VLTKNhatRac.exe

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

MalFamily: Ispy **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	687.50 KB (704000 bytes)
Compile time:	2018-11-16 08:55:55
MD5:	479fdfb2b1e0860dc5cd825187d47f67
SHA1:	306f7489aa343cad54aaebe12a0f4e5ac23727a7
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2019-01-22 05:24:06

URL(s) file hosting

http://kimyen.net/upload/VLTKNhatRac.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2019-01-20 16:56:37	32/71	

Import library

mscoree.dll

12 Behaviors detected by system signatures

Domain Sinkholed or blacklisted

- Alert: Honeypot blocked domain: kimyen.net

Anomalous binary characteristics

- anomaly: Unprintable characters found in section name

Exhibits behavior characteristic of iSpy Keylogger

- C2: 192.168.56.1
- C2: 112.213.89.26
- C2:
- User: kimmaosuvuong@kimyen.club
- User: kimmaosuvuong@kimyen.club
- User: kimmaosuvuong@kimyen.club
- User: kimmaosuvuong@kimyen.club
- User: kimmaosuvuong@kimyen.club
- User: kimmaosuvuong@kimyen.club
- User: kimmaosuvuong@kimyen.club
- User: kimmaosuvuong@kimyen.club
- User: kimmaosuvuong@kimyen.club

The binary likely contains encrypted or compressed data.

- section: name: f"7@'\x13B), entropy: 8.00, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ|IMAGE_SCN_MEM_WRITE, raw_size: 0x0009f400, virtual_size: 0x0009f2b0

Performs some HTTP requests

- url: http://kimyen.net/vltk/chayrac/VLTKChayrac.txt
- url: http://free.timeanddate.com/clock/i3jl68nm/n246/tlir/tt0/tw0/tm3/th1
- url: http://kimyen.club/vltk/chayrac/VLTKChayrac.txt

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://kimyen.net/vltk/chayrac/VLTKChayrac.txt
- suspicious_request: http://free.timeanddate.com/clock/i3jl68nm/n246/tlir/tt0/tw0/tm3/th1
- suspicious_request: http://kimyen.club/vltk/chayrac/VLTKChayrac.txt

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

- ioc: l.q5
- ioc: u.6nRT
- ioc: 1.025600VB29121CAB-D44294DD178BFBFF000206C2

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: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/VirtualProtect
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap

- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: KERNEL32.dll/VirtualProtect
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariable
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariableW
- 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/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/GetUserPreferredUILanguages
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: KERNEL32.dll/CompareStringOrdinal
- DynamicLoader: KERNEL32.dll/SetThreadErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- 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/VirtualProtect
- 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: KERNEL32.dll/GetCurrentDirectory
- DynamicLoader: KERNEL32.dll/GetCurrentDirectoryW
- DynamicLoader: ole32.dll/CoTaskMemAlloc

- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: nlssorting.dll/SortGetHandle
- DynamicLoader: nlssorting.dll/SortCloseHandle
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegCreateKeyEx
- DynamicLoader: ADVAPI32.dll/RegCreateKeyExW
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: KERNEL32.dll/GetModuleHandle
- DynamicLoader: KERNEL32.dll/GetModuleHandleW
- DynamicLoader: KERNEL32.dll/LoadLibrary
- DynamicLoader: KERNEL32.dll/LoadLibraryW
- 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/GetProcAddress
- DynamicLoader: KERNEL32.dll/WideCharToMultiByte
- DynamicLoader: USER32.dll/DefWindowProcW
- DynamicLoader: GDI32.dll/GetStockObject
- 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/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/GetModuleFileName
- DynamicLoader: KERNEL32.dll/GetModuleFileNameW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSize
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfo
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValue
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/LCMapStringEx
- DynamicLoader: VERSION.dll/VerLanguageName
- DynamicLoader: VERSION.dll/VerLanguageNameW
- 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: 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/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: 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: USER32.dll/GetSystemMetrics
- DynamicLoader: GDI32.dll/GetDeviceCaps
- DynamicLoader: USER32.dll/CreateIconFromResourceEx
- DynamicLoader: uxtheme.dll/GetThemeAppProperties
- DynamicLoader: uxtheme.dll/GetThemeAppPropertiesW
- DynamicLoader: uxtheme.dll/OpenThemeData
- DynamicLoader: uxtheme.dll/OpenThemeDataW
- DynamicLoader: GDI32.dll/GetTextExtentPoint32W
- DynamicLoader: GDI32.dll/DeleteObject
- DynamicLoader: OLEAUT32.dll/OleCreatePictureIndirect
- DynamicLoader: USER32.dll/GetIconInfo
- DynamicLoader: GDI32.dll/GetObject
- DynamicLoader: GDI32.dll/GetObjectW
- DynamicLoader: GDI32.dll/DeleteObject
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/CloseHandle
- 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: USER32.dll/CopyImage
- DynamicLoader: USER32.dll/LoadCursor
- DynamicLoader: USER32.dll/LoadCursorW
- DynamicLoader: gdiplus.dll/GdipLoadImageFromStream
- DynamicLoader: WindowsCodecs.dll/DllGetClassObject
- DynamicLoader: KERNEL32.dll/WerRegisterMemoryBlock
- DynamicLoader: gdiplus.dll/GdipImageForceValidation
- DynamicLoader: gdiplus.dll/GdipGetImageType
- DynamicLoader: gdiplus.dll/GdipGetImageRawFormat
- DynamicLoader: gdiplus.dll/GdipCreateFontFamilyFromName
- DynamicLoader: GDI32.dll/CreateCompatibleDC
- DynamicLoader: GDI32.dll/SelectObject
- DynamicLoader: GDI32.dll/GetTextMetricsW
- DynamicLoader: GDI32.dll/DeleteDC
- 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: 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/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: ADVAPI32.dll/RegSetValueEx
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: USER32.dll/SetWindowText
- DynamicLoader: USER32.dll/SetWindowTextW
- DynamicLoader: KERNEL32.dll/GetStartupInfo
- DynamicLoader: KERNEL32.dll/GetStartupInfoW
- 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/GetSystemMetrics
- 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/EnableThemeDialogTexture
- DynamicLoader: uxtheme.dll/OpenThemeData
- DynamicLoader: uxtheme.dll/GetThemeBool
- DynamicLoader: USER32.dll/GetWindow
- DynamicLoader: USER32.dll/MapWindowPoints
- DynamicLoader: comctl32.dll/InitCommonControlsEx
- DynamicLoader: IMM32.DLL/ImmAssociateContext
- DynamicLoader: uxtheme.dll/GetThemeTextMetrics
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: uxtheme.dll/GetThemeTextExtent
- DynamicLoader: uxtheme.dll/GetThemeBackgroundExtent
- DynamicLoader: USER32.dll/PostMessage
- DynamicLoader: USER32.dll/PostMessageW
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: comctl32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/IsThemePartDefined
- DynamicLoader: uxtheme.dll/GetThemeMargins
- 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: USER32.dll/SystemParametersInfo
- DynamicLoader: USER32.dll/SystemParametersInfoW
- DynamicLoader: comctl32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/GetThemeFont
- DynamicLoader: uxtheme.dll/GetThemeColor
- DynamicLoader: IMM32.DLL/ImmIsIME
- DynamicLoader: comctl32.dll/RegisterClassNameW
- DynamicLoader: USER32.dll/InvalidateRect
- DynamicLoader: uxtheme.dll/GetThemePartSize
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: gdiplus.dll/GdipImageGetFrameDimensionsCount
- DynamicLoader: gdiplus.dll/GdipImageGetFrameDimensionsList
- DynamicLoader: ole32.dll/OleInitialize
- DynamicLoader: ole32.dll/RegisterDragDrop
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: shell32.dll/DragAcceptFiles
- DynamicLoader: USER32.dll/SendMessage

- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: uxtheme.dll/
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKey
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: KERNEL32.dll/CreateDirectory
- DynamicLoader: KERNEL32.dll/CreateDirectoryW
- DynamicLoader: USER32.dll/MonitorFromWindow
- DynamicLoader: USER32.dll/GetMonitorInfo
- DynamicLoader: USER32.dll/GetMonitorInfoW
- DynamicLoader: GDI32.dll/CreateDC
- DynamicLoader: GDI32.dll/CreateDCW
- DynamicLoader: GDI32.dll/GetDeviceCaps
- DynamicLoader: USER32.dll/UpdateWindow
- DynamicLoader: USER32.dll/SetTimer
- 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: USER32.dll/InvalidateRect
- DynamicLoader: USER32.dll/GetWindowThreadProcessId
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: GDI32.dll/GetNearestColor
- DynamicLoader: GDI32.dll/CreateSolidBrush
- DynamicLoader: USER32.dll/FillRect
- DynamicLoader: gdiplus.dll/GdipCreateHalftonePalette
- DynamicLoader: GDI32.dll/SelectPalette
- DynamicLoader: gdiplus.dll/GdipSetPageUnit
- DynamicLoader: gdiplus.dll/GdipSaveGraphics
- DynamicLoader: uxtheme.dll/DrawThemeBackground
- DynamicLoader: uxtheme.dll/DrawThemeBackgroundW
- DynamicLoader: GDI32.dll/SetTextColor
- DynamicLoader: GDI32.dll/SetBkColor
- DynamicLoader: USER32.dll/GetSysColorBrush
- DynamicLoader: uxtheme.dll/BufferedPaintInit
- DynamicLoader: uxtheme.dll/BufferedPaintRenderAnimation
- DynamicLoader: uxtheme.dll/GetThemeTransitionDuration
- DynamicLoader: uxtheme.dll/BeginBufferedAnimation
- DynamicLoader: uxtheme.dll/IsThemeBackgroundPartiallyTransparent
- DynamicLoader: uxtheme.dll/DrawThemeParentBackgroundEx
- DynamicLoader: gdiplus.dll/GdipRestoreGraphics
- DynamicLoader: uxtheme.dll/DrawThemeBackground
- DynamicLoader: uxtheme.dll/EndBufferedAnimation
- 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/DispatchMessageA
- DynamicLoader: USER32.dll/BeginPaint
- DynamicLoader: USER32.dll/EndPaint
- DynamicLoader: GDI32.dll/CreateCompatibleDC
- DynamicLoader: GDI32.dll/GetObjectType
- DynamicLoader: GDI32.dll/CreateCompatibleBitmap
- DynamicLoader: GDI32.dll/GetDIBits

- DynamicLoader: GDI32.dll/DeleteObject
- DynamicLoader: GDI32.dll/CreateDIBSection
- DynamicLoader: GDI32.dll/SelectObject
- DynamicLoader: gdiplus.dll/GdipTranslateWorldTransform
- DynamicLoader: gdiplus.dll/GdipSetClipRectI
- DynamicLoader: USER32.dll/SystemParametersInfo
- DynamicLoader: USER32.dll/SystemParametersInfoW
- DynamicLoader: uxtheme.dll/IsThemeBackgroundPartiallyTransparent
- DynamicLoader: uxtheme.dll/IsThemeBackgroundPartiallyTransparentW
- DynamicLoader: gdiplus.dll/GdipGetRegionHRgn
- DynamicLoader: GDI32.dll/CreateRectRgn
- DynamicLoader: GDI32.dll/GetClipRgn
- DynamicLoader: GDI32.dll/SelectClipRgn
- DynamicLoader: uxtheme.dll/DrawThemeParentBackground
- DynamicLoader: uxtheme.dll/DrawThemeParentBackgroundW
- DynamicLoader: uxtheme.dll/GetThemeBackgroundContentRect
- DynamicLoader: uxtheme.dll/GetThemeBackgroundContentRectW
- DynamicLoader: gdiplus.dll/GdipGetTextRenderingHint
- DynamicLoader: GDI32.dll/GetTextAlign
- DynamicLoader: GDI32.dll/GetTextColor
- DynamicLoader: GDI32.dll/GetBkMode
- DynamicLoader: GDI32.dll/SetBkMode
- DynamicLoader: GDI32.dll/BitBlt
- DynamicLoader: GDI32.dll/DeleteDC
- DynamicLoader: uxtheme.dll/DrawThemeParentBackground
- DynamicLoader: uxtheme.dll/DrawThemeText
- DynamicLoader: GDI32.dll/SetTextColor
- DynamicLoader: uxtheme.dll/BeginBufferedPaint
- DynamicLoader: uxtheme.dll/EndBufferedPaint
- DynamicLoader: gdiplus.dll/GdipCombineRegionRegion
- DynamicLoader: gdiplus.dll/GdipGetNearestColor
- DynamicLoader: gdiplus.dll/GdipCreateSolidFill
- DynamicLoader: gdiplus.dll/GdipFillRectangleI
- DynamicLoader: gdiplus.dll/GdipDeleteBrush
- DynamicLoader: gdiplus.dll/GdipGetImageWidth
- DynamicLoader: gdiplus.dll/GdipGetImageHeight
- DynamicLoader: gdiplus.dll/GdipCloneRegion
- DynamicLoader: gdiplus.dll/GdipCombineRegionRectI
- DynamicLoader: gdiplus.dll/GdipSetClipRegion
- DynamicLoader: gdiplus.dll/GdipDrawImageRectI
- DynamicLoader: uxtheme.dll/GetThemeBackgroundContentRect
- DynamicLoader: uxtheme.dll/DrawThemeTextEx
- DynamicLoader: USER32.dll/WaitMessage
- DynamicLoader: USER32.dll/FindWindowEx
- DynamicLoader: USER32.dll/FindWindowExA
- DynamicLoader: ADVAPI32.dll/RegEnumValue
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: KERNEL32.dll/OpenProcess
- DynamicLoader: KERNEL32.dll/VirtualAllocEx
- DynamicLoader: ADVAPI32.dll/ConvertSidToStringSidW
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: CRYPTSP.dll/CryptGetDefaultProviderW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: USER32.dll/GetCursorPos
- DynamicLoader: USER32.dll/MonitorFromPoint
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: USER32.dll/IsChild
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/

- DynamicLoader: KERNEL32.dll/GetACP
- DynamicLoader: KERNEL32.dll/UnmapViewOfFile
- DynamicLoader: KERNEL32.dll/FindFirstFile
- DynamicLoader: KERNEL32.dll/FindFirstFileW
- DynamicLoader: KERNEL32.dll/FindClose
- DynamicLoader: KERNEL32.dll/FindNextFile
- DynamicLoader: KERNEL32.dll/FindNextFileW
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: KERNEL32.dll/GetTimeZoneInformation
- DynamicLoader: KERNEL32.dll/GetDynamicTimeZoneInformation
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: ole32.dll/CoWaitForMultipleHandles
- DynamicLoader: KERNEL32.dll/GetFileMUIPath
- DynamicLoader: KERNEL32.dll/LoadLibraryEx
- DynamicLoader: KERNEL32.dll/LoadLibraryExW
- DynamicLoader: KERNEL32.dll/FreeLibrary
- DynamicLoader: KERNEL32.dll/FreeLibraryW
- DynamicLoader: USER32.dll/LoadStringW
- DynamicLoader: USER32.dll/GetDlgItem
- DynamicLoader: KERNEL32.dll/WriteProcessMemory
- DynamicLoader: USER32.dll/GetForegroundWindow
- DynamicLoader: USER32.dll/GetWindowThreadProcessId
- DynamicLoader: USER32.dll/SetCursor
- DynamicLoader: comctl32.dll/_TrackMouseEvent
- DynamicLoader: USER32.dll/GetKeyState
- DynamicLoader: ADVAPI32.dll/OpenSCManagerW
- DynamicLoader: ADVAPI32.dll/OpenService
- DynamicLoader: ADVAPI32.dll/OpenServiceW
- DynamicLoader: ADVAPI32.dll/CloseServiceHandle
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileA
- DynamicLoader: KERNEL32.dll/DeviceIoControl
- DynamicLoader: KERNEL32.dll/DeviceIoControl
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/VirtualProtect
- DynamicLoader: KERNEL32.dll/VirtualProtectW
- DynamicLoader: USER32.dll/CallWindowProcW
- DynamicLoader: KERNEL32.dll/GetVolumeInformation
- DynamicLoader: KERNEL32.dll/GetVolumeInformationW
- DynamicLoader: KERNEL32.dll/ReadProcessMemory
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: KERNEL32.dll/CloseHandleW
- DynamicLoader: OLEAUT32.dll/SysAllocStringLen
- DynamicLoader: OLEAUT32.dll/SysAllocStringLenW
- DynamicLoader: OLEAUT32.dll/SysFreeString
- DynamicLoader: KERNEL32.dll/RtlZeroMemory
- DynamicLoader: OLEAUT32.dll/SysStringLen
- DynamicLoader: ADVAPI32.dll/SystemFunction041
- DynamicLoader: ADVAPI32.dll/SystemFunction041W
- DynamicLoader: ADVAPI32.dll/SystemFunction040
- DynamicLoader: ADVAPI32.dll/SystemFunction040W
- DynamicLoader: OLEAUT32.dll/SysStringLen
- DynamicLoader: USER32.dll/PostMessage
- DynamicLoader: USER32.dll/PostMessageW
- 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: ws2_32.dll/GetAddrInfoW
- DynamicLoader: ws2_32.dll/freeaddrinfo
- DynamicLoader: ws2_32.dll/WSAConnect
- DynamicLoader: ws2_32.dll/recv
- DynamicLoader: ws2_32.dll/shutdown
- DynamicLoader: KERNEL32.dll/EnumCalendarInfoExEx
- DynamicLoader: KERNEL32.dll/GetCalendarInfoEx
- DynamicLoader: KERNEL32.dll/EnumSystemLocalesEx
- DynamicLoader: KERNEL32.dll/EnumTimeFormatsEx
- DynamicLoader: KERNEL32.dll/CreateEvent
- DynamicLoader: KERNEL32.dll/CreateEventW
- DynamicLoader: KERNEL32.dll/QueryPerformanceFrequency
- DynamicLoader: KERNEL32.dll/QueryPerformanceCounter
- 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: sechost.dll/CloseServiceHandle
- 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: 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: sechost.dll/NotifyServiceStatusChangeA
- DynamicLoader: winhttp.dll/WinHttpOpen
- DynamicLoader: winhttp.dll/WinHttpOpenW
- DynamicLoader: winhttp.dll/WinHttpCloseHandle
- DynamicLoader: winhttp.dll/WinHttpCloseHandleW
- DynamicLoader: winhttp.dll/WinHttpSetTimeouts
- DynamicLoader: winhttp.dll/WinHttpSetTimeoutsW
- DynamicLoader: winhttp.dll/WinHttpGetIEProxyConfigForCurrentUser
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: KERNEL32.dll/SetEvent
- DynamicLoader: KERNEL32.dll/ResetEvent
- 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: IPHLPAPI.DLL/GetAdaptersAddresses
- DynamicLoader: ws2_32.dll/send
- DynamicLoader: ws2_32.dll/setsockopt
- DynamicLoader: USER32.dll/GetCapture
- DynamicLoader: KERNEL32.dll/CreateSemaphore
- DynamicLoader: KERNEL32.dll/CreateSemaphoreA

- DynamicLoader: KERNEL32.dll/ReleaseMutex
- DynamicLoader: KERNEL32.dll/CreateMutex
- DynamicLoader: KERNEL32.dll/CreateMutexW
- DynamicLoader: OLEAUT32.dll/SysAllocStringLen
- DynamicLoader: OLEAUT32.dll/SysAllocStringLenW
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo

A process attempted to delay the analysis task.

- Process: VLTKNhatRac.exe tried to sleep 1358 seconds, actually delayed analysis time by 0 seconds

Guard pages use detected - possible anti-debugging.

Creates RWX memory

SetUnhandledExceptionFilter detected (possible anti-debug)

6 HTTP Request(s) detected

http://kimyen.net/vltk/chayrac/VLTKChayrac.txt
Hostname: kimyen.net
IP Address: 10.1.26.180
Port: 80
Count: 1

http://kimyen.net/vltk/chayrac/VLTKChayrac.txt
Hostname: kimyen.net
IP Address: 10.1.26.180
Port: 80
Count: 9

http://free.timeanddate.com/clock/i3jl68nm/n246/tlir/tt0/tw0/tm3/th1
Hostname: free.timeanddate.com
IP Address: 151.101.16.69
Port: 80
Count: 1

http://free.timeanddate.com/clock/i3jl68nm/n246/tlir/tt0/tw0/tm3/th1
Hostname: free.timeanddate.com
IP Address: 151.101.16.69
Port: 80
Count: 12

http://kimyen.club/vltk/chayrac/VLTKChayrac.txt

Hostname: kimyen.club
IP Address: 112.213.89.26
Port: 80
Count: 1

http://kimyen.club/vltk/chayrac/VLTKChayrac.txt
Hostname: kimyen.club
IP Address: 112.213.89.26
Port: 80
Count: 9

1 Host(s) detected

IP Address	Hostname	Reverse DNS
112.213.89.26 ?		

1 Countr(y|ies) detected

Hosts	Country
1	Vietnam ?