flashupdate_022.exe

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

MalFamily: Msilperseus **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	127.50 KB (130560 bytes)
Compile time:	2018-01-23 04:53:17
MD5:	57e66eb958f00a58df90b24ce6a45f18
SHA1:	c0c7461fd08f0b60b40b8a0c940188bb4286c585
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-12-29 22:27:04

URL(s) file hosting

https://wonderful-davinci-e6a9e8.netlify.com/flashupdate_022.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-08-27 23:26:13	50/68	

Import library

mscoree.dll

13 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of

being hostile

Installs itself for autorun at Windows startup

- task: "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /TN web /MO 2 /TR %appdata%\web.exe /f

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

- Injection: flashupdate_022.exe(2744) -> flashupdate_022.exe(2056)

Uses Windows utilities for basic functionality

- command: "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /TN web /MO 2 /TR %appdata%\web.exe /f
- command: "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /TN web /MO 2 /TR %appdata%\web.exe /f
- command: schtasks /Create /SC MINUTE /TN web /MO 2 /TR %appdata%\web.exe /f
- command: schtasks /Create /SC MINUTE /TN web /MO 2 /TR %appdata%\web.exe /f

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: 0x0000ec00, virtual_size: 0x0000eac4

Performs some HTTP requests

- url: http://lancetasks.com/files/cinstaller.exe
- url: http://lancetasks.com/files/web.exe

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

- get_no_useragent: HTTP traffic contains a GET request with no user-agent header
- suspicious_request: http://lancetasks.com/files/cinstaller.exe
- suspicious_request: http://lancetasks.com/files/web.exe

Drops a binary and executes it

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

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/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- 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: uxtheme.dll/IsAppThemed
- DynamicLoader: uxtheme.dll/IsAppThemedW
- DynamicLoader: KERNEL32.dll/CreateActCtx
- DynamicLoader: KERNEL32.dll/CreateActCtxA
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: USER32.dll/RegisterWindowMessage
- DynamicLoader: USER32.dll/RegisterWindowMessageW
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/AdjustWindowRectEx
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentThread
- DynamicLoader: KERNEL32.dll/DuplicateHandle
- DynamicLoader: KERNEL32.dll/GetCurrentThreadId
- DynamicLoader: KERNEL32.dll/GetCurrentActCtx
- DynamicLoader: KERNEL32.dll/ActivateActCtx
- DynamicLoader: KERNEL32.dll/lstrlen
- DynamicLoader: KERNEL32.dll/lstrlenW
- DynamicLoader: KERNEL32.dll/GetModuleHandle
- DynamicLoader: KERNEL32.dll/GetModuleHandleW
- DynamicLoader: KERNEL32.dll/GetProcAddress
- DynamicLoader: USER32.dll/DefWindowProcW
- DynamicLoader: GDI32.dll/GetStockObject
- DynamicLoader: KERNEL32.dll/GetUserDefaultUILanguage
- DynamicLoader: USER32.dll/RegisterClass
- DynamicLoader: USER32.dll/RegisterClassW
- DynamicLoader: USER32.dll/CreateWindowEx
- DynamicLoader: USER32.dll/CreateWindowExW
- DynamicLoader: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/GetWindowLong
- DynamicLoader: USER32.dll/GetWindowLongW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/CallWindowProc
- DynamicLoader: USER32.dll/CallWindowProcW
- DynamicLoader: USER32.dll/GetClientRect
- DynamicLoader: USER32.dll/GetWindowRect
- DynamicLoader: USER32.dll/GetParent
- DynamicLoader: KERNEL32.dll/DeactivateActCtx
- DynamicLoader: KERNEL32.dll/GetSystemDefaultLCID
- DynamicLoader: KERNEL32.dll/GetSystemDefaultLCIDW
- DynamicLoader: GDI32.dll/GetStockObject
- DynamicLoader: GDI32.dll/GetObject
- DynamicLoader: GDI32.dll/GetObjectW
- DynamicLoader: USER32.dll/GetDC
- DynamicLoader: KERNEL32.dll/GetCurrentProcessId
- DynamicLoader: KERNEL32.dll/GetCurrentProcessIdW
- DynamicLoader: KERNEL32.dll/FindAtom
- DynamicLoader: KERNEL32.dll/FindAtomW

- DynamicLoader: KERNEL32.dll/AddAtom
- DynamicLoader: KERNEL32.dll/AddAtomW
- DynamicLoader: MSCOREE.DLL/LoadLibraryShim
- DynamicLoader: mscoreei.dll/LoadLibraryShim_RetAddr
- DynamicLoader: mscoreei.dll/LoadLibraryShim
- DynamicLoader: gdiplus.dll/GdiplusStartup
- DynamicLoader: KERNEL32.dll/IsProcessorFeaturePresent
- DynamicLoader: USER32.dll/GetWindowInfo
- DynamicLoader: USER32.dll/GetAncestor
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/EnumDisplayDevicesA
- DynamicLoader: GDI32.dll/ExtTextOutW
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: gdiplus.dll/GdipCreateFontFromLogfontW
- DynamicLoader: KERNEL32.dll/RegOpenKeyExW
- DynamicLoader: KERNEL32.dll/RegQueryInfoKeyA
- DynamicLoader: KERNEL32.dll/RegCloseKey
- DynamicLoader: KERNEL32.dll/RegCreateKeyExW
- DynamicLoader: KERNEL32.dll/RegQueryValueExW
- DynamicLoader: KERNEL32.dll/RegEnumValueW
- DynamicLoader: KERNEL32.dll/RegQueryInfoKeyW
- DynamicLoader: MSCOREE.DLL/ND_RI2
- DynamicLoader: mscoreei.dll/ND_RI2_RetAddr
- DynamicLoader: mscoreei.dll/ND_RI2
- DynamicLoader: MSCOREE.DLL/ND_RU1
- DynamicLoader: mscoreei.dll/ND_RU1_RetAddr
- DynamicLoader: mscoreei.dll/ND_RU1
- DynamicLoader: gdiplus.dll/GdipGetFontUnit
- DynamicLoader: gdiplus.dll/GdipGetFontSize
- DynamicLoader: gdiplus.dll/GdipGetFontStyle
- DynamicLoader: gdiplus.dll/GdipGetFamily
- DynamicLoader: USER32.dll/ReleaseDC
- DynamicLoader: gdiplus.dll/GdipCreateFromHDC
- DynamicLoader: gdiplus.dll/GdipGetDpiY
- DynamicLoader: gdiplus.dll/GdipGetFontHeight
- DynamicLoader: gdiplus.dll/GdipGetEmHeight
- DynamicLoader: gdiplus.dll/GdipGetLineSpacing
- DynamicLoader: gdiplus.dll/GdipDeleteGraphics
- DynamicLoader: gdiplus.dll/GdipCreateFont
- DynamicLoader: gdiplus.dll/GdipDeleteFont
- DynamicLoader: gdiplus.dll/GdipGetFamilyName
- DynamicLoader: GDI32.dll/CreateCompatibleDC
- DynamicLoader: GDI32.dll/GetCurrentObject
- DynamicLoader: GDI32.dll/SaveDC
- DynamicLoader: GDI32.dll/GetDeviceCaps
- DynamicLoader: GDI32.dll/CreateFontIndirect
- DynamicLoader: GDI32.dll/CreateFontIndirectW
- DynamicLoader: GDI32.dll/GetObject
- DynamicLoader: GDI32.dll/GetObjectW
- DynamicLoader: GDI32.dll/SelectObject
- DynamicLoader: GDI32.dll/GetMapMode
- DynamicLoader: GDI32.dll/GetTextMetricsW
- DynamicLoader: USER32.dll/DrawTextExW
- DynamicLoader: USER32.dll/DrawTextExWW
- 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: USER32.dll/GetProcessWindowStation
- DynamicLoader: USER32.dll/GetUserObjectInformation
- DynamicLoader: USER32.dll/GetUserObjectInformationA
- DynamicLoader: KERNEL32.dll/SetConsoleCtrlHandler
- DynamicLoader: KERNEL32.dll/SetConsoleCtrlHandlerW
- DynamicLoader: KERNEL32.dll/GetModuleHandle
- DynamicLoader: KERNEL32.dll/GetModuleHandleW
- DynamicLoader: USER32.dll/GetClassInfo
- DynamicLoader: USER32.dll/GetClassInfoW
- DynamicLoader: USER32.dll/RegisterClass
- DynamicLoader: USER32.dll/RegisterClassW
- DynamicLoader: USER32.dll/CreateWindowEx
- DynamicLoader: USER32.dll/CreateWindowExW
- DynamicLoader: USER32.dll/DefWindowProc
- DynamicLoader: USER32.dll/DefWindowProcW
- DynamicLoader: USER32.dll/GetSysColor
- DynamicLoader: USER32.dll/GetSysColorW
- DynamicLoader: GDI32.dll/CreateCompatibleDC
- DynamicLoader: gdiplus.dll/GdipGetLogFontW
- DynamicLoader: MSCOREE.DLL/ND_WU1
- DynamicLoader: mscoreei.dll/ND_WU1_RetAddr
- DynamicLoader: mscoreei.dll/ND_WU1
- DynamicLoader: GDI32.dll/CreateFontIndirect
- DynamicLoader: GDI32.dll/CreateFontIndirectW
- DynamicLoader: GDI32.dll/SelectObject
- DynamicLoader: GDI32.dll/GetTextMetricsW
- DynamicLoader: GDI32.dll/GetTextExtentPoint32W
- DynamicLoader: GDI32.dll/DeleteDC
- DynamicLoader: uxtheme.dll/GetThemeAppProperties
- DynamicLoader: uxtheme.dll/GetThemeAppPropertiesW
- DynamicLoader: uxtheme.dll/OpenThemeData
- DynamicLoader: uxtheme.dll/OpenThemeDataW
- DynamicLoader: uxtheme.dll/IsThemePartDefined
- DynamicLoader: uxtheme.dll/IsThemePartDefinedW
- DynamicLoader: gdiplus.dll/GdipCreateRegion
- DynamicLoader: gdiplus.dll/GdipGetClip
- DynamicLoader: gdiplus.dll/GdipCreateMatrix
- DynamicLoader: gdiplus.dll/GdipGetWorldTransform
- DynamicLoader: gdiplus.dll/GdipIsMatrixIdentity
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: gdiplus.dll/GdipGetMatrixElements
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: gdiplus.dll/GdipDeleteMatrix
- DynamicLoader: gdiplus.dll/GdipIsInfiniteRegion
- DynamicLoader: gdiplus.dll/GdipDeleteRegion
- DynamicLoader: gdiplus.dll/GdipGetDC
- DynamicLoader: GDI32.dll/OffsetViewportOrgEx
- DynamicLoader: uxtheme.dll/GetThemePartSize
- DynamicLoader: uxtheme.dll/GetThemePartSizeW
- DynamicLoader: GDI32.dll/RestoreDC
- DynamicLoader: gdiplus.dll/GdipReleaseDC
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: USER32.dll/SetWindowText
- DynamicLoader: USER32.dll/SetWindowTextW
- DynamicLoader: KERNEL32.dll/GetStartupInfo
- DynamicLoader: KERNEL32.dll/GetStartupInfoW
- DynamicLoader: USER32.dll/GetSystemMetrics

- DynamicLoader: GDI32.dll/GetDeviceCaps
- DynamicLoader: USER32.dll/CreateIconFromResourceEx
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: USER32.dll/GetSystemMenu
- DynamicLoader: USER32.dll/GetWindowPlacement
- DynamicLoader: USER32.dll/EnableMenuItem
- DynamicLoader: USER32.dll/GetClientRect
- DynamicLoader: USER32.dll/GetWindowTextLength
- DynamicLoader: USER32.dll/GetWindowTextLengthW
- DynamicLoader: USER32.dll/GetWindowText
- DynamicLoader: USER32.dll/GetWindowTextW
- DynamicLoader: USER32.dll/SetWindowPos
- DynamicLoader: USER32.dll/RedrawWindow
- DynamicLoader: USER32.dll/ShowWindow
- DynamicLoader: USER32.dll/GetClassInfo
- DynamicLoader: USER32.dll/GetClassInfoW
- DynamicLoader: comctl32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/OpenThemeData
- DynamicLoader: uxtheme.dll/IsThemePartDefined
- DynamicLoader: uxtheme.dll/GetThemeMargins
- DynamicLoader: uxtheme.dll/GetThemeBool
- DynamicLoader: uxtheme.dll/GetThemeInt
- DynamicLoader: comctl32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/SetWindowTheme
- DynamicLoader: uxtheme.dll/CloseThemeData
- 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: comctl32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/GetThemeFont
- DynamicLoader: uxtheme.dll/GetThemeColor
- DynamicLoader: IMM32.DLL/ImmIsIME
- DynamicLoader: USER32.dll/MapWindowPoints
- DynamicLoader: USER32.dll/GetWindow
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: comctl32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/EnableThemeDialogTexture
- DynamicLoader: comctl32.dll/RegisterClassNameW
- DynamicLoader: KERNEL32.dll/SetErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: culture.dll/ConvertLangIdToCultureName
- DynamicLoader: MSCOREE.DLL/ND_RI4
- DynamicLoader: mscoreei.dll/ND_RI4_RetAddr
- DynamicLoader: mscoreei.dll/ND_RI4

- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGetProvParam
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptSetKeyParam
- DynamicLoader: CRYPTSP.dll/CryptDecrypt
- DynamicLoader: CRYPTSP.dll/CryptEncrypt
- DynamicLoader: KERNEL32.dll/ReleaseMutex
- DynamicLoader: KERNEL32.dll/CreateMutex
- DynamicLoader: KERNEL32.dll/CreateMutexW
- DynamicLoader: KERNEL32.dll/CloseHandle
- 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: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/OpenProcess
- DynamicLoader: KERNEL32.dll/OpenProcessW
- DynamicLoader: psapi.dll/EnumProcessModules
- DynamicLoader: psapi.dll/EnumProcessModulesW
- DynamicLoader: psapi.dll/GetModuleInformation
- DynamicLoader: psapi.dll/GetModuleInformationW
- DynamicLoader: psapi.dll/GetModuleBaseName
- DynamicLoader: psapi.dll/GetModuleBaseNameW
- DynamicLoader: psapi.dll/GetModuleFileNameEx
- DynamicLoader: psapi.dll/GetModuleFileNameExW
- DynamicLoader: KERNEL32.dll/CreateProcess
- DynamicLoader: KERNEL32.dll/CreateProcessW
- DynamicLoader: KERNEL32.dll/GetThreadContext
- DynamicLoader: KERNEL32.dll/ReadProcessMemory
- DynamicLoader: KERNEL32.dll/VirtualAllocEx
- DynamicLoader: KERNEL32.dll/WriteProcessMemory
- DynamicLoader: KERNEL32.dll/VirtualProtectEx
- DynamicLoader: KERNEL32.dll/SetThreadContext
- DynamicLoader: KERNEL32.dll/ResumeThread
- DynamicLoader: USER32.dll/PostThreadMessage
- DynamicLoader: USER32.dll/PostThreadMessageW
- DynamicLoader: USER32.dll/InvalidateRect
- DynamicLoader: USER32.dll/GetWindowThreadProcessId
- DynamicLoader: USER32.dll/PostMessage
- DynamicLoader: USER32.dll/PostMessageW
- DynamicLoader: ole32.dll/OleInitialize
- DynamicLoader: ole32.dll/CoRegisterMessageFilter
- DynamicLoader: USER32.dll/GetFocus
- DynamicLoader: USER32.dll/SetFocus
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: ole32.dll/CoRevokeInitializeSpy
- DynamicLoader: USER32.dll/GetKeyboardLayout
- DynamicLoader: gdiplus.dll/GdipCreateHalftonePalette
- DynamicLoader: GDI32.dll/SelectPalette
- DynamicLoader: gdiplus.dll/GdipSetPageUnit
- DynamicLoader: gdiplus.dll/GdipSaveGraphics
- DynamicLoader: GDI32.dll/GetNearestColor
- DynamicLoader: GDI32.dll/CreateSolidBrush
- DynamicLoader: USER32.dll/FillRect
- DynamicLoader: GDI32.dll/DeleteObject

- 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/GetMessageA
- DynamicLoader: USER32.dll/DestroyIcon
- DynamicLoader: USER32.dll/DestroyWindow
- DynamicLoader: USER32.dll/EnumThreadWindows
- DynamicLoader: USER32.dll/IsWindowVisible
- DynamicLoader: ole32.dll/OleUninitialize
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: ole32.dll/CoWaitForMultipleHandles
- DynamicLoader: USER32.dll/SetClassLong
- DynamicLoader: USER32.dll/SetClassLongW
- DynamicLoader: USER32.dll/PostMessage
- DynamicLoader: USER32.dll/PostMessageW
- DynamicLoader: USER32.dll/UnregisterClass
- DynamicLoader: USER32.dll/UnregisterClassW
- DynamicLoader: KERNEL32.dll/DeleteAtom
- DynamicLoader: KERNEL32.dll/DeleteAtomW
- DynamicLoader: USER32.dll/IsWindow
- DynamicLoader: KERNEL32.dll/GetProcAddress
- DynamicLoader: USER32.dll/DefWindowProcW
- DynamicLoader: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/SetClassLong
- DynamicLoader: USER32.dll/SetClassLongW
- DynamicLoader: USER32.dll/DestroyWindow
- DynamicLoader: USER32.dll/DestroyWindowW
- DynamicLoader: USER32.dll/PostMessage
- DynamicLoader: USER32.dll/PostMessageW
- DynamicLoader: GDI32.dll/DeleteObject
- DynamicLoader: uxtheme.dll/CloseThemeData
- DynamicLoader: uxtheme.dll/CloseThemeDataW
- DynamicLoader: GDI32.dll/DeleteObject
- DynamicLoader: GDI32.dll/DeleteDC
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- 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: 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: 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/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- DynamicLoader: KERNEL32.dll/GetVersionEx
- DynamicLoader: KERNEL32.dll/GetVersionExW
- 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/CloseHandle
- DynamicLoader: KERNEL32.dll/lstrlen
- DynamicLoader: KERNEL32.dll/lstrlenW
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: KERNEL32.dll/RtlMoveMemory
- DynamicLoader: KERNEL32.dll/RtlMoveMemoryW
- DynamicLoader: shell32.dll/ShellExecuteEx
- DynamicLoader: shell32.dll/ShellExecuteExW
- DynamicLoader: ole32.dll/OleInitialize
- DynamicLoader: ole32.dll/CreateBindCtx
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: PROPSYS.dll/PSCreateMemoryPropertyStore
- DynamicLoader: PROPSYS.dll/PSPropertyBag_WriteDWORD
- DynamicLoader: ole32.dll/CoGetApartmentType
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetMalloc
- DynamicLoader: PROPSYS.dll/PSPropertyBag_ReadDWORD
- DynamicLoader: PROPSYS.dll/PSPropertyBag_ReadGUID
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: apphelp.dll/ApphelpCheckShellObject

- DynamicLoader: ole32.dll/CoCreateInstance
- 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: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: shell32.dll/
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_Size_ExW
- DynamicLoader: PROPSYS.dll/PSPropertyBag_ReadStrAlloc
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_ExW
- DynamicLoader: ADVAPI32.dll/InitializeSecurityDescriptor
- DynamicLoader: ADVAPI32.dll/SetEntriesInAclW
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: ADVAPI32.dll/SetSecurityDescriptorDacl
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: ADVAPI32.dll/IsTextUnicode
- DynamicLoader: comctl32.dll/
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: PROPSYS.dll/
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegGetValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ole32.dll/CoTaskMemRealloc
- DynamicLoader: PROPSYS.dll/InitPropVariantFromStringAsVector
- DynamicLoader: PROPSYS.dll/PSCoerceToCanonicalValue
- DynamicLoader: PROPSYS.dll/PropVariantToStringAlloc
- DynamicLoader: ole32.dll/PropVariantClear
- DynamicLoader: ole32.dll/CoAllowSetForegroundWindow
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: ADVAPI32.dll/SaferGetPolicyInformation
- DynamicLoader: ntdll.dll/RtlDllShutdownInProgress
- DynamicLoader: comctl32.dll/
- DynamicLoader: ole32.dll/OleUninitialize
- DynamicLoader: ole32.dll/CoRevokeInitializeSpy
- DynamicLoader: comctl32.dll/
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ADVAPI32.dll/GetUserName
- DynamicLoader: ADVAPI32.dll/GetUserNameW
- DynamicLoader: KERNEL32.dll/SetErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: KERNEL32.dll/GetACP
- DynamicLoader: KERNEL32.dll/GetUserDefaultUILanguage
- DynamicLoader: KERNEL32.dll/UnmapViewOfFile
- DynamicLoader: KERNEL32.dll/GetCurrentProcess
- DynamicLoader: KERNEL32.dll/GetCurrentProcessW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx

- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: KERNEL32.dll/GetFileType
- DynamicLoader: KERNEL32.dll/GetFileSize
- DynamicLoader: KERNEL32.dll/ReadFile
- DynamicLoader: MSCOREE.DLL/ND_RI2
- DynamicLoader: mscoreei.dll/ND_RI2_RetAddr
- DynamicLoader: mscoreei.dll/ND_RI2
- DynamicLoader: KERNEL32.dll/CreateEvent
- DynamicLoader: KERNEL32.dll/CreateEventW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- 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: rasapi32.dll/RasEnumConnections
- DynamicLoader: rasapi32.dll/RasEnumConnectionsW
- DynamicLoader: rtutils.dll/TraceRegisterExA
- DynamicLoader: rtutils.dll/TracePrintfExA
- DynamicLoader: sechost.dll/OpenSCManagerW
- DynamicLoader: sechost.dll/OpenServiceW
- DynamicLoader: sechost.dll/QueryServiceStatus
- DynamicLoader: sechost.dll/CloseServiceHandle
- DynamicLoader: WS2_32.dll/WSAStartup
- DynamicLoader: WS2_32.dll/WSASocket
- DynamicLoader: WS2_32.dll/WSASocketW
- DynamicLoader: WS2_32.dll/setsockopt
- DynamicLoader: WS2_32.dll/WSAEventSelect
- DynamicLoader: WS2_32.dll/ioctlsocket
- DynamicLoader: WS2_32.dll/closesocket
- DynamicLoader: KERNEL32.dll/GetCurrentProcessId
- DynamicLoader: KERNEL32.dll/GetCurrentProcessIdW
- DynamicLoader: KERNEL32.dll/GetComputerName
- DynamicLoader: KERNEL32.dll/GetComputerNameW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/ConvertStringSecurityDescriptorToSecurityDescriptor
- DynamicLoader: ADVAPI32.dll/ConvertStringSecurityDescriptorToSecurityDescriptorW
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: KERNEL32.dll/CreateFileMapping
- DynamicLoader: KERNEL32.dll/CreateFileMappingW
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/MapViewOfFile
- DynamicLoader: KERNEL32.dll/UnmapViewOfFile
- DynamicLoader: KERNEL32.dll/VirtualQuery
- DynamicLoader: KERNEL32.dll/ReleaseMutex
- DynamicLoader: ADVAPI32.dll/CreateWellKnownSid
- DynamicLoader: ADVAPI32.dll/CreateWellKnownSidW
- DynamicLoader: KERNEL32.dll/CreateMutex
- DynamicLoader: KERNEL32.dll/CreateMutexW
- DynamicLoader: KERNEL32.dll/WaitForSingleObject
- DynamicLoader: KERNEL32.dll/OpenMutex
- DynamicLoader: KERNEL32.dll/OpenMutexW
- DynamicLoader: KERNEL32.dll/OpenProcess
- DynamicLoader: KERNEL32.dll/OpenProcessW
- DynamicLoader: KERNEL32.dll/GetProcessTimes
- DynamicLoader: KERNEL32.dll/GetProcessTimesW
- DynamicLoader: WS2_32.dll/ioctlsocket
- DynamicLoader: WS2_32.dll/WSAIoctl
- DynamicLoader: KERNEL32.dll/FormatMessage

- DynamicLoader: KERNEL32.dll/FormatMessageW
- DynamicLoader: WS2_32.dll/WSAEventSelect
- DynamicLoader: rasapi32.dll/RasConnectionNotification
- DynamicLoader: rasapi32.dll/RasConnectionNotificationW
- DynamicLoader: sechost.dll/NotifyServiceStatusChangeA
- DynamicLoader: ADVAPI32.dll/RegOpenCurrentUser
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegNotifyChangeKeyValue
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: winhttp.dll/WinHttpGetIEProxyConfigForCurrentUser
- DynamicLoader: KERNEL32.dll/SetEvent
- DynamicLoader: KERNEL32.dll/SwitchToThread
- DynamicLoader: KERNEL32.dll/ResetEvent
- DynamicLoader: ole32.dll/CoWaitForMultipleHandles
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: ole32.dll/NdrOleInitializeExtension
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: KERNEL32.dll/LocalFree
- DynamicLoader: IPHLPAPI.DLL/GetNetworkParams
- DynamicLoader: DNSAPI.dll/DnsQueryConfig
- DynamicLoader: IPHLPAPI.DLL/GetAdaptersAddresses
- DynamicLoader: IPHLPAPI.DLL/GetIpInterfaceEntry
- DynamicLoader: IPHLPAPI.DLL/GetBestInterfaceEx
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: IPHLPAPI.DLL/GetAdaptersAddresses
- DynamicLoader: WS2_32.dll/inet_addr
- DynamicLoader: WS2_32.dll/getaddrinfo
- DynamicLoader: WS2_32.dll/freeaddrinfo
- DynamicLoader: IPHLPAPI.DLL/GetAdaptersAddresses
- DynamicLoader: WS2_32.dll/WSAConnect
- DynamicLoader: WS2_32.dll/send
- DynamicLoader: WS2_32.dll/setsockopt
- DynamicLoader: WS2_32.dll/recv
- DynamicLoader: WS2_32.dll/shutdown
- DynamicLoader: KERNEL32.dll/WriteFile
- 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: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: SspiCli.dll/GetUserNameExW
- DynamicLoader: ADVAPI32.dll/GetUserNameW
- DynamicLoader: XmlLite.dll/CreateXmlWriter
- DynamicLoader: XmlLite.dll/CreateXmlWriterOutputWithEncodingName
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: wbemcore.dll/Reinitialize
- DynamicLoader: WTSAPI32.dll/WTSQueryUserToken
- 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: UxTheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: ole32.dll/CoRevokeInitializeSpy
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: OLEAUT32.dll/SysAllocString
- DynamicLoader: OLEAUT32.dll/SysStringLen
- DynamicLoader: OLEAUT32.dll/SysFreeString
- DynamicLoader: OLEAUT32.dll/

Guard pages use detected - possible anti-debugging.

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

- process: schtasks.exe, PID 2228

Creates RWX memory

SetUnhandledExceptionFilter detected (possible anti-debug)

2 HTTP Request(s) detected

http://lancetasks.com/files/cinstaller.exe
Hostname: lancetasks.com
IP Address: 178.62.254.226
Port: 80
Count: 1

http://lancetasks.com/files/web.exe
Hostname: lancetasks.com
IP Address: 178.62.254.226
Port: 80
Count: 1