmentType
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetMalloc
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ADVAPI32.dll/OpenThreadToken
- DynamicLoader: shell32.dll/
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: shell32.dll/SHGetPathFromIDListA
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: kernel32.dll/NlsGetCacheUpdateCount
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_Size_ExW
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ADVAPI32.dll/InitializeSecurityDescriptor
- DynamicLoader: ADVAPI32.dll/SetEntriesInAclW
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: ADVAPI32.dll/SetSecurityDescriptorDacl
- DynamicLoader: ADVAPI32.dll/IsTextUnicode
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: kernel32.dll/GetComputerNameA
- DynamicLoader: ADVAPI32.dll/GetUserNameA
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_ExW
- DynamicLoader: comctl32.dll/
- DynamicLoader: kernel32.dll/GetCalendarInfoW
- DynamicLoader: ADVAPI32.dll/RegCreateKeyA



- DynamicLoader: ADVAPI32.dll/RegSetValueExA
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: kernel32.dll/WritePrivateProfileStringA
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExA
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExA
- DynamicLoader: ADVAPI32.dll/RegDeleteKeyA
- DynamicLoader: ADVAPI32.dll/RegOpenKeyA
- DynamicLoader: ADVAPI32.dll/RegDeleteValueA
- DynamicLoader: USER32.dll/GetForegroundWindow
- DynamicLoader: USER32.dll/GetWindowThreadProcessId
- DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
- DynamicLoader: kernel32.dll/Process32First
- DynamicLoader: kernel32.dll/OpenProcess
- DynamicLoader: Psapi.dll/GetModuleFileNameExA
- DynamicLoader: kernel32.dll/Process32Next
- DynamicLoader: kernel32.dll/Thread32First
- DynamicLoader: kernel32.dll/Thread32Next
- DynamicLoader: kernel32.dll/OpenThread
- DynamicLoader: kernel32.dll/ResumeThread
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: OLEAUT32.dll/OleLoadPictureEx
- DynamicLoader: OLEAUT32.dll/DispCallFunc
- DynamicLoader: OLEAUT32.dll/LoadTypeLibEx
- DynamicLoader: OLEAUT32.dll/UnRegisterTypeLib
- DynamicLoader: OLEAUT32.dll/CreateTypeLib2
- DynamicLoader: OLEAUT32.dll/VarDateFromUpdate
- DynamicLoader: OLEAUT32.dll/VarUpdateFromDate
- DynamicLoader: OLEAUT32.dll/GetAltMonthNames
- DynamicLoader: OLEAUT32.dll/VarNumFromParseNum
- DynamicLoader: OLEAUT32.dll/VarParseNumFromStr
- DynamicLoader: OLEAUT32.dll/VarDecFromR4
- DynamicLoader: OLEAUT32.dll/VarDecFromR8
- DynamicLoader: OLEAUT32.dll/VarDecFromDate
- DynamicLoader: OLEAUT32.dll/VarDecFromI4
- DynamicLoader: OLEAUT32.dll/VarDecFromCy
- DynamicLoader: OLEAUT32.dll/VarR4FromDec
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromTypeInfo
- DynamicLoader: OLEAUT32.dll/GetRecordInfoFromGuids
- DynamicLoader: OLEAUT32.dll/SafeArrayGetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArraySetRecordInfo
- DynamicLoader: OLEAUT32.dll/SafeArrayGetIID
- DynamicLoader: OLEAUT32.dll/SafeArraySetIID
- DynamicLoader: OLEAUT32.dll/SafeArrayCopyData
- DynamicLoader: OLEAUT32.dll/SafeArrayAllocDescriptorEx
- DynamicLoader: OLEAUT32.dll/SafeArrayCreateEx
- DynamicLoader: OLEAUT32.dll/VarFormat
- DynamicLoader: OLEAUT32.dll/VarFormatDateTime
- DynamicLoader: OLEAUT32.dll/VarFormatNumber
- DynamicLoader: OLEAUT32.dll/VarFormatPercent
- DynamicLoader: OLEAUT32.dll/VarFormatCurrency
- DynamicLoader: OLEAUT32.dll/VarWeekdayName
- DynamicLoader: OLEAUT32.dll/VarMonthName
- DynamicLoader: OLEAUT32.dll/VarAdd
- DynamicLoader: OLEAUT32.dll/VarAnd
- DynamicLoader: OLEAUT32.dll/VarCat
- DynamicLoader: OLEAUT32.dll/VarDiv
- DynamicLoader: OLEAUT32.dll/VarEqv
- DynamicLoader: OLEAUT32.dll/VarIdiv
- DynamicLoader: OLEAUT32.dll/VarImp
- DynamicLoader: OLEAUT32.dll/VarMod
- DynamicLoader: OLEAUT32.dll/VarMul



- DynamicLoader: OLEAUT32.dll/VarOr
- DynamicLoader: OLEAUT32.dll/VarPow
- DynamicLoader: OLEAUT32.dll/VarSub
- DynamicLoader: OLEAUT32.dll/VarXor
- DynamicLoader: OLEAUT32.dll/VarAbs
- DynamicLoader: OLEAUT32.dll/VarFix
- DynamicLoader: OLEAUT32.dll/VarInt
- DynamicLoader: OLEAUT32.dll/VarNeg
- DynamicLoader: OLEAUT32.dll/VarNot
- DynamicLoader: OLEAUT32.dll/VarRound
- DynamicLoader: OLEAUT32.dll/VarCmp
- DynamicLoader: OLEAUT32.dll/VarDecAdd
- DynamicLoader: OLEAUT32.dll/VarDecCmp
- DynamicLoader: OLEAUT32.dll/VarBstrCat
- DynamicLoader: OLEAUT32.dll/VarCyMull4
- DynamicLoader: OLEAUT32.dll/VarBstrCmp
- DynamicLoader: ole32.dll/CoCreateInstanceEx
- DynamicLoader: ole32.dll/CLSIDFromProgIDEx
- DynamicLoader: SXS.DLL/SxsOleAut32MapIIDOrCLSIDToTypeLibrary
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/MonitorFromWindow
- DynamicLoader: USER32.dll/MonitorFromRect
- DynamicLoader: USER32.dll/MonitorFromPoint
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: ole32.dll/CLSIDFromOle1Class
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject2
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext

A process attempted to delay the analysis task.

- Process: svchost.exe tried to sleep 360 seconds, actually delayed analysis time by 0 seconds

Guard pages use detected - possible anti-debugging.

Anomalous file deletion behavior detected (10+)

- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\~DF59C63E380EE41A3C.TMP
- DeletedFile: C:\Windows\system\explorer.exe
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\~DF852859D0636F2F74.TMP
- DeletedFile: C:\Windows\system\spoolsv.exe
- DeletedFile: C:\Users\Seven01\AppData\Roaming\mrsys.exe
- DeletedFile: C:\Windows\system\udsys.exe
- DeletedFile: C:\Windows\system\udsys.exe
- DeletedFile: C:\Windows\system\svchost.exe
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\~DF5036AE2C8A3917ED.TMP
- DeletedFile: C:\Windows\Tasks\Adobe Flash Player Updater.job
- DeletedFile: C:\Windows\Tasks\SCHEDLGU.TXT
- DeletedFile: C:\Windows\Tasks\SCHEDLGU.TXT
- DeletedFile: C:\Users\Seven01\AppData\Local\Temp\~DF7B38986FB937EF42.TMP

Creates RWX memory

SetUnhandledExceptionFilter detected (possible anti-debug)