Scanned.exe

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

MalFamily: Razy **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	314.34 KB (321888 bytes)
Compile time:	2018-11-01 20:43:39
MD5:	d30bd44d161347d5ecf0aa5f6ee9506e
SHA1:	e70a38e58e2c0d5f28b911859612067574c16c74
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-12-01 03:48:06

URL(s) file hosting

http://ifcjohannesburg.org/11/Scanned.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-11-29 21:27:16	46/70	

Import library

mscoree.dll

17 Behaviors detected by system signatures

Attempts to modify or disable Security Center warnings

Attempts to disable UAC

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\FolderN\name.exe

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Roaming\FolderN

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
- data: C:\Users\Seven01\AppData\Roaming\FolderN\name.exe.lnk

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

- Injection: Scanned.exe(2748) -> Scanned.exe(2436)

Uses Windows utilities for basic functionality

- command: "cmd.exe"
- command: reg add "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows" /v Load /t REG_SZ /d "C:\Users\Seven01\AppData\Roaming\FolderN\name.exe.lnk" /f
- command: C:\Program Files (x86)\Internet Explorer\iexplore.exe C:\Users\Seven01\AppData\Local\Temp\Scanned.exe
- command: C:\Program Files (x86)\Internet Explorer\iexplore.exe C:\Users\Seven01\AppData\Roaming\tmp.exe

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.81, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00031c00, virtual_size: 0x00031ae4

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Roaming\tmp.exe

A process created a hidden window

- Process: Scanned.exe -> "cmd.exe"

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

- ioc: v2.0.50727

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: 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: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptExportKey
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: mscorjit.dll/getJit
- DynamicLoader: KERNEL32.dll/IsWow64Process
- DynamicLoader: mscorwks.dll/StrongNameSignatureVerificationEx
- DynamicLoader: mscorwks.dll/StrongNameSignatureVerificationExW
- DynamicLoader: MSCOREE.DLL/GetMetaDataInternalInterface
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface_RetAddr
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface
- DynamicLoader: mscorwks.dll/GetMetaDataInternalInterface
- DynamicLoader: CRYPTSP.dll/CryptVerifySignatureA
- DynamicLoader: KERNEL32.dll/GetUserDefaultUILanguage
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentThread
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: KERNEL32.dll/GetCurrentThreadId
- DynamicLoader: ole32.dll/OleInitialize
- DynamicLoader: KERNEL32.dll/lstrlen
- DynamicLoader: KERNEL32.dll/lstrlenW
- DynamicLoader: ole32.dll/CoRegisterMessageFilter
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetCurrentProcessId
- DynamicLoader: KERNEL32.dll/GetCurrentProcessIdW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValue
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivilegesW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/OpenProcess
- DynamicLoader: KERNEL32.dll/OpenProcessW
- DynamicLoader: KERNEL32.dll/GetExitCodeProcess
- DynamicLoader: KERNEL32.dll/GetExitCodeProcessW
- DynamicLoader: KERNEL32.dll/SetProcessWorkingSetSize
- DynamicLoader: mscorwks.dll/StrongNameSignatureVerificationEx
- DynamicLoader: mscorwks.dll/StrongNameSignatureVerificationExW
- DynamicLoader: MSCOREE.DLL/GetMetaDataInternalInterface
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariable
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariableW
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtQuerySystemInformationW
- DynamicLoader: KERNEL32.dll/SetErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: mscoreei.dll/LoadLibraryShim_RetAddr

- DynamicLoader: mscoreei.dll/LoadLibraryShim
- DynamicLoader: culture.dll/ConvertLangIdToCultureName
- DynamicLoader: CRYPTSP.dll/CryptGetProvParam
- DynamicLoader: CRYPTSP.dll/CryptSetKeyParam
- DynamicLoader: CRYPTSP.dll/CryptDecrypt
- DynamicLoader: CRYPTSP.dll/CryptEncrypt
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: KERNEL32.dll/GetACP
- DynamicLoader: KERNEL32.dll/UnmapViewOfFile
- DynamicLoader: KERNEL32.dll/CreateDirectory
- DynamicLoader: KERNEL32.dll/CreateDirectoryW
- DynamicLoader: KERNEL32.dll/SetFileAttributes
- DynamicLoader: KERNEL32.dll/SetFileAttributesW
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: KERNEL32.dll/CreatePipe
- DynamicLoader: KERNEL32.dll/CreatePipeW
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: KERNEL32.dll/GetCurrentDirectory
- DynamicLoader: KERNEL32.dll/GetCurrentDirectoryW
- DynamicLoader: KERNEL32.dll/CreateProcess
- DynamicLoader: KERNEL32.dll/CreateProcessW
- DynamicLoader: KERNEL32.dll/GetFileType
- DynamicLoader: KERNEL32.dll/GetConsoleCP
- DynamicLoader: KERNEL32.dll/GetConsoleCPW
- DynamicLoader: KERNEL32.dll/GetConsoleOutputCP
- DynamicLoader: KERNEL32.dll/GetConsoleOutputCPW
- DynamicLoader: KERNEL32.dll/WriteFile
- DynamicLoader: ole32.dll/CLSIDFromProgIDEx
- DynamicLoader: sxs.dll/SxsLookupClrGuid
- DynamicLoader: KERNEL32.dll/ReleaseActCtx
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: sxs.dll/SxsOleAut32RedirectTypeLibrary
- DynamicLoader: ADVAPI32.dll/RegOpenKeyW
- DynamicLoader: ADVAPI32.dll/RegQueryValueW
- DynamicLoader: sxs.dll/SxsOleAut32MapConfiguredClsidToReferenceClsid
- 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: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.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: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: propsys.dll/PSCreateMemoryPropertyStore
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetApartmentType
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetMalloc
- DynamicLoader: ole32.dll/CreateBindCtx
- 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: comctl32.dll/
- DynamicLoader: shell32.dll/
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: ole32.dll/PropVariantClear
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_ExW
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: comctl32.dll/
- DynamicLoader: ADVAPI32.dll/RegQueryValueW
- DynamicLoader: apphelp.dll/ApphelpCheckShellObject
- DynamicLoader: LINKINFO.dll/CreateLinkInfoW
- DynamicLoader: USER32.dll/IsCharAlphaW
- DynamicLoader: USER32.dll/CharPrevW
- DynamicLoader: ntshrui.dll/GetNetResourceFromLocalPathW
- DynamicLoader: srvcli.dll/NetShareEnum
- DynamicLoader: cscapi.dll/CscNetApiGetInterface
- DynamicLoader: slc.dll/SLGetWindowsInformationDWORD
- DynamicLoader: SHLWAPI.dll/PathRemoveFileSpecW
- DynamicLoader: LINKINFO.dll/DestroyLinkInfo
- DynamicLoader: KERNEL32.dll/CopyFile
- DynamicLoader: KERNEL32.dll/CopyFileW
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: ole32.dll/CoWaitForMultipleHandles
- DynamicLoader: mscorwks.dll/StrongNameSignatureVerificationEx
- DynamicLoader: mscorwks.dll/StrongNameSignatureVerificationExW
- DynamicLoader: MSCOREE.DLL/GetMetaDataInternalInterface
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: KERNEL32.dll/RtlMoveMemory
- DynamicLoader: KERNEL32.dll/RtlMoveMemoryW
- DynamicLoader: shell32.dll/ShellExecuteEx
- DynamicLoader: shell32.dll/ShellExecuteExW
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: KERNEL32.dll/DeleteFile
- DynamicLoader: KERNEL32.dll/DeleteFileW
- DynamicLoader: mscorwks.dll/StrongNameSignatureVerificationEx
- DynamicLoader: mscorwks.dll/StrongNameSignatureVerificationExW
- DynamicLoader: MSCOREE.DLL/GetMetaDataInternalInterface
- DynamicLoader: KERNEL32.dll/LoadLibraryA
- DynamicLoader: KERNEL32.dll/GetProcAddress
- DynamicLoader: KERNEL32.dll/CreateProcessA
- DynamicLoader: KERNEL32.dll/ReadProcessMemory

- DynamicLoader: KERNEL32.dll/WriteProcessMemory
- DynamicLoader: KERNEL32.dll/GetThreadContext
- DynamicLoader: ntdll.dll/NtSetContextThread
- DynamicLoader: ntdll.dll/NtUnmapViewOfSection
- DynamicLoader: KERNEL32.dll/VirtualAllocEx
- DynamicLoader: ntdll.dll/NtResumeThread
- DynamicLoader: KERNEL32.dll/GetStartupInfo
- DynamicLoader: KERNEL32.dll/GetStartupInfoW
- DynamicLoader: KERNEL32.dll/CreateProcess
- DynamicLoader: KERNEL32.dll/CreateProcessW
- DynamicLoader: USER32.dll/WaitForInputIdle
- DynamicLoader: USER32.dll/WaitForInputIdleW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: netutils.dll/NetApiBufferFree
- DynamicLoader: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: comctl32.dll/
- DynamicLoader: KERNEL32.dll/CreateActCtxW
- DynamicLoader: KERNEL32.dll/AddRefActCtx
- DynamicLoader: KERNEL32.dll/ReleaseActCtx
- DynamicLoader: KERNEL32.dll/ActivateActCtx
- DynamicLoader: KERNEL32.dll/DeactivateActCtx
- DynamicLoader: KERNEL32.dll/GetCurrentActCtx
- DynamicLoader: KERNEL32.dll/QueryActCtxW
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: kernel32.dll/SetThreadUILanguage
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: kernel32.dll/CopyFileExW
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: kernel32.dll/SetConsoleInputExeNameW
- DynamicLoader: ntdll.dll/NtQueryInformationProcess
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- 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/VarDateFromUdate
- DynamicLoader: OLEAUT32.dll/VarUdateFromDate
- 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/VarCyMulI4
- 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: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: LPK.dll/LpkEditControl
- DynamicLoader: comctl32.DLL/HIMAGELIST_QueryInterface
- DynamicLoader: comctl32.DLL/DrawShadowText
- DynamicLoader: comctl32.DLL/DrawSizeBox
- DynamicLoader: comctl32.DLL/DrawScrollBar
- DynamicLoader: comctl32.DLL/SizeBoxHwnd
- DynamicLoader: comctl32.DLL/ScrollBar_MouseMove
- DynamicLoader: comctl32.DLL/ScrollBar_Menu
- DynamicLoader: comctl32.DLL/HandleScrollCmd
- DynamicLoader: comctl32.DLL/DetachScrollBars
- DynamicLoader: comctl32.DLL/AttachScrollBars
- DynamicLoader: comctl32.DLL/CCSetScrollInfo
- DynamicLoader: comctl32.DLL/CCGetScrollInfo
- DynamicLoader: comctl32.DLL/CCEnableScrollBar
- DynamicLoader: comctl32.DLL/QuerySystemGestureStatus
- DynamicLoader: uxtheme.dll/
- DynamicLoader: uxtheme.dll/CloseThemeData
- DynamicLoader: GDI32.dll/GetLayout
- DynamicLoader: GDI32.dll/GdiRealizationInfo

- DynamicLoader: GDI32.dll/FontIsLinked
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: GDI32.dll/GetTextFaceAliasW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: GDI32.dll/GetFontAssocStatus
- DynamicLoader: ADVAPI32.dll/RegQueryValueExA
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: GDI32.dll/GetTextFaceAliasW
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: kernel32.dll/GetModuleHandleA
- DynamicLoader: kernel32.dll/GetProcAddress
- DynamicLoader: kernel32.dll/SetProcessDEPPolicy
- DynamicLoader: kernel32.dll/SetProcessDEPPolicy
- DynamicLoader: USER32.dll/CallWindowProcA
- DynamicLoader: PSAPI.DLL/EnumProcesses
- DynamicLoader: kernel32.dll/OpenProcess
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: PSAPI.DLL/EnumProcessModules
- DynamicLoader: PSAPI.DLL/GetModuleBaseNameA
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.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/VarDateFromUdate
- DynamicLoader: OLEAUT32.dll/VarUdateFromDate
- 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: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: LPK.dll/LpkEditControl
- DynamicLoader: comctl32.DLL/HIMAGELIST_QueryInterface
- DynamicLoader: comctl32.DLL/DrawShadowText
- DynamicLoader: comctl32.DLL/DrawSizeBox
- DynamicLoader: comctl32.DLL/DrawScrollBar
- DynamicLoader: comctl32.DLL/SizeBoxHwnd
- DynamicLoader: comctl32.DLL/ScrollBar_MouseMove
- DynamicLoader: comctl32.DLL/ScrollBar_Menu
- DynamicLoader: comctl32.DLL/HandleScrollCmd
- DynamicLoader: comctl32.DLL/DetachScrollBars
- DynamicLoader: comctl32.DLL/AttachScrollBars
- DynamicLoader: comctl32.DLL/CCSetScrollInfo
- DynamicLoader: comctl32.DLL/CCGetScrollInfo
- DynamicLoader: comctl32.DLL/CCEnableScrollBar
- DynamicLoader: comctl32.DLL/QuerySystemGestureStatus
- DynamicLoader: UxTheme.dll/
- DynamicLoader: UxTheme.dll/CloseThemeData
- DynamicLoader: GDI32.dll/GetLayout
- DynamicLoader: GDI32.dll/GdiRealizationInfo
- DynamicLoader: GDI32.dll/FontIsLinked
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: GDI32.dll/GetTextFaceAliasW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: GDI32.dll/GetFontAssocStatus

- DynamicLoader: ADVAPI32.dll/RegQueryValueExA
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: GDI32.dll/GetTextFaceAliasW
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: kernel32.dll/GetModuleHandleA
- DynamicLoader: kernel32.dll/GetProcAddress
- DynamicLoader: kernel32.dll/SetProcessDEPPolicy
- DynamicLoader: kernel32.dll/SetProcessDEPPolicy
- DynamicLoader: USER32.dll/CallWindowProcA
- DynamicLoader: PSAPI.DLL/EnumProcesses
- DynamicLoader: kernel32.dll/OpenProcess
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: PSAPI.DLL/EnumProcessModules
- DynamicLoader: PSAPI.DLL/GetModuleBaseNameA
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: kernel32.dll/SetThreadUILanguage
- DynamicLoader: kernel32.dll/CopyFileExW
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: kernel32.dll/SetConsoleInputExeNameW
- DynamicLoader: ADVAPI32.dll/SaferIdentifyLevel
- DynamicLoader: ADVAPI32.dll/SaferComputeTokenFromLevel
- DynamicLoader: ADVAPI32.dll/SaferCloseLevel
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- 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/VarDateFromUdate
- DynamicLoader: OLEAUT32.dll/VarUdateFromDate
- 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: VERSION.dll/VerQueryValueA
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeA
- DynamicLoader: VERSION.dll/GetFileVersionInfoA
- 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: kernel32.dll/GetModuleHandleA
- DynamicLoader: kernel32.dll/GetProcAddress
- DynamicLoader: kernel32.dll/SetProcessDEPPolicy
- DynamicLoader: kernel32.dll/SetProcessDEPPolicy
- DynamicLoader: OLE32.DLL/CoCreateGuid
- DynamicLoader: OLE32.DLL/StringFromGUID2
- DynamicLoader: kernel32.dll/NlsGetCacheUpdateCount
- DynamicLoader: kernel32.dll/GetCurrentProcess
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueA
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/CreateMutexA
- DynamicLoader: kernel32.dll/WaitForSingleObject
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- 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/VarDateFromUdate
- DynamicLoader: OLEAUT32.dll/VarUdateFromDate

- 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/VarCyMulI4
- DynamicLoader: OLEAUT32.dll/VarBstrCmp
- DynamicLoader: OLE32.DLL/CoCreateInstanceEx
- DynamicLoader: OLE32.DLL/CLSIDFromProgIDEx
- DynamicLoader: VERSION.DLL/VerQueryValueA
- DynamicLoader: VERSION.DLL/GetFileVersionInfoSizeA
- DynamicLoader: VERSION.DLL/GetFileVersionInfoA
- 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: kernel32.dll/GetModuleHandleA

- DynamicLoader: kernel32.dll/GetProcAddress
- DynamicLoader: kernel32.dll/SetProcessDEPPolicy
- DynamicLoader: kernel32.dll/SetProcessDEPPolicy
- DynamicLoader: OLE32.DLL/CoCreateGuid
- DynamicLoader: OLE32.DLL/StringFromGUID2
- DynamicLoader: kernel32.dll/NlsGetCacheUpdateCount
- DynamicLoader: kernel32.dll/GetCurrentProcess
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueA
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/CreateMutexA
- DynamicLoader: kernel32.dll/WaitForSingleObject
- DynamicLoader: kernel32.dll/RtlMoveMemory
- DynamicLoader: USER32.dll/SetTimer
- DynamicLoader: ws2_32.dll/WSAStartup
- DynamicLoader: USER32.dll/CreateWindowExA
- DynamicLoader: USER32.dll/SetWindowLongA
- DynamicLoader: kernel32.dll/GetFileAttributesW
- DynamicLoader: kernel32.dll/GetVersion
- DynamicLoader: Shell32.DLL/
- DynamicLoader: Secur32.dll/GetUserNameExW
- DynamicLoader: OLE32.DLL/CoCreateInstance
- DynamicLoader: ADVAPI32.dll/LsaOpenPolicy
- DynamicLoader: ADVAPI32.dll/LsaQueryInformationPolicy
- DynamicLoader: ADVAPI32.dll/GetLengthSid
- DynamicLoader: OLE32.DLL/CoTaskMemAlloc
- DynamicLoader: ADVAPI32.dll/GetLengthSid
- DynamicLoader: ADVAPI32.dll/CopySid
- DynamicLoader: ADVAPI32.dll/LsaFreeMemory
- DynamicLoader: ADVAPI32.dll/LsaClose
- DynamicLoader: SAMLIB.dll/SamConnect
- DynamicLoader: RPCRT4.dll/NdrClientCall2
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeW
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcStringFreeW
- DynamicLoader: RPCRT4.dll/RpcBindingFree
- DynamicLoader: SAMLIB.dll/SamOpenDomain
- DynamicLoader: SAMLIB.dll/SamCloseHandle
- DynamicLoader: SAMLIB.dll/SamLookupNamesInDomain
- DynamicLoader: SAMLIB.dll/SamFreeMemory
- DynamicLoader: SAMLIB.dll/SamLookupIdsInDomain
- DynamicLoader: SAMLIB.dll/SamOpenUser
- DynamicLoader: SAMLIB.dll/SamQueryInformationUser
- DynamicLoader: OLE32.DLL/CoGetMalloc
- DynamicLoader: OLE32.DLL/CoTaskMemFree
- DynamicLoader: OLE32.DLL/PropVariantClear
- DynamicLoader: PROPSYS.dll/VariantToPropVariant
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: PROPSYS.dll/PropVariantToUInt32
- DynamicLoader: USER32.dll/CreateWindowExW
- DynamicLoader: USER32.dll/RegisterRawInputDevices
- DynamicLoader: USER32.dll/RegisterWindowMessageW
- DynamicLoader: Shell32.DLL/
- DynamicLoader: USER32.dll/SetClipboardViewer
- DynamicLoader: USER32.dll/SetWindowLongA
- DynamicLoader: kernel32.dll/GetCalendarInfoW
- DynamicLoader: USER32.dll/SendMessageA
- DynamicLoader: USER32.dll/CallWindowProcA
- DynamicLoader: ws2_32.dll/htons
- DynamicLoader: ws2_32.dll/inet_addr
- DynamicLoader: ws2_32.dll/socket
- DynamicLoader: ws2_32.dll/connect

- DynamicLoader: ws2_32.dll/closesocket
- DynamicLoader: kernel32.dll/Sleep
- DynamicLoader: USER32.dll/GetLastInputInfo
- DynamicLoader: kernel32.dll/GetTickCount
- 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/VarDateFromUdate
- DynamicLoader: OLEAUT32.dll/VarUdateFromDate
- 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/VarCyMulI4

- DynamicLoader: OLEAUT32.dll/VarBstrCmp
- DynamicLoader: OLE32.DLL/CoCreateInstanceEx
- DynamicLoader: OLE32.DLL/CLSIDFromProgIDEx
- DynamicLoader: VERSION.dll/VerQueryValueA
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeA
- DynamicLoader: VERSION.dll/GetFileVersionInfoA
- 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: kernel32.dll/GetModuleHandleA
- DynamicLoader: kernel32.dll/GetProcAddress
- DynamicLoader: kernel32.dll/SetProcessDEPPolicy
- DynamicLoader: kernel32.dll/SetProcessDEPPolicy
- DynamicLoader: OLE32.DLL/CoCreateGuid
- DynamicLoader: OLE32.DLL/StringFromGUID2
- DynamicLoader: kernel32.dll/NlsGetCacheUpdateCount
- DynamicLoader: kernel32.dll/GetCurrentProcess
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueA
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/CreateMutexA
- DynamicLoader: kernel32.dll/WaitForSingleObject
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/
- 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/VarDateFromUdate
- DynamicLoader: OLEAUT32.dll/VarUdateFromDate
- 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: VERSION.DLL/VerQueryValueA
- DynamicLoader: VERSION.DLL/GetFileVersionInfoSizeA
- DynamicLoader: VERSION.DLL/GetFileVersionInfoA
- 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: kernel32.dll/GetModuleHandleA
- DynamicLoader: kernel32.dll/GetProcAddress
- DynamicLoader: kernel32.dll/SetProcessDEPPolicy
- DynamicLoader: kernel32.dll/SetProcessDEPPolicy
- DynamicLoader: OLE32.DLL/CoCreateGuid
- DynamicLoader: OLE32.DLL/StringFromGUID2
- DynamicLoader: kernel32.dll/NlsGetCacheUpdateCount
- DynamicLoader: kernel32.dll/GetCurrentProcess
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueA
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/CreateMutexA
- DynamicLoader: kernel32.dll/WaitForSingleObject
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: OLEAUT32.dll/

Guard pages use detected - possible anti-debugging.

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

- process: Scanned.exe, PID 2436

Creates RWX memory

Attempts to connect to a dead IP:Port (1 unique times)

- IP: 46.183.220.104:10101 (Latvia)

SetUnhandledExceptionFilter detected (possible anti-debug)

1 Host(s) detected

IP Address	Hostname	Reverse DNS
46.183.220.104		ip-220-104.dataclub.eu.

1 Countr(y|ies) detected

Hosts	Country
1	Latvia