Purchase%20Order.exe

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

MalFamily: Lokibot **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	565.50 KB (579072 bytes)
Compile time:	2018-11-02 17:00:25
MD5:	07086eafd9df9870e02d2aea71cc2fd7
SHA1:	bd63386f10e61ddcea32647a1e2fb79635bb9353
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-11-04 13:51:04

URL(s) file hosting

https://dealertrafficgenerator.com/Oja/Purchase%20Order.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-11-03 16:00:21	24/67	

Import library

mscoree.dll

18 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET TROJAN LokiBot User-Agent (Charon/Inferno)

- signature: ET TROJAN LokiBot Checkin
- signature: ET TROJAN LokiBot Request for C2 Commands Detected M2
- signature: ET TROJAN LokiBot Request for C2 Commands Detected M1
- signature: ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1
- signature: ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2

Collects information to fingerprint the system

Harvests information related to installed mail clients

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7d19c9e894f20d4780a31c9a9f17da11
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\00471e98b7a362469ed97e3915fd4111
- 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\{D9734F19-8CFB-411D-BC59-833E334FCB5E}
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\10b0e4d6eb1de34dabd532a0806a0fec\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\818ecc2f310b344f807e8af5dc013189\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\192e64c97bf3a54488a039619c763627
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\32a3dc9c400a4b448b60ab7fe553a392\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\32a3dc9c400a4b448b60ab7fe553a392
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\818ecc2f310b344f807e8af5dc013189
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\43e0bb79f0f2d84db98ff4f730d23d24
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7760e21103136b47946c9c80fa097f15
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Email
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\Email
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\6a50d9bd87f9a8478751861a1591a6c2
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\6a50d9bd87f9a8478751861a1591a6c2\Email
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\192e64c97bf3a54488a039619c763627\Email
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\10b0e4d6eb1de34dabd532a0806a0fec
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ddb0922fc50b8d42be5a821ede840761\Email
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ddb0922fc50b8d42be5a821ede840761
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7d19c9e894f20d4780a31c9a9f17da11\Email
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Email
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7760e21103136b47946c9c80fa097f15\Email
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Email
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\Email
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\43e0bb79f0f2d84db98ff4f730d23d24\Email
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\00471e98b7a362469ed97e3915fd4111\Email
 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\Email
 - key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook
 - key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook

Harvests information related to installed instant messenger clients

 - file: C:\Users\Seven01\AppData\Roaming\.purple\accounts.xml

Harvests credentials from local FTP client softwares

 - file: C:\Users\Seven01\AppData\Roaming\FileZilla\sitemanager.xml
 - file: C:\Users\Seven01\AppData\Roaming\FileZilla\recentservers.xml
 - file: C:\Users\Seven01\AppData\Roaming\Far Manager\Profile\PluginsData\42E4AEB1-A230-44F4-B33C-F195BB654931.db
 - file: C:\Program Files (x86)\FTPGetter\Profile\servers.xml
 - file: C:\Users\Seven01\AppData\Roaming\FTPGetter\servers.xml
 - file: C:\Users\Seven01\AppData\Roaming\Estsoft\ALFTP\ESTdb2.dat
 - key: HKEY_CURRENT_USER\Software\Far\Plugins\FTP\Hosts
 - key: HKEY_CURRENT_USER\Software\Far2\Plugins\FTP\Hosts
 - key: HKEY_CURRENT_USER\Software\Ghisler\Total Commander
 - key: HKEY_CURRENT_USER\Software\LinasFTP\Site Manager

Creates a hidden or system file

 - file: C:\Users\Seven01\AppData\Roaming\E62877\73E4A9.exe
 - file: C:\Users\Seven01\AppData\Roaming\E62877

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

- Spam: services.exe (480) called API GetSystemTimeAsFileTime 3847480 times

Queries information on disks, possibly for anti-virtualization

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

- Injection: Purchase20Order.exe(808) -> vbc.exe(2740)

Uses Windows utilities for basic functionality

- command: C:\Windows\system32\sc.exe start w32time task_started

Anomalous .NET characteristics

- anomalous_version: Assembly version is set to 0

Performs some HTTP requests

- url: http://publicspeaking.co.id/ojaa/Panel/five/fre.php

HTTP traffic contains suspicious features which may be indicative of malware related traffic

- post_no_referer: HTTP traffic contains a POST request with no referer header
- http_version_old: HTTP traffic uses version 1.0
- suspicious_request: http://publicspeaking.co.id/ojaa/Panel/five/fre.php

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/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/EventSetInformation
- DynamicLoader: clr.dll/SetRuntimeInfo
- DynamicLoader: clr.dll/_CorExeMain
- DynamicLoader: MSCOREE.DLL/CreateConfigStream
- DynamicLoader: mscoreei.dll/CreateConfigStream_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream
- DynamicLoader: KERNEL32.dll/GetNumaHighestNodeNumber
- DynamicLoader: KERNEL32.dll/FlsSetValue
- DynamicLoader: KERNEL32.dll/FlsGetValue
- DynamicLoader: KERNEL32.dll/FlsAlloc
- DynamicLoader: KERNEL32.dll/FlsFree

- DynamicLoader: KERNEL32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/AddSIDToBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/CreateBoundaryDescriptorW
- DynamicLoader: KERNEL32.dll/CreatePrivateNamespaceW
- DynamicLoader: KERNEL32.dll/OpenPrivateNamespaceW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: KERNEL32.dll/DeleteBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/WerRegisterRuntimeExceptionModule
- DynamicLoader: KERNEL32.dll/RaiseException
- DynamicLoader: MSCOREE.DLL/
- DynamicLoader: mscoreei.dll/
- DynamicLoader: KERNELBASE.dll/SetSystemFileCacheSize
- DynamicLoader: ntdll.dll/NtSetSystemInformation
- DynamicLoader: KERNELBASE.dll/PrivIsDllSynchronizationHeld
- DynamicLoader: KERNEL32.dll/AddDllDirectory
- DynamicLoader: KERNEL32.dll/SortGetHandle
- DynamicLoader: KERNEL32.dll/SortCloseHandle
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/ReleaseMutex
- DynamicLoader: KERNEL32.dll/CreateMutex
- DynamicLoader: KERNEL32.dll/CreateMutexW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetUserPreferredUILanguages
- DynamicLoader: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr

- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: KERNEL32.dll/SetThreadErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: KERNEL32.dll/CompareStringOrdinal
- DynamicLoader: clr.dll/CreateAssemblyNameObject
- DynamicLoader: clr.dll/CreateAssemblyNameObjectW
- DynamicLoader: ole32.dll/CoGetObjectContext
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: ole32.dll/NdrOleInitializeExtension
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: clr.dll/CreateAssemblyEnum
- DynamicLoader: clr.dll/CreateAssemblyEnumW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/ResolveLocaleName
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/LoadLibraryA
- DynamicLoader: KERNEL32.dll/WideCharToMultiByte
- DynamicLoader: KERNEL32.dll/GetProcAddress
- DynamicLoader: KERNEL32.dll/GetModuleHandleA
- 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/CreateProcessA
- DynamicLoader: KERNEL32.dll/GetThreadContext
- DynamicLoader: KERNEL32.dll/Wow64GetThreadContext
- DynamicLoader: KERNEL32.dll/SetThreadContext
- DynamicLoader: KERNEL32.dll/Wow64SetThreadContext
- DynamicLoader: KERNEL32.dll/ReadProcessMemory
- DynamicLoader: KERNEL32.dll/WriteProcessMemory
- DynamicLoader: ntdll.dll/NtUnmapViewOfSection
- DynamicLoader: KERNEL32.dll/VirtualAllocEx
- DynamicLoader: KERNEL32.dll/ResumeThread

- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: KERNEL32.dll/CreateActCtxW
- DynamicLoader: KERNEL32.dll/AddRefActCtx
- DynamicLoader: KERNEL32.dll/ReleaseActCtx
- DynamicLoader: KERNEL32.dll/ActivateActCtx
- DynamicLoader: KERNEL32.dll/DeactivateActCtx
- DynamicLoader: KERNEL32.dll/GetCurrentActCtx
- DynamicLoader: KERNEL32.dll/QueryActCtxW
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: vaultcli.dll/VaultEnumerateItems
- DynamicLoader: vaultcli.dll/VaultEnumerateVaults
- DynamicLoader: vaultcli.dll/VaultFree
- DynamicLoader: vaultcli.dll/VaultGetItem
- DynamicLoader: vaultcli.dll/VaultOpenVault
- DynamicLoader: vaultcli.dll/VaultCloseVault
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: NETAPI32.DLL/NetUserGetInfo
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptSetKeyParam
- DynamicLoader: CRYPTSP.dll/CryptDecrypt
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: NETAPI32.DLL/NetUserGetInfo
- DynamicLoader: NETAPI32.DLL/NetUserGetInfo
- DynamicLoader: SETUPAPI.dll/SetupDiGetClassDevsW
- DynamicLoader: SETUPAPI.dll/SetupDiEnumDeviceInfo
- DynamicLoader: SETUPAPI.dll/SetupDiGetDeviceRegistryPropertyW
- DynamicLoader: SETUPAPI.dll/SetupDiDestroyDeviceInfoList
- DynamicLoader: WINTRUST.dll/WinVerifyTrust
- DynamicLoader: SETUPAPI.dll/SetupDiEnumDeviceInterfaces
- DynamicLoader: SETUPAPI.dll/SetupDiGetDeviceInterfaceDetailW
- DynamicLoader: kernel32.dll/GetSystemFirmwareTable
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess

- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess

- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent

- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess

- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess

- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: ntdll.dll/ZwQueryInformationProcess
- DynamicLoader: dfdts.dll/DfdGetDefaultPolicyAndSMARTW
- DynamicLoader: dfdts.dll/DfdGetDefaultPolicyAndSMARTA
- DynamicLoader: dfdts.dll/DfdGetDefaultPolicyAndSMART
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ole32.dll/CoInitializeSecurity
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: w32time.dll/SvchostEntry_W32Time
- DynamicLoader: w32time.dll/SvchostPushServiceGlobals
- DynamicLoader: sechost.dll/ConvertStringSecurityDescriptorToSecurityDescriptorW
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/WSASocketW
- DynamicLoader: WS2_32.dll/WSAIoctl
- DynamicLoader: WS2_32.dll/
- 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: dsrole.dll/DsRoleGetPrimaryDomainInformation
- DynamicLoader: dsrole.dll/DsRoleFreeMemory
- DynamicLoader: SspiCli.dll/LsaRegisterPolicyChangeNotification
- DynamicLoader: w32time.dll/TimeProvClose
- DynamicLoader: w32time.dll/TimeProvCommand
- DynamicLoader: w32time.dll/TimeProvOpen
- DynamicLoader: WS2_32.dll/getaddrinfo
- DynamicLoader: WS2_32.dll/freeaddrinfo
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/WSAEventSelect
- DynamicLoader: WS2_32.dll/GetAddrInfoW
- DynamicLoader: vmictimeprovider.dll/TimeProvClose
- DynamicLoader: vmictimeprovider.dll/TimeProvCommand
- DynamicLoader: vmictimeprovider.dll/TimeProvOpen
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventEnabled
- DynamicLoader: ADVAPI32.dll/EventWrite
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: WS2_32.dll/FreeAddrInfoW
- DynamicLoader: WS2_32.dll/WSAAddressToStringW
- DynamicLoader: WS2_32.dll/
- DynamicLoader: WS2_32.dll/
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: SspiCli.dll/LsaUnregisterPolicyChangeNotification
- DynamicLoader: USERENV.dll/UnregisterGPNotification
- DynamicLoader: GPAPI.dll/UnregisterGPNotificationInternal

A process attempted to delay the analysis task.

- Process: vbc.exe tried to sleep 720 seconds, actually delayed analysis time by 0 seconds

Guard pages use detected - possible anti-debugging.

Creates RWX memory

SetUnhandledExceptionFilter detected (possible anti-debug)

2 HTTP Request(s) detected

http://publicspeaking.co.id/ojaa/Panel/five/fre.php
Hostname: publicspeaking.co.id
IP Address: 0.0.0.0
Port: 80
Count: 2

http://publicspeaking.co.id/ojaa/Panel/five/fre.php
Hostname: publicspeaking.co.id
IP Address: 0.0.0.0
Port: 80
Count: 12