VALKYRIE COMODO

Summary

File Name: DNI.docx.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

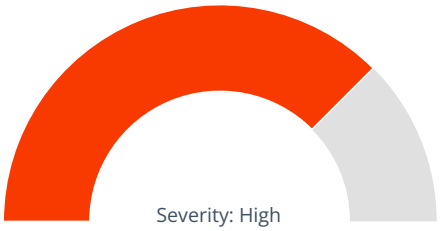
SHA1: ec4d1dd578dee5f32edebc8b97c99ce9d5f69e1a

MD5: bb34c3ef615576c659f6f8761233d45d

MALWARE

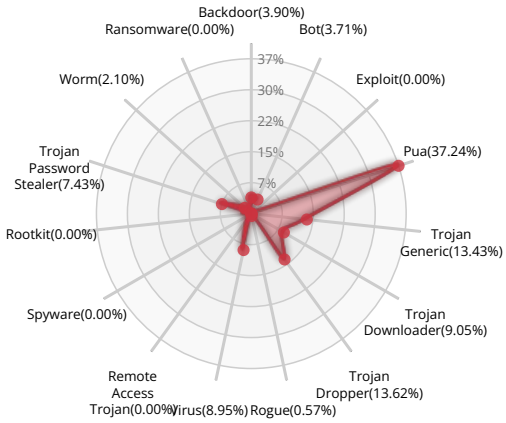
Valkyrie Final Verdict

DETECTION SECTION

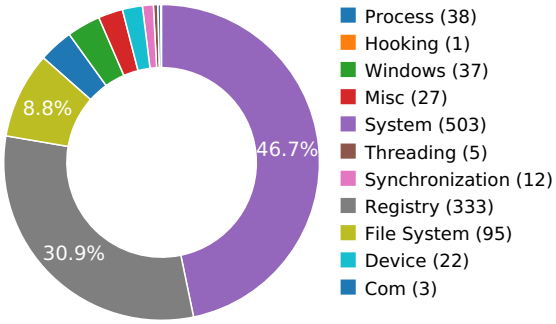


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

Hooking and other Techniques for Hiding Protection 1 (100.00%)

VALKYRIE COMODO

Activity Details

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\ec4d1dd578dee5f32edebc8b97c99ce9d5f69e1a.exe
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\UxTheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\ec4d1dd578dee5f32edebc8b97c99ce9d5f69e1a.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
C:\Users\user\AppData\Local\Temp\explorer\explorer.exe
C:\Windows\SysWOW64\shell32.dll
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
\??\MountPointManager
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004b.db
C:\Users\desktop.ini
C:\Users\user\AppData\Local\Temp\explorer
C:\Windows\SysWOW64\shlwapi.dll
C:\Windows\System32\en-US\DUser.dll.mui
C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9
C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\COMCTL32.dll.mui
C:\Users\user\AppData\Local\Temp\imageres.dll
C:\Windows\System32\imageres.dll
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\explorer\DNI.docx

READ REGISTRY KEYS

HKEY_CURRENT_USER\Control Panel\Mouse\SwapMouseButtons
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DontShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClassicShell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\SeparateProcess
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoNetCrawling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSimpleStartMenu
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DontPrettyPath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideIcons
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\MapNetDrvBtn
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\WebView
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Filter
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\NoNetCrawling
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AutoCheckSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\IconsOnly
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowTypeOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\DocObject
HKEY_CURRENT_USER\Software\Classes\Folder\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\BrowseInPlace
HKEY_CURRENT_USER\Software\Classes\Folder\BrowseInPlace
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\BrowseInPlace
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\IsShortcut

HKEY_CURRENT_USER\Software\Classes\Folder\IsShortcut
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\IsShortcut
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\AlwaysShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\NeverShowExt
HKEY_CURRENT_USER\Software\Classes\Folder\NeverShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\NeverShowExt

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsFree
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.CreateEventExW
kernel32.dll.CreateSemaphoreExW
kernel32.dll.SetThreadStackGuarantee
kernel32.dll.CreateThreadpoolTimer
kernel32.dll.SetThreadpoolTimer
kernel32.dll.WaitForThreadpoolTimerCallbacks
kernel32.dll.CloseThreadpoolTimer
kernel32.dll.CreateThreadpoolWait
kernel32.dll.SetThreadpoolWait
kernel32.dll.CloseThreadpoolWait
kernel32.dll.FlushProcessWriteBuffers
kernel32.dll.FreeLibraryWhenCallbackReturns
kernel32.dll.GetCurrentProcessorNumber
kernel32.dll.GetLogicalProcessorInformation
kernel32.dll.CreateSymbolicLinkW
kernel32.dll.EnumSystemLocalesEx
kernel32.dll.CompareStringEx
kernel32.dll.GetDateFormatEx
kernel32.dll.GetLocaleInfoEx
kernel32.dll.GetTimeFormatEx
kernel32.dll.GetUserDefaultLocaleName
kernel32.dll.IsValidLocaleName

kernel32.dll.LCMapStringEx
kernel32.dll.GetTickCount64
kernel32.dll.GetNativeSystemInfo
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
kernel32.dll.Wow64DisableWow64FsRedirection
kernel32.dll.Wow64RevertWow64FsRedirection
dwmapi.dll.DwmIsCompositionEnabled
comctl32.dll.RegisterClassNameW
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
uxtheme.dll.OpenThemeData
uxtheme.dll.GetThemeBool
imm32.dll.ImmGetContext
imm32.dll.ImmReleaseContext
imm32.dll.ImmAssociateContext
imm32.dll.ImmIsIME
comctl32.dll.HIMAGELIST_QueryInterface
comctl32.dll.DrawShadowText
comctl32.dll.DrawSizeBox
comctl32.dll.DrawScrollBar
comctl32.dll.SizeBoxHwnd
comctl32.dll.ScrollBar_MouseMove
comctl32.dll.ScrollBar_Menu
comctl32.dll.HandleScrollCmd
comctl32.dll.DetachScrollBars
comctl32.dll.AttachScrollBars
comctl32.dll.CCSetScrollInfo
comctl32.dll.CCGetScrollInfo
comctl32.dll.CCEnableScrollBar
comctl32.dll.QuerySystemGestureStatus
uxtheme.dll.#49
ole32.dll.OleInitialize
ole32.dll.CreateBindCtx

ole32.dll.CoTaskMemAlloc
propsys.dll.PSCreateMemoryPropertyStore
propsys.dll.PSPropertyBag_WriteDWORD
ole32.dll.CoGetApartmentType
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoTaskMemFree
comctl32.dll.#236
oleaut32.dll.#6
ole32.dll.CoGetMalloc
propsys.dll.PSPropertyBag_ReadDWORD
comctl32.dll.#320
ole32.dll.StringFromGUID2
comctl32.dll.#324
comctl32.dll.#323

REGISTRY KEYS

HKEY_CURRENT_USER\Control Panel\Mouse
HKEY_CURRENT_USER\Control Panel\Mouse\SwapMouseButtons
HKEY_CURRENT_USER\Software\AutoIt v3\AutoIt
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\ec4d1dd578dee5f32edebc8b97c99ce9d5f69e1a.exe
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\ec4d1dd578dee5f32edebc8b97c99ce9d5f69e1a.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation

HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions
HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Explorer
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\AccessProviders
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DontShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClassicShell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\SeparateProcess

EXECUTED COMMANDS

C:\Users\user\AppData\Local\Temp\explorer\explorer.exe
C:\Users\user\AppData\Local\Temp\explorer\DNI.docx

READ FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\ec4d1dd578dee5f32edebc8b97c99ce9d5f69e1a.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\UxTheme.dll.Config
C:\Windows\System32\uxtheme.dll

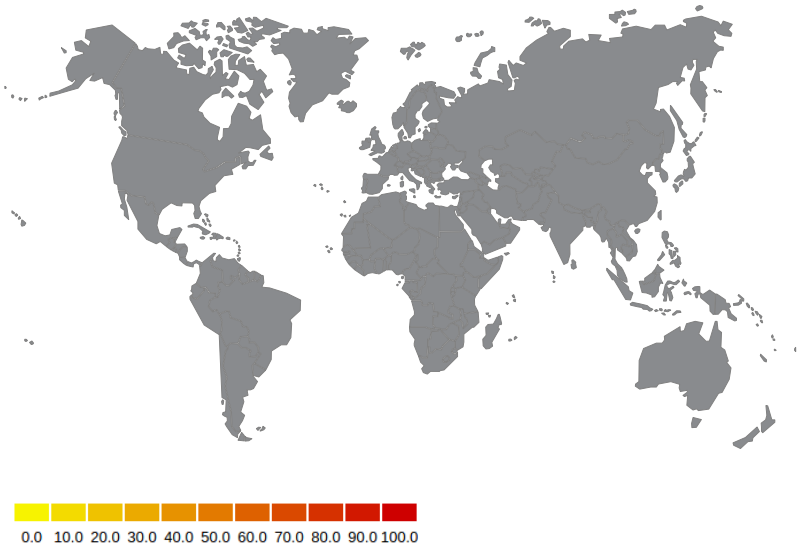
C:\Windows\SysWOW64\shell32.dll
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004b.db
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Windows\SysWOW64\shlwapi.dll
C:\Windows\System32\en-US\DUser.dll.mui
C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\COMCTL32.dll.mui
C:\Windows\System32\imageres.dll
C:\Windows\Fonts\staticcache.dat

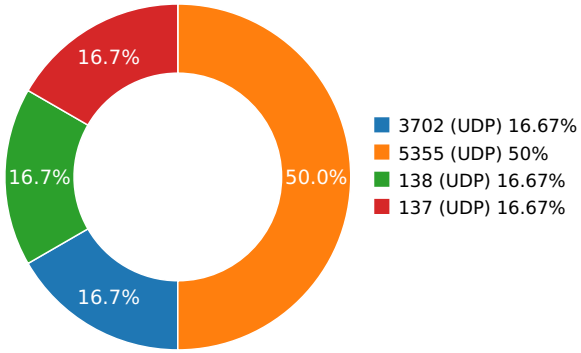
MUTEXES

CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

Network Behavior

CONTACTED IPS	NETWORK PORT DISTRIBUTION





Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.05615496635	Sandbox	224.0.0.252	5355
3.05771613121	Sandbox	224.0.0.252	5355
3.06939697266	Sandbox	239.255.255.250	3702
3.0825521946	Sandbox	192.168.56.255	137
5.61215901375	Sandbox	224.0.0.252	5355
9.07955098152	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	DNI.docx.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	ec4d1dd578dee5f32edebc8b97c99ce9d5f69e1a
MD5:	bb34c3ef615576c659f6f8761233d45d
First Seen Date:	2023-06-30 16:54:29.717715 (3 years ago)
Number Of Clients Seen:	4
Last Analysis Date:	2023-06-30 18:36:47.346149 (3 years ago)
Human Expert Analysis Date:	2023-07-01 17:01:17.144578 (3 years ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	5
Trid	[[61.7, u'Win64 Executable (generic)'], [14.7, u'Win32 Dynamic Link Library (generic)'], [10.0, u'Win32 Executable (generic)'], [4.5, u'OS/2 Executable (generic)'], [4.4, u'Generic Win/DOS Executable']]
Compilation Time Stamp	0x643AB103 [Sat Apr 15 14:13:23 2023 UTC]
ProductVersion	5.14.3.2
FileVersion	5.14.3.1
CompanyName	explorer
Translation	0x0809 0x04b0
Entry Point	0x427f4a (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	838144
Ssdeep	12288:uCdOy3vVrKxR5CXbNjAOxK/j2n+4YG/6c1mFFja3mXgcjfRlgsUBgaVRfQ:uCdxte/80jYLT3U1jfsWaVRfQ
Sha256	9013f2145338d67c6208878ef3ac63739b05c37749b864284496ca986f1c0944
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/e/c/4/d/ec4d1dd578dee5f32edebc8b97c99ce9d5f69e1a', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2023:06:30 16:54:06+00:00', u'EXE:InitializedDataSize': 256000, u'File:FileModifyDate': u'2023:06:30 16:54:06+00:00', u'EXE:FileVersionNumber': u'6.8.5.2', u'EXE:FileVersion': u'5.14.3.1', u'File:FileSize': u'818 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'5.14.3.2', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'explorer', u'File:FileName': u'ec4d1dd578dee5f32edebc8b97c99ce9d5f69e1a', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.1, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2023:04:15 14:13:23+00:00', u'EXE:FileFlagsMask': u'0x0000', u'EXE:LinkerVersion': 12.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/e/c/4/d', u'EXE:EntryPoint': u'0x27f4a', u'EXE:SubsystemVersion': 5.1, u'EXE:CodeSize': 581120, u'File:FileInodeChangeDate': u'2023:06:30 16:54:06+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (British)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'9.15.5.3'}]
Mime Type	application/x-dosexec
Imphash	afcdf79be1557326c854b6e20cb900a7

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x8dd2e	0x8de00	6.67587543996	c2c2260508750422d20cd5cbb116b146
.rdata	0x8f000	0x2e10e	0x2e200	5.76073164877	4513b58651e3d8d87c81a396e5b2f1d1
.data	0xbe000	0x8f74	0x5200	1.19881067447	c2de4a3d214eae7e87c7bfc06bd79775
.rsrc	0xc7000	0x4024	0x4200	4.42616086813	095463d526329ae2375c4f586a38d089
.reloc	0xcc000	0x7130	0x7200	6.78237732804	1254908a9a03d2bcf12045d49cd572b9

PE Imports

- WSOCK32.dll
  - WSACleanup
  - socket
  - inet_ntoa
  - setsockopt
  - ntohs
  - recvfrom
  - ioctlsocket
  - htons
  - WSAStartup
  - __WSAFDIsSet
  - select
  - accept
  - listen
  - bind
  - closesocket
  - WSAGetLastError
  - recv
  - sendto
  - send
  - inet_addr
  - gethostbyname
  - gethostname
  - connect
- VERSION.dll
  - GetFileVersionInfoW
  - GetFileVersionInfoSizeW
  - VerQueryValueW
- WINMM.dll
  - timeGetTime
  - waveOutSetVolume
  - mciSendStringW
- COMCTL32.dll
  - ImageList_ReplaceIcon
  - ImageList_Destroy
  - ImageList_Remove
  - ImageList_SetDragCursorImage
  - ImageList_BeginDrag
  - ImageList_DragEnter
  - ImageList_DragLeave
  - ImageList_EndDrag
  - ImageList_DragMove
  - InitCommonControlsEx
  - ImageList_Create
- MPR.dll
  - WNetUseConnectionW
  - WNetCancelConnection2W
  - WNetGetConnectionW
  - WNetAddConnection2W
- WININET.dll
  - InternetQueryDataAvailable
  - InternetCloseHandle
  - InternetOpenW
  - InternetSetOptionW
  - InternetCrackUrlW
  - HttpQueryInfoW
  - InternetQueryOptionW
  - HttpOpenRequestW
  - HttpSendRequestW

    - FtpOpenFileW
    - FtpGetFileSize
    - InternetOpenUrlW
    - InternetReadFile
    - InternetConnectW
- PSAPI.DLL
    - GetProcessMemoryInfo
- IPHLPAPI.DLL
    - IcmpCreateFile
    - IcmpCloseHandle
    - IcmpSendEcho
- USERENV.dll
    - DestroyEnvironmentBlock
    - UnloadUserProfile
    - CreateEnvironmentBlock
    - LoadUserProfileW
- UxTheme.dll
    - IsThemeActive
- KERNEL32.dll
    - DuplicateHandle
    - CreateThread
    - WaitForSingleObject
    - HeapAlloc
    - GetProcessHeap
    - HeapFree
    - Sleep
    - GetCurrentThreadId
    - MultiByteToWideChar
    - MulDiv
    - GetVersionExW
    - IsWow64Process
    - GetSystemInfo
    - FreeLibrary
    - LoadLibraryA
    - GetProcAddress
    - SetErrorMode
    - GetModuleFileNameW
    - WideCharToMultiByte
    - lstrcpyW
    - lstrlenW
    - GetModuleHandleW
    - QueryPerformanceCounter
    - VirtualFreeEx
    - OpenProcess
    - VirtualAllocEx
    - WriteProcessMemory
    - ReadProcessMemory
    - CreateFileW
    - SetFilePointerEx
    - SetEndOfFile
    - ReadFile
    - WriteFile
    - FlushFileBuffers
    - TerminateProcess
    - CreateToolhelp32Snapshot
    - Process32FirstW
    - Process32NextW
    - SetFileTime
    - GetFileAttributesW
    - FindFirstFileW
    - SetCurrentDirectoryW
    - GetLongPathNameW
    - GetShortPathNameW
    - DeleteFileW
    - FindNextFileW
    - CopyFileExW
    - MoveFileW
    - CreateDirectoryW
    - RemoveDirectoryW
    - SetSystemPowerState
    - QueryPerformanceFrequency
    - FindResourceW
    - LoadResource
    - LockResource
    - SizeofResource

- EnumResourceNamesW
- OutputDebugStringW
- GetTempPathW
- GetTempFileNameW
- DeviceIoControl
- GetLocalTime
- CompareStringW
- GetCurrentProcess
- EnterCriticalSection
- LeaveCriticalSection
- GetStdHandle
- CreatePipe
- InterlockedExchange
- TerminateThread
- LoadLibraryExW
- FindResourceExW
- CopyFileW
- VirtualFree
- FormatMessageW
- GetExitCodeProcess
- GetPrivateProfileStringW
- WritePrivateProfileStringW
- GetPrivateProfileSectionW
- WritePrivateProfileSectionW
- GetPrivateProfileSectionNamesW
- FileTimeToLocalFileTime
- FileTimeToSystemTime
- SystemTimeToFileTime
- LocalFileTimeToFileTime
- GetDriveTypeW
- GetDiskFreeSpaceExW
- GetDiskFreeSpaceW
- GetVolumeInformationW
- SetVolumeLabelW
- CreateHardLinkW
- SetFileAttributesW
- CreateEventW
- SetEvent
- GetEnvironmentVariableW
- SetEnvironmentVariableW
- GlobalLock
- GlobalUnlock
- GlobalAlloc
- GetFileSize
- GlobalFree
- GlobalMemoryStatusEx
- Beep
- GetSystemDirectoryW
- HeapReAlloc
- HeapSize
- GetComputerNameW
- GetWindowsDirectoryW
- GetCurrentProcessId
- GetProcessIoCounters
- CreateProcessW
- GetProcessId
- SetPriorityClass
- LoadLibraryW
- VirtualAlloc
- IsDebuggerPresent
- GetCurrentDirectoryW
- lstrcmpiW
- DecodePointer
- GetLastError
- RaiseException
- InitializeCriticalSectionAndSpinCount
- DeleteCriticalSection
- InterlockedDecrement
- InterlockedIncrement
- GetCurrentThread
- CloseHandle
- GetFullPathNameW
- EncodePointer
- ExitProcess
- GetModuleHandleExW

    - ExitThread
    - GetSystemTimeAsFileTime
    - ResumeThread
    - GetCommandLineW
    - IsProcessorFeaturePresent
    - IsValidCodePage
    - GetACP
    - GetOEMCP
    - GetCPInfo
    - SetLastError
    - UnhandledExceptionFilter
    - SetUnhandledExceptionFilter
    - TlsAlloc
    - TlsGetValue
    - TlsSetValue
    - TlsFree
    - GetStartupInfoW
    - GetStringTypeW
    - SetStdHandle
    - GetFileType
    - GetConsoleCP
    - GetConsoleMode
    - RtlUnwind
    - ReadConsoleW
    - GetTimeZoneInformation
    - GetDateFormatW
    - GetTimeFormatW
    - LCMapStringW
    - GetEnvironmentStringsW
    - FreeEnvironmentStringsW
    - WriteConsoleW
    - FindClose
    - SetEnvironmentVariableA
- USER32.dll
    - AdjustWindowRectEx
    - CopyImage
    - SetWindowPos
    - GetCursorInfo
    - RegisterHotKey
    - ClientToScreen
    - GetKeyboardLayoutNameW
    - IsCharAlphaW
    - IsCharAlphaNumericW
    - IsCharLowerW
    - IsCharUpperW
    - GetMenuStringW
    - GetSubMenu
    - GetCaretPos
    - IsZoomed
    - MonitorFromPoint
    - GetMonitorInfoW
    - SetWindowLongW
    - SetLayeredWindowAttributes
    - FlashWindow
    - GetClassLongW
    - TranslateAcceleratorW
    - IsDialogMessageW
    - GetSysColor
    - InflateRect
    - DrawFocusRect
    - DrawTextW
    - FrameRect
    - DrawFrameControl
    - FillRect
    - PtInRect
    - DestroyAcceleratorTable
    - CreateAcceleratorTableW
    - SetCursor
    - GetWindowDC
    - GetSystemMetrics
    - GetActiveWindow
    - CharNextW
    - wsprintfW
    - RedrawWindow
    - DrawMenuBar

- DestroyMenu
- SetMenu
- GetWindowTextLengthW
- CreateMenu
- IsDlgButtonChecked
- DefDlgProcW
- CallWindowProcW
- ReleaseCapture
- SetCapture
- CreateIconFromResourceEx
- mouse_event
- ExitWindowsEx
- SetActiveWindow
- FindWindowExW
- EnumThreadWindows
- SetMenuDefaultItem
- InsertMenuItemW
- IsMenu
- TrackPopupMenuEx
- GetCursorPos
- DeleteMenu
- SetRect
- GetMenuItemID
- GetMenuItemCount
- SetMenuItemInfoW
- GetMenuItemInfoW
- SetForegroundWindow
- IsIconic
- FindWindowW
- MonitorFromRect
- keybd_event
- SendInput
- GetAsyncKeyState
- SetKeyboardState
- GetKeyboardState
- GetKeyState
- VkKeyScanW
- LoadStringW
- DialogBoxParamW
- MessageBeep
- EndDialog
- SendDlgItemMessageW
- GetDlgItem
- SetWindowTextW
- CopyRect
- ReleaseDC
- GetDC
- EndPaint
- BeginPaint
- GetClientRect
- GetMenu
- DestroyWindow
- EnumWindows
- GetDesktopWindow
- IsWindow
- IsWindowEnabled
- IsWindowVisible
- EnableWindow
- InvalidateRect
- GetWindowLongW
- GetWindowThreadProcessId
- AttachThreadInput
- GetFocus
- GetWindowTextW
- ScreenToClient
- SendMessageTimeoutW
- EnumChildWindows
- CharUpperBuffW
- GetParent
- GetDlgCtrlID
- SendMessageW
- MapVirtualKeyW
- PostMessageW
- GetWindowRect
- SetUserObjectSecurity

    - CloseDesktop
    - CloseWindowStation
    - OpenDesktopW
    - SetProcessWindowStation
    - GetProcessWindowStation
    - OpenWindowStationW
    - GetUserObjectSecurity
    - MessageBoxW
    - DefWindowProcW
    - SetClipboardData
    - EmptyClipboard
    - CountClipboardFormats
    - CloseClipboard
    - GetClipboardData
    - IsClipboardFormatAvailable
    - OpenClipboard
    - BlockInput
    - GetMessageW
    - LockWindowUpdate
    - DispatchMessageW
    - TranslateMessage
    - PeekMessageW
    - UnregisterHotKey
    - CheckMenuRadioItem
    - CharLowerBuffW
    - MoveWindow
    - SetFocus
    - PostQuitMessage
    - KillTimer
    - CreatePopupMenu
    - RegisterWindowMessageW
    - SetTimer
    - ShowWindow
    - CreateWindowExW
    - RegisterClassExW
    - LoadIconW
    - LoadCursorW
    - GetSysColorBrush
    - GetForegroundWindow
    - MessageBoxA
    - DestroyIcon
    - SystemParametersInfoW
    - LoadImageW
    - GetClassNameW
- GDI32.dll
    - StrokePath
    - DeleteObject
    - GetTextExtentPoint32W
    - ExtCreatePen
    - GetDeviceCaps
    - EndPath
    - SetPixel
    - CloseFigure
    - CreateCompatibleBitmap
    - CreateCompatibleDC
    - SelectObject
    - StretchBlt
    - GetDIBits
    - LineTo
    - AngleArc
    - MoveToEx
    - Ellipse
    - DeleteDC
    - GetPixel
    - CreateDCW
    - GetStockObject
    - GetTextFaceW
    - CreateFontW
    - SetTextColor
    - PolyDraw
    - BeginPath
    - Rectangle
    - SetViewportOrgEx
    - GetObjectW
    - SetBkMode

    - RoundRect
    - SetBkColor
    - CreatePen
    - CreateSolidBrush
    - StrokeAndFillPath
- COMDLG32.dll
    - GetOpenFileNameW
    - GetSaveFileNameW
- ADVAPI32.dll
    - GetAce
    - RegEnumValueW
    - RegDeleteValueW
    - RegDeleteKeyW
    - RegEnumKeyExW
    - RegSetValueExW
    - RegOpenKeyExW
    - RegCloseKey
    - RegQueryValueExW
    - RegConnectRegistryW
    - InitializeSecurityDescriptor
    - InitializeAcl
    - AdjustTokenPrivileges
    - OpenThreadToken
    - OpenProcessToken
    - LookupPrivilegeValueW
    - DuplicateTokenEx
    - CreateProcessAsUserW
    - CreateProcessWithLogonW
    - GetLengthSid
    - CopySid
    - LogonUserW
    - AllocateAndInitializeSid
    - CheckTokenMembership
    - RegCreateKeyExW
    - FreeSid
    - GetTokenInformation
    - GetSecurityDescriptorDacl
    - GetAclInformation
    - AddAce
    - SetSecurityDescriptorDacl
    - GetUserNameW
    - InitiateSystemShutdownExW
- SHELL32.dll
    - DragQueryPoint
    - ShellExecuteExW
    - DragQueryFileW
    - SHEmptyRecycleBinW
    - SHGetPathFromIDListW
    - SHBrowseForFolderW
    - SHCreateShellItem
    - SHGetDesktopFolder
    - SHGetSpecialFolderLocation
    - SHGetFolderPathW
    - SHFileOperationW
    - ExtractIconExW
    - Shell_NotifyIconW
    - ShellExecuteW
    - DragFinish
- ole32.dll
    - CoTaskMemAlloc
    - CoTaskMemFree
    - CLSIDFromString
    - ProgIDFromCLSID
    - CLSIDFromProgID
    - OleSetMenuDescriptor
    - MkParseDisplayName
    - OleSetContainedObject
    - CoCreateInstance
    - IIDFromString
    - StringFromGUID2
    - CreateStreamOnHGlobal
    - OleInitialize
    - OleUninitialize
    - CoInitialize
    - CoUninitialize

- GetRunningObjectTable
- CoGetInstanceFromFile
- CoGetObject
- CoSetProxyBlanket
- CoCreateInstanceEx
- CoInitializeSecurity

- OLEAUT32.dll
  - LoadTypeLibEx
  - VariantCopyInd
  - SysReAllocString
  - SysFreeString
  - SafeArrayDestroyDescriptor
  - SafeArrayDestroyData
  - SafeArrayUnaccessData
  - SafeArrayAccessData
  - SafeArrayAllocData
  - SafeArrayAllocDescriptorEx
  - SafeArrayCreateVector
  - RegisterTypeLib
  - CreateStdDispatch
  - DispCallFunc
  - VariantChangeType
  - SysStringLen
  - VariantTimeToSystemTime
  - VarR8FromDec
  - SafeArrayGetVartype
  - VariantCopy
  - VariantClear
  - OleLoadPicture
  - QueryPathOfRegTypeLib
  - RegisterTypeLibForUser
  - UnRegisterTypeLibForUser
  - UnRegisterTypeLib
  - CreateDispTypeInfo
  - SysAllocString
  - VariantInit

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 815952, u'sha256': u'245fc49e4e955e1db3975b826dcf27ad2eb32a6831caa4cb6b501a3914bcfaa9', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 816248, u'sha256': u'd600403cdb8f3e53190412c75e8f2928b2add06a0f8000be6cfbf75c387b2206', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 820512, u'sha256': u'4fe35e21717d34ceb4717f9e9de8fde1b3de80d76a59bb87405910c2f1d6284b', u'type': u'data', u'size': 1428}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 821940, u'sha256': u'9306910d4bb273465765832df77fb1fd78bd6e0bcbf9908636e323c34c92b613', u'type': u'data', u'size': 1674}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 823616, u'sha256': u'e47fa3aec12353f6370b941bc5855e5551530c7b26f925b5a2e2692a0201450c', u'type': u'data', u'size': 1168}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 824784, u'sha256': u'4854e5abce2237256df24b69c9759fc1e8caa423a54bfe661ba7031afd8375eb', u'type': u'data', u'size': 1532}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 826316, u'sha256': u'd38369002e36f73866a0d40b13e069b9ffdbda50957f4c88d52a72fecb9b4e45', u'type': u'data', u'size': 1628}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 827944, u'sha256': u'58ea125e6b5fa2cbc5a8ed819c7f50c9bca1cfe55f94c7cff3feb60f25ac6073', u'type': u'data', u'size': 1126}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 829072, u'sha256': u'b3711acbe8e01fee7fd362112b4e42da05c728e98b85c0a3b4cb075977849cee', u'type': u'data', u'size': 344}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 829416, u'sha256': u'158ccc2c23fec3ef582233193402f8b463710e480c98894d6d4b762fc3873451', u'type': u'data', u'size': 678}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 830096, u'sha256': u'852391035320228f8de3412c040f63d082abc6cc8ab8d715d1d5a92c243cbd97', u'type': u'MS Windows icon resource - 1 icon, 32x32', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 830116, u'sha256': u'ae172a9a2fd008910b537c92a95b38bfba0e5bbdaaca719bf686e6415a7a2ba1', u'type': u'MS Windows icon resource - 1 icon, 16x16, 16 colors', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 830136, u'sha256': u'6b7a67eeb27d2f22efaac88a9d9afd86a0d38ffb084d19df169695a5ae58bfcc', u'type': u'data', u'size': 380}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 830516, u'sha256': u'1bd8139910a81485aadb0bb28586e233768486de8c09f6a565ae457805702d39', u'type': u'ASCII text, with CRLF line terminators', u'size': 1007}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS