whe.exe

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

MalFamily: Deepscan **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	332.50 KB (340480 bytes)
Compile time:	2019-08-22 00:11:14
MD5:	af5141d170da335a2e7024f82b7b96df
SHA1:	b49fe533f37b41bcb0b74e1e1141b2aa55adb25a
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2019-08-22 10:18:05

URL(s) file hosting

http://lmvadvogados.com.br/wp-content/themes/twentynineteen/sass/mixins/whe.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2019-08-21 22:39:51	39/71	

Import library

mscoree.dll

17 Behaviors detected by system signatures

Collects information to fingerprint the system

Harvests information related to installed mail clients

- file: C:\Users\Seven01\AppData\Roaming\Thunderbird\profiles.ini
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password
- 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
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password
- 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\9375CFF0413111d3B88A00104B2A6676\00000003
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
- key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676

Harvests credentials from local FTP client softwares

- file: C:\Users\Seven01\AppData\Roaming\FileZilla\recentservers.xml

- file: C:\Users\Seven01\AppData\Roaming\SmartFTP\Client 2.0\Favorites\Quick Connect*.xml
- file: C:\Users\Seven01\AppData\Roaming\SmartFTP\Client 2.0\Favorites\Quick Connect\
- file: C:\Users\Seven01\AppData\Roaming\FTPGetter\servers.xml
- file: C:\Users\Seven01\AppData\Roaming\Ipswitch\WS_FTP\Sites\ws_ftp.ini
- file: C:\cftp\Ftplist.txt
- key: HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites

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

Retrieves Windows ProductID, probably to fingerprint the sandbox

Installs itself for autorun at Windows startup

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

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

- Spam: services.exe (480) called API GetSystemTimeAsFileTime 3415339 times

Performs some HTTP requests

- url: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab

A process created a hidden window

- Process: svchost.exe -> \\?\C:\Windows\system32\wbem\WMIADAP.EXE

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

- ioc: inetsim.org0

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/FlsAlloc
- DynamicLoader: KERNEL32.dll/FlsFree
- DynamicLoader: KERNEL32.dll/FlsGetValue
- DynamicLoader: KERNEL32.dll/FlsSetValue
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionEx
- DynamicLoader: KERNEL32.dll/CreateEventExW
- DynamicLoader: KERNEL32.dll/CreateSemaphoreExW
- DynamicLoader: KERNEL32.dll/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/CreateThreadpoolTimer
- DynamicLoader: KERNEL32.dll/SetThreadpoolTimer
- DynamicLoader: KERNEL32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: KERNEL32.dll/CloseThreadpoolTimer
- DynamicLoader: KERNEL32.dll/CreateThreadpoolWait
- DynamicLoader: KERNEL32.dll/SetThreadpoolWait
- DynamicLoader: KERNEL32.dll/CloseThreadpoolWait
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: KERNEL32.dll/GetCurrentProcessorNumber
- DynamicLoader: KERNEL32.dll/GetLogicalProcessorInformation
- DynamicLoader: KERNEL32.dll/CreateSymbolicLinkW
- DynamicLoader: KERNEL32.dll/SetDefaultDllDirectories
- DynamicLoader: KERNEL32.dll/EnumSystemLocalesEx
- DynamicLoader: KERNEL32.dll/CompareStringEx
- DynamicLoader: KERNEL32.dll/GetDateFormatEx
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx

- DynamicLoader: KERNEL32.dll/GetTimeFormatEx
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/IsValidLocaleName
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: KERNEL32.dll/GetCurrentPackageId
- DynamicLoader: KERNEL32.dll/GetTickCount64
- DynamicLoader: KERNEL32.dll/GetFileInformationByHandleExW
- DynamicLoader: KERNEL32.dll/SetFileInformationByHandleW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: MSCOREE.DLL/
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: mscoreei.dll/RegisterShimImplCallback
- DynamicLoader: mscoreei.dll/RegisterShimImplCleanupCallback
- DynamicLoader: mscoreei.dll/SetShellShimInstance
- DynamicLoader: mscoreei.dll/OnShimDllMainCalled
- DynamicLoader: mscoreei.dll/_CorExeMain_RetAddr
- DynamicLoader: mscoreei.dll/_CorExeMain
- DynamicLoader: SHLWAPI.dll/UrlIsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/FlsAlloc
- DynamicLoader: KERNEL32.dll/FlsGetValue
- DynamicLoader: KERNEL32.dll/FlsSetValue
- DynamicLoader: KERNEL32.dll/FlsFree
- DynamicLoader: KERNEL32.dll/InitializeCriticalSectionAndSpinCount
- DynamicLoader: KERNEL32.dll/IsProcessorFeaturePresent
- DynamicLoader: msvcrt.dll/_set_error_mode
- DynamicLoader: msvcrt.dll/?set_terminate@@YAP6AXXZP6AXXZ@Z
- DynamicLoader: msvcrt.dll/_get_terminate
- DynamicLoader: KERNEL32.dll/FindActCtxSectionStringW
- DynamicLoader: KERNEL32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: mscorwks.dll/SetLoadedByMscoree
- DynamicLoader: mscorwks.dll/_CorExeMain
- DynamicLoader: mscorwks.dll/GetCLRFunction
- DynamicLoader: ADVAPI32.dll/RegisterTraceGuidsW
- DynamicLoader: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: ADVAPI32.dll/GetTraceLoggerHandle
- DynamicLoader: ADVAPI32.dll/GetTraceEnableLevel
- DynamicLoader: ADVAPI32.dll/GetTraceEnableFlags
- DynamicLoader: ADVAPI32.dll/TraceEvent
- DynamicLoader: MSCOREE.DLL/IEE
- DynamicLoader: mscoreei.dll/IEE_RetAddr
- DynamicLoader: mscoreei.dll/IEE
- DynamicLoader: mscorwks.dll/IEE
- DynamicLoader: MSCOREE.DLL/GetStartupFlags
- DynamicLoader: mscoreei.dll/GetStartupFlags_RetAddr
- DynamicLoader: mscoreei.dll/GetStartupFlags
- DynamicLoader: MSCOREE.DLL/GetHostConfigurationFile
- DynamicLoader: mscoreei.dll/GetHostConfigurationFile_RetAddr
- DynamicLoader: mscoreei.dll/GetHostConfigurationFile
- DynamicLoader: mscoreei.dll/GetCORVersion_RetAddr
- DynamicLoader: mscoreei.dll/GetCORVersion
- DynamicLoader: MSCOREE.DLL/GetCORSystemDirectory
- DynamicLoader: mscoreei.dll/GetCORSystemDirectory_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream

- DynamicLoader: ntdll.dll/RtlUnwind
- DynamicLoader: KERNEL32.dll/IsWow64Process
- DynamicLoader: KERNEL32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/SetThreadStackGuarantee
- DynamicLoader: KERNEL32.dll/FlsSetValue
- DynamicLoader: KERNEL32.dll/FlsGetValue
- DynamicLoader: KERNEL32.dll/FlsAlloc
- DynamicLoader: KERNEL32.dll/FlsFree
- DynamicLoader: KERNEL32.dll/AddVectoredContinueHandler
- DynamicLoader: KERNEL32.dll/RemoveVectoredContinueHandler
- DynamicLoader: ADVAPI32.dll/ConvertSidToStringSidW
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: KERNEL32.dll/FlushProcessWriteBuffers
- DynamicLoader: KERNEL32.dll/GetWriteWatch
- DynamicLoader: KERNEL32.dll/ResetWriteWatch
- DynamicLoader: KERNEL32.dll/CreateMemoryResourceNotification
- DynamicLoader: KERNEL32.dll/QueryMemoryResourceNotification
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: KERNEL32.dll/QueryActCtxW
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextA
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptGetHashParam
- DynamicLoader: ADVAPI32.dll/CryptImportKey
- DynamicLoader: ADVAPI32.dll/CryptExportKey
- DynamicLoader: ADVAPI32.dll/CryptGenKey
- DynamicLoader: ADVAPI32.dll/CryptGetKeyParam
- DynamicLoader: ADVAPI32.dll/CryptDestroyKey
- DynamicLoader: ADVAPI32.dll/CryptVerifySignatureA
- DynamicLoader: ADVAPI32.dll/CryptSignHashA
- DynamicLoader: ADVAPI32.dll/CryptGetProvParam
- DynamicLoader: ADVAPI32.dll/CryptGetUserKey
- DynamicLoader: ADVAPI32.dll/CryptEnumProvidersA
- DynamicLoader: MSCOREE.DLL/GetMetaDataInternalInterface
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface_RetAddr
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface
- DynamicLoader: mscorwks.dll/GetMetaDataInternalInterface
- DynamicLoader: mscorjit.dll/getJit
- DynamicLoader: KERNEL32.dll/IsWow64Process

- DynamicLoader: KERNEL32.dll/lstrlen
- DynamicLoader: KERNEL32.dll/lstrlenW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: KERNEL32.dll/GetUserDefaultUILanguage
- DynamicLoader: KERNEL32.dll/SetErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariable
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariableW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: ole32.dll/CreateBindCtx
- DynamicLoader: ole32.dll/CoGetObjectContext
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: ole32.dll/NdrOleInitializeExtension
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: ole32.dll/MkParseDisplayName
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: KERNEL32.dll/GetThreadPreferredUILanguages
- DynamicLoader: KERNEL32.dll/SetThreadPreferredUILanguages
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetSystemDefaultLocaleName
- DynamicLoader: ole32.dll/BindMoniker
- DynamicLoader: SXS.DLL/SxsOleAut32RedirectTypeLibrary
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: ADVAPI32.dll/RegQueryValueW
- DynamicLoader: SXS.DLL/SxsOleAut32MapConfiguredClsidToReferenceClsid
- DynamicLoader: SXS.DLL/SxsLookupClrGuid
- DynamicLoader: KERNEL32.dll/ReleaseActCtx
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: mscoreei.dll/_CorDllMain_RetAddr
- DynamicLoader: mscoreei.dll/_CorDllMain
- DynamicLoader: MSCOREE.DLL/GetTokenForVTableEntry
- DynamicLoader: MSCOREE.DLL/SetTargetForVTableEntry
- DynamicLoader: MSCOREE.DLL/GetTargetForVTableEntry
- DynamicLoader: mscoreei.dll/GetTokenForVTableEntry_RetAddr
- DynamicLoader: mscoreei.dll/GetTokenForVTableEntry
- DynamicLoader: mscoreei.dll/SetTargetForVTableEntry_RetAddr
- DynamicLoader: mscoreei.dll/SetTargetForVTableEntry
- DynamicLoader: mscoreei.dll/GetTargetForVTableEntry_RetAddr

- DynamicLoader: mscoreei.dll/GetTargetForVTableEntry
- DynamicLoader: KERNEL32.dll/GetLastError
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: OLEAUT32.dll/VariantInit
- DynamicLoader: OLEAUT32.dll/VariantClear
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: KERNEL32.dll/CreateEvent
- DynamicLoader: KERNEL32.dll/CreateEventW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/SwitchToThread
- DynamicLoader: KERNEL32.dll/SetEvent
- DynamicLoader: ole32.dll/CoWaitForMultipleHandles
- DynamicLoader: ole32.dll/IIDFromString
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: KERNEL32.dll/LoadLibrary
- DynamicLoader: KERNEL32.dll/LoadLibraryA
- DynamicLoader: KERNEL32.dll/GetProcAddress
- DynamicLoader: wminet_utils.dll/ResetSecurity
- DynamicLoader: wminet_utils.dll/SetSecurity
- DynamicLoader: wminet_utils.dll/BlessIWbemServices
- DynamicLoader: wminet_utils.dll/BlessIWbemServicesObject
- DynamicLoader: wminet_utils.dll/GetPropertyHandle
- DynamicLoader: wminet_utils.dll/WritePropertyValue
- DynamicLoader: wminet_utils.dll/Clone
- DynamicLoader: wminet_utils.dll/VerifyClientKey
- DynamicLoader: wminet_utils.dll/GetQualifierSet
- DynamicLoader: wminet_utils.dll/Get
- DynamicLoader: wminet_utils.dll/Put
- DynamicLoader: wminet_utils.dll/Delete
- DynamicLoader: wminet_utils.dll/GetNames
- DynamicLoader: wminet_utils.dll/BeginEnumeration
- DynamicLoader: wminet_utils.dll/Next
- DynamicLoader: wminet_utils.dll/EndEnumeration
- DynamicLoader: wminet_utils.dll/GetPropertyQualifierSet
- DynamicLoader: wminet_utils.dll/Clone
- DynamicLoader: wminet_utils.dll/GetObjectText
- DynamicLoader: wminet_utils.dll/SpawnDerivedClass
- DynamicLoader: wminet_utils.dll/SpawnInstance
- DynamicLoader: wminet_utils.dll/CompareTo
- DynamicLoader: wminet_utils.dll/GetPropertyOrigin
- DynamicLoader: wminet_utils.dll/InheritsFrom
- DynamicLoader: wminet_utils.dll/GetMethod
- DynamicLoader: wminet_utils.dll/PutMethod
- DynamicLoader: wminet_utils.dll/DeleteMethod
- DynamicLoader: wminet_utils.dll/BeginMethodEnumeration
- DynamicLoader: wminet_utils.dll/NextMethod
- DynamicLoader: wminet_utils.dll/EndMethodEnumeration
- DynamicLoader: wminet_utils.dll/GetMethodQualifierSet
- DynamicLoader: wminet_utils.dll/GetMethodOrigin
- DynamicLoader: wminet_utils.dll/QualifierSet_Get
- DynamicLoader: wminet_utils.dll/QualifierSet_Put
- DynamicLoader: wminet_utils.dll/QualifierSet_Delete
- DynamicLoader: wminet_utils.dll/QualifierSet_GetNames
- DynamicLoader: wminet_utils.dll/QualifierSet_BeginEnumeration
- DynamicLoader: wminet_utils.dll/QualifierSet_Next
- DynamicLoader: wminet_utils.dll/QualifierSet_EndEnumeration
- DynamicLoader: wminet_utils.dll/GetCurrentApartmentType
- DynamicLoader: wminet_utils.dll/GetDemultiplexedStub
- DynamicLoader: wminet_utils.dll/CreateInstanceEnumWmi
- DynamicLoader: wminet_utils.dll/CreateClassEnumWmi
- DynamicLoader: wminet_utils.dll/ExecQueryWmi
- DynamicLoader: wminet_utils.dll/ExecNotificationQueryWmi
- DynamicLoader: wminet_utils.dll/PutInstanceWmi

- DynamicLoader: wminet_utils.dll/PutClassWmi
- DynamicLoader: wminet_utils.dll/CloneEnumWbemClassObject
- DynamicLoader: wminet_utils.dll/ConnectServerWmi
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: OLEAUT32.dll/SysStringLen
- DynamicLoader: KERNEL32.dll/ZeroMemory
- DynamicLoader: KERNEL32.dll/ZeroMemoryA
- DynamicLoader: KERNEL32.dll/RtlZeroMemory
- DynamicLoader: KERNEL32.dll/RegOpenKeyExW
- DynamicLoader: mscoreei.dll/LoadLibraryShim_RetAddr
- DynamicLoader: mscoreei.dll/LoadLibraryShim
- DynamicLoader: culture.dll/ConvertLangIdToCultureName
- DynamicLoader: ADVAPI32.dll/GetUserName
- DynamicLoader: ADVAPI32.dll/GetUserNameW
- DynamicLoader: KERNEL32.dll/GetComputerName
- DynamicLoader: KERNEL32.dll/GetComputerNameW
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: 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: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: USER32.dll/CreateWindowEx
- DynamicLoader: USER32.dll/CreateWindowExW
- DynamicLoader: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/GetWindowLong
- DynamicLoader: USER32.dll/GetWindowLongW
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentThread
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: KERNEL32.dll/GetCurrentThreadId
- DynamicLoader: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/CallWindowProc
- DynamicLoader: USER32.dll/CallWindowProcW
- DynamicLoader: USER32.dll/RegisterWindowMessage
- DynamicLoader: USER32.dll/RegisterWindowMessageW
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: KERNEL32.dll/GetCurrentProcessId
- DynamicLoader: KERNEL32.dll/GetCurrentProcessIdW
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValue
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivilegesW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: ntdll.dll/NtQuerySystemInformation

- DynamicLoader: ntdll.dll/NtQuerySystemInformationW
- DynamicLoader: KERNEL32.dll/GetTempPath
- DynamicLoader: KERNEL32.dll/GetTempPathW
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentProcessW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/GetTokenInformationW
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: KERNEL32.dll/LocalAllocW
- DynamicLoader: MSCOREE.DLL/ND_RI4
- DynamicLoader: mscoreei.dll/ND_RI4_RetAddr
- DynamicLoader: mscoreei.dll/ND_RI4
- DynamicLoader: ADVAPI32.dll/DuplicateTokenEx
- DynamicLoader: ADVAPI32.dll/DuplicateTokenExW
- DynamicLoader: ADVAPI32.dll/CheckTokenMembership
- DynamicLoader: ADVAPI32.dll/CheckTokenMembershipW
- DynamicLoader: KERNEL32.dll/DeleteFile
- DynamicLoader: KERNEL32.dll/DeleteFileW
- DynamicLoader: KERNEL32.dll/CreateIoCompletionPort
- DynamicLoader: KERNEL32.dll/PostQueuedCompletionStatus
- DynamicLoader: ntdll.dll/NtQueryInformationThread
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtGetCurrentProcessorNumber
- DynamicLoader: shfolder.dll/SHGetFolderPath
- DynamicLoader: shfolder.dll/SHGetFolderPathW
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: MLANG.dll/
- DynamicLoader: WININET.dll/FindFirstUrlCacheEntryA
- DynamicLoader: KERNEL32.dll/SetFileInformationByHandle
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: urlmon.dll/CreateUri
- DynamicLoader: KERNEL32.dll/InitializeSRWLock
- DynamicLoader: KERNEL32.dll/AcquireSRWLockExclusive
- DynamicLoader: KERNEL32.dll/AcquireSRWLockShared
- DynamicLoader: KERNEL32.dll/ReleaseSRWLockExclusive
- DynamicLoader: KERNEL32.dll/ReleaseSRWLockShared
- DynamicLoader: KERNEL32.dll/InitializeSRWLock
- DynamicLoader: KERNEL32.dll/AcquireSRWLockExclusive
- DynamicLoader: KERNEL32.dll/AcquireSRWLockShared
- DynamicLoader: KERNEL32.dll/ReleaseSRWLockExclusive
- DynamicLoader: KERNEL32.dll/ReleaseSRWLockShared
- DynamicLoader: WININET.dll/FindNextUrlCacheEntryA
- DynamicLoader: WININET.dll/FindCloseUrlCache
- DynamicLoader: ADVAPI32.dll/CryptAcquireContext
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextA
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/CryptReleaseContextW
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: vaultcli.dll/VaultEnumerateVaults
- DynamicLoader: KERNEL32.dll/GetSystemTimeAsFileTime
- DynamicLoader: USER32.dll/GetLastInputInfo

- DynamicLoader: KERNEL32.dll/FindFirstFile
- DynamicLoader: KERNEL32.dll/FindFirstFileW
- DynamicLoader: KERNEL32.dll/FindClose
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKey
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyEx
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: ole32.dll/CLSIDFromProgIDEx
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/GetClientRect
- DynamicLoader: USER32.dll/GetWindowRect
- DynamicLoader: USER32.dll/GetParent
- DynamicLoader: ole32.dll/OleInitialize
- DynamicLoader: ole32.dll/CoRegisterMessageFilter
- DynamicLoader: USER32.dll/PeekMessage
- DynamicLoader: USER32.dll/PeekMessageW
- DynamicLoader: USER32.dll/IsWindowUnicode
- DynamicLoader: USER32.dll/GetMessageW
- DynamicLoader: USER32.dll/TranslateMessage
- DynamicLoader: USER32.dll/DispatchMessageW
- DynamicLoader: USER32.dll/WaitMessage
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: tschannel.dll/DllGetClassObject
- DynamicLoader: tschannel.dll/DllCanUnloadNow
- DynamicLoader: SHELL32.dll/SHChangeNotify
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: RasApi32.dll/RasEnumConnectionsW
- DynamicLoader: RasApi32.dll/RasConnectionNotificationW
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/SetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/LocaleNameToLCID
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/LCIDToLocaleName
- DynamicLoader: kernel32.dll/GetSystemDefaultLocaleName
- DynamicLoader: FastProx.dll/DllGetClassObject

- DynamicLoader: FastProx.dll/DllCanUnloadNow
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: kernel32.dll/RegQueryValueExW
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- 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: OLEAUT32.dll/
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: WMI.DLL/WmiQueryAllDataW
- DynamicLoader: WMI.DLL/WmiQuerySingleInstanceW
- DynamicLoader: WMI.DLL/WmiSetSingleItemW
- DynamicLoader: WMI.DLL/WmiSetSingleInstanceW
- DynamicLoader: WMI.DLL/WmiExecuteMethodW
- DynamicLoader: WMI.DLL/WmiNotificationRegistrationW
- DynamicLoader: WMI.DLL/WmiMofEnumerateResourcesW
- DynamicLoader: WMI.DLL/WmiFileHandleToInstanceNameW
- DynamicLoader: WMI.DLL/WmiDevInstToInstanceNameW
- DynamicLoader: WMI.DLL/WmiQueryGuidInformation
- DynamicLoader: WMI.DLL/WmiOpenBlock
- DynamicLoader: WMI.DLL/WmiCloseBlock
- DynamicLoader: WMI.DLL/WmiFreeBuffer
- DynamicLoader: WMI.DLL/WmiEnumerateGuids
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: WINBRAND.dll/BrandingLoadString
- DynamicLoader: SECURITY.DLL/InitSecurityInterfaceW
- DynamicLoader: CRYPTSP.dll/SystemFunction035
- DynamicLoader: schannel.DLL/SpUserModeInitialize
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: ntdll.dll/RtlInitUnicodeString
- DynamicLoader: ntdll.dll/RtlFreeUnicodeString
- DynamicLoader: ntdll.dll/NtSetSystemEnvironmentValue
- DynamicLoader: ntdll.dll/NtQuerySystemEnvironmentValue
- DynamicLoader: ntdll.dll/NtCreateFile
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtQueryDirectoryObject
- DynamicLoader: ntdll.dll/NtQueryObject
- DynamicLoader: ntdll.dll/NtOpenDirectoryObject
- DynamicLoader: ntdll.dll/NtQueryInformationProcess
- DynamicLoader: ntdll.dll/NtQueryInformationToken
- DynamicLoader: ntdll.dll/NtOpenFile
- DynamicLoader: ntdll.dll/NtClose
- DynamicLoader: ntdll.dll/NtFsControlFile
- DynamicLoader: ntdll.dll/NtQueryVolumeInformationFile
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: NETAPI32.DLL/NetGroupEnum
- DynamicLoader: NETAPI32.DLL/NetGroupGetInfo
- DynamicLoader: NETAPI32.DLL/NetGroupSetInfo

- DynamicLoader: NETAPI32.DLL/NetLocalGroupGetInfo
- DynamicLoader: NETAPI32.DLL/NetLocalGroupSetInfo
- DynamicLoader: NETAPI32.DLL/NetGroupGetUsers
- DynamicLoader: NETAPI32.DLL/NetLocalGroupGetMembers
- DynamicLoader: NETAPI32.DLL/NetLocalGroupEnum
- DynamicLoader: NETAPI32.DLL/NetShareEnum
- DynamicLoader: NETAPI32.DLL/NetShareGetInfo
- DynamicLoader: NETAPI32.DLL/NetShareAdd
- DynamicLoader: NETAPI32.DLL/NetShareEnumSticky
- DynamicLoader: NETAPI32.DLL/NetShareSetInfo
- DynamicLoader: NETAPI32.DLL/NetShareDel
- DynamicLoader: NETAPI32.DLL/NetShareDelSticky
- DynamicLoader: NETAPI32.DLL/NetShareCheck
- DynamicLoader: NETAPI32.DLL/NetUserEnum
- DynamicLoader: NETAPI32.DLL/NetUserGetInfo
- DynamicLoader: NETAPI32.DLL/NetUserSetInfo
- DynamicLoader: NETAPI32.DLL/NetGroupEnum
- DynamicLoader: NETAPI32.DLL/NetApiBufferFree
- DynamicLoader: NETAPI32.DLL/NetQueryDisplayInformation
- DynamicLoader: NETAPI32.DLL/NetServerSetInfo
- DynamicLoader: NETAPI32.DLL/NetServerGetInfo
- DynamicLoader: NETAPI32.DLL/NetGetDCName
- DynamicLoader: NETAPI32.DLL/NetWkstaGetInfo
- DynamicLoader: NETAPI32.DLL/NetGetAnyDCName
- DynamicLoader: NETAPI32.DLL/NetServerEnum
- DynamicLoader: NETAPI32.DLL/NetUserModalsGet
- DynamicLoader: NETAPI32.DLL/NetScheduleJobAdd
- DynamicLoader: NETAPI32.DLL/NetScheduleJobDel
- DynamicLoader: NETAPI32.DLL/NetScheduleJobEnum
- DynamicLoader: NETAPI32.DLL/NetScheduleJobGetInfo
- DynamicLoader: NETAPI32.DLL/NetUseGetInfo
- DynamicLoader: NETAPI32.DLL/NetEnumerateTrustedDomains
- DynamicLoader: NETAPI32.DLL/DsGetDcNameW
- DynamicLoader: NETAPI32.DLL/DsRoleGetPrimaryDomainInformation
- DynamicLoader: NETAPI32.DLL/DsRoleFreeMemory
- DynamicLoader: NETAPI32.DLL/NetRenameMachineInDomain
- DynamicLoader: NETAPI32.DLL/NetJoinDomain
- DynamicLoader: NETAPI32.DLL/NetUnjoinDomain
- DynamicLoader: WKSCLI.DLL/NetWkstaGetInfo
- DynamicLoader: cscapi.dll/CscNetApiGetInterface
- DynamicLoader: kernel32.dll/GetDiskFreeSpaceExW
- DynamicLoader: kernel32.dll/GetVolumePathNameW
- DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
- DynamicLoader: kernel32.dll/Thread32First
- DynamicLoader: kernel32.dll/Thread32Next
- DynamicLoader: kernel32.dll/Process32First
- DynamicLoader: kernel32.dll/Process32Next
- DynamicLoader: kernel32.dll/Module32First
- DynamicLoader: kernel32.dll/Module32Next
- DynamicLoader: kernel32.dll/Heap32ListFirst
- DynamicLoader: kernel32.dll/GlobalMemoryStatusEx
- DynamicLoader: kernel32.dll/GetSystemDefaultUILanguage
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextW

- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: SHLWAPI.dll/PathIsDirectoryW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegNotifyChangeKeyValue
- DynamicLoader: SspiCli.dll/GetUserNameExW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: ole32.dll/NdrOleInitializeExtension
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: ole32.dll/CLSIDFromOle1Class
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject
- DynamicLoader: CLBCatQ.DLL/GetCatalogObject2
- DynamicLoader: tschannel.dll/DllGetClassObject
- DynamicLoader: tschannel.dll/DllCanUnloadNow
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: SHLWAPI.dll/PathIsPrefixW
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: XmlLite.dll/CreateXmlReader
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: kernel32.dll/FlsAlloc
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: kernel32.dll/FlsSetValue
- DynamicLoader: kernel32.dll/FlsFree
- DynamicLoader: kernel32.dll/IsProcessorFeaturePresent
- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: kernel32.dll/FlsAlloc
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: kernel32.dll/FlsSetValue
- DynamicLoader: kernel32.dll/FlsFree
- DynamicLoader: kernel32.dll/IsProcessorFeaturePresent

- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: WS2_32.dll/GetAddrInfoW
- DynamicLoader: WS2_32.dll/WSASocketW
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/WSAIoctl
- DynamicLoader: WS2_32.dll/FreeAddrInfoW
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: schannel.dll/SpUserModeInitialize
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: WS2_32.dll/WSASend
- DynamicLoader: WS2_32.dll/WSARecv
- DynamicLoader: secur32.dll/FreeContextBuffer
- DynamicLoader: ncrypt.dll/SslOpenProvider
- DynamicLoader: ncrypt.dll/GetSChannelInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: ncrypt.dll/SslIncrementProviderReferenceCount
- DynamicLoader: ncrypt.dll/SslImportKey
- DynamicLoader: bcryptprimitives.dll/GetCipherInterface
- DynamicLoader: ncrypt.dll/SslLookupCipherSuiteInfo
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: ncrypt.dll/BCryptOpenAlgorithmProvider
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: ncrypt.dll/BCryptGetProperty
- DynamicLoader: ncrypt.dll/BCryptCreateHash
- DynamicLoader: ncrypt.dll/BCryptHashData
- DynamicLoader: ncrypt.dll/BCryptFinishHash
- DynamicLoader: ncrypt.dll/BCryptDestroyHash
- DynamicLoader: CRYPT32.dll/CertGetCertificateChain
- DynamicLoader: USERENV.dll/GetUserProfileDirectoryW
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: sechost.dll/ConvertStringSidToSidW
- DynamicLoader: USERENV.dll/RegisterGPNotification
- DynamicLoader: GPAPI.dll/RegisterGPNotificationInternal
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: sechost.dll/QueryServiceConfigW
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptVerifySignatureA
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: cryptnet.dll/CryptRetrieveObjectByUrlW
- DynamicLoader: cryptnet.dll/I_CryptNetGetConnectivity
- DynamicLoader: SensApi.dll/IsNetworkAlive
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/NdrClientCall2
- DynamicLoader: cryptnet.dll/CryptRetrieveObjectByUrlW
- DynamicLoader: WINHTTP.dll/WinHttpOpen
- DynamicLoader: WINHTTP.dll/WinHttpSetTimeouts
- DynamicLoader: WINHTTP.dll/WinHttpSetOption

- DynamicLoader: WINHTTP.dll/WinHttpCrackUrl
- DynamicLoader: WINHTTP.dll/WinHttpConnect
- DynamicLoader: WINHTTP.dll/WinHttpOpenRequest
- DynamicLoader: WINHTTP.dll/WinHttpGetDefaultProxyConfiguration
- DynamicLoader: WINHTTP.dll/WinHttpGetIEProxyConfigForCurrentUser
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ADVAPI32.dll/RegDeleteTreeA
- DynamicLoader: ADVAPI32.dll/RegDeleteTreeW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: NSI.dll/NsiAllocateAndGetTable
- DynamicLoader: CFGMGR32.dll/CM_Open_Class_Key_ExW
- DynamicLoader: IPHLPAPI.DLL/ConvertInterfaceGuidToLuid
- DynamicLoader: IPHLPAPI.DLL/GetIfEntry2
- DynamicLoader: IPHLPAPI.DLL/GetIpForwardTable2
- DynamicLoader: IPHLPAPI.DLL/GetIpNetEntry2
- DynamicLoader: IPHLPAPI.DLL/FreeMibTable
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: NSI.dll/NsiFreeTable
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: WINHTTP.dll/WinHttpGetProxyForUrl
- DynamicLoader: ADVAPI32.dll/RegDeleteTreeA
- DynamicLoader: ADVAPI32.dll/RegDeleteTreeW
- DynamicLoader: WINHTTP.dll/WinHttpSendRequest
- DynamicLoader: WINHTTP.dll/WinHttpReceiveResponse
- DynamicLoader: WINHTTP.dll/WinHttpQueryHeaders
- DynamicLoader: WINHTTP.dll/WinHttpQueryDataAvailable
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WINHTTP.dll/WinHttpReadData
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WINHTTP.dll/WinHttpCloseHandle
- DynamicLoader: cryptnet.dll/I_CryptNetSetUrlCacheFlushInfo
- DynamicLoader: setupapi.dll/SetupIterateCabinetW
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: Cabinet.dll/
- DynamicLoader: Cabinet.dll/
- DynamicLoader: Cabinet.dll/
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceConfigA
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeA
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingA
- DynamicLoader: RPCRT4.dll/RpcEpResolveBinding
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: RPCRT4.dll/RpcStringFreeA
- DynamicLoader: RPCRT4.dll/NdrClientCall2
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: bcryptprimitives.dll/GetHashInterface
- DynamicLoader: CRYPT32.dll/CertVerifyCertificateChainPolicy
- DynamicLoader: CRYPT32.dll/CertFreeCertificateChain
- DynamicLoader: CRYPT32.dll/CertDuplicateCertificateContext
- DynamicLoader: CRYPT32.dll/CertFreeCertificateContext
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: sechost.dll/LookupAccountNameLocalW

- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: kernel32.dll/GetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/SetThreadPreferredUILanguages
- DynamicLoader: kernel32.dll/LocaleNameToLCID
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/LCIDToLocaleName
- DynamicLoader: kernel32.dll/GetSystemDefaultLocaleName
- DynamicLoader: fastprox.dll/DllGetClassObject
- DynamicLoader: fastprox.dll/DllCanUnloadNow
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: PSAPI.DLL/EnumProcesses
- DynamicLoader: PSAPI.DLL/EnumProcessModules
- DynamicLoader: PSAPI.DLL/GetModuleBaseNameW
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: USER32.dll/GetLastInputInfo
- 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: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: kernel32.dll/RegOpenKeyExW
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ole32.dll/CLSIDFromString
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoGetCallContext
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: ADVAPI32.dll/EventWrite
- DynamicLoader: ADVAPI32.dll/EventActivityIdControl
- DynamicLoader: ADVAPI32.dll/EventWriteTransfer
- DynamicLoader: ADVAPI32.dll/EventEnabled

A process attempted to delay the analysis task.

- Process: WmiPrvSE.exe tried to sleep 361 seconds, actually delayed analysis time by 0 seconds
- Process: whe.exe tried to sleep 513 seconds, actually delayed analysis time by 0 seconds

Guard pages use detected - possible anti-debugging.

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

- process: FlashPlayerUpdateService.exe, PID 2356

Creates RWX memory

Attempts to connect to a dead IP:Port (2 unique times)

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

SetUnhandledExceptionFilter detected (possible anti-debug)

1 HTTP Request(s) detected

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab

Hostname: www.download.windowsupdate.com
IP Address: 93.184.221.240
Port: 80
Count: 1