VALKYRIE COMODO

Summary

File Name: Odeme_Onay_Kopyas.exe

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

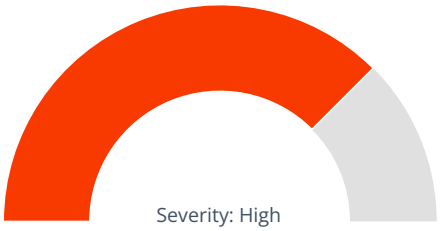
SHA1: b2965a7783b66b66618be73bf8115e92dab29b57

MD5: 706aa6e6ec6c73d221f82bd4ab0d12c8

MALWARE

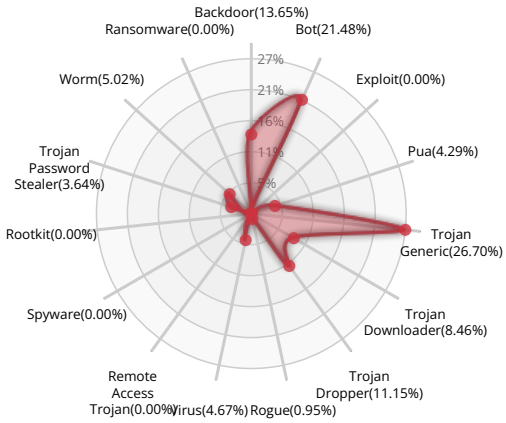
Valkyrie Final Verdict

DETECTION SECTION

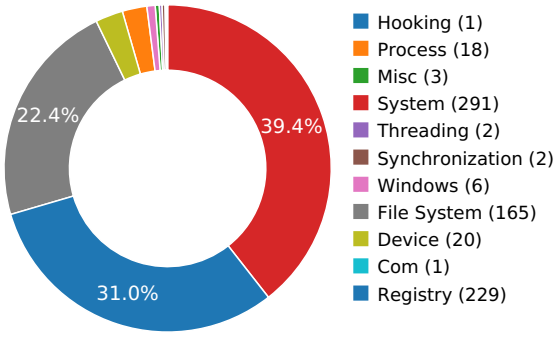


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

STATIC ANOMALY

Anomalous binary characteristics — Show sources

MALWARE ANALYSIS SYSTEM EVASION

Network activity detected but not expressed in API logs

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\b2965a7783b66b66618be73bf8115e92dab29b57.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\SysWOW64\shell32.dll
C:\
C:\Users
C:\Users\desktop.ini
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
\Device\KsecDD
\??\MountPointManager
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\b2965a7783b66b66618be73bf8115e92dab29b57.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
C:\Users\user\AppData\Local\Temp\Countee
C:\Windows\SysWOW64\ntdll.dll

READ REGISTRY KEYS

HKEY_CURRENT_USER\Control Panel\Mouse\SwapMouseButtons
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\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
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_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
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\AllowFileCLSIDJunctions
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\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue

kernel32.dll.FlsFree
kernel32.dll.IsProcessorFeaturePresent
kernel32.dll.IsWow64Process
kernel32.dll.GetNativeSystemInfo
uxtheme.dll.IsThemeActive
ole32.dll.CoGetMalloc
ole32.dll.CoGetApartmentType
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
ole32.dll.CoTaskMemFree
comctl32.dll.#236
oleaut32.dll.#6
ole32.dll.CoTaskMemAlloc
ole32.dll.CreateBindCtx
comctl32.dll.#320
ole32.dll.StringFromGUID2
comctl32.dll.#324
comctl32.dll.#323
comctl32.dll.#388
comctl32.dll.#328
comctl32.dll.#334
advapi32.dll.RegEnumKeyW
oleaut32.dll.#2
ole32.dll.CoCreateInstance
advapi32.dll.IsTextUnicode
comctl32.dll.#332
comctl32.dll.#338
comctl32.dll.#339
advapi32.dll.OpenThreadToken
shell32.dll.#102
ole32.dll.CoInitializeEx
cryptbase.dll.SystemFunction036
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoUninitialize

ole32.dll.CoRevokeInitializeSpy
oleaut32.dll.#500
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
comctl32.dll.#386
dwmapi.dll.DwmIsCompositionEnabled
comctl32.dll.RegisterClassNameW
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
shell32.dll.#66
kernel32.dll.VirtualProtect
user32.dll.CallWindowProcA
comctl32.dll.#321

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\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\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\Windows\CurrentVersion\ShellCompatibility\Applications\b2965a7783b66b66618be73bf8115e92dab29b57.exe
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\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_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
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
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

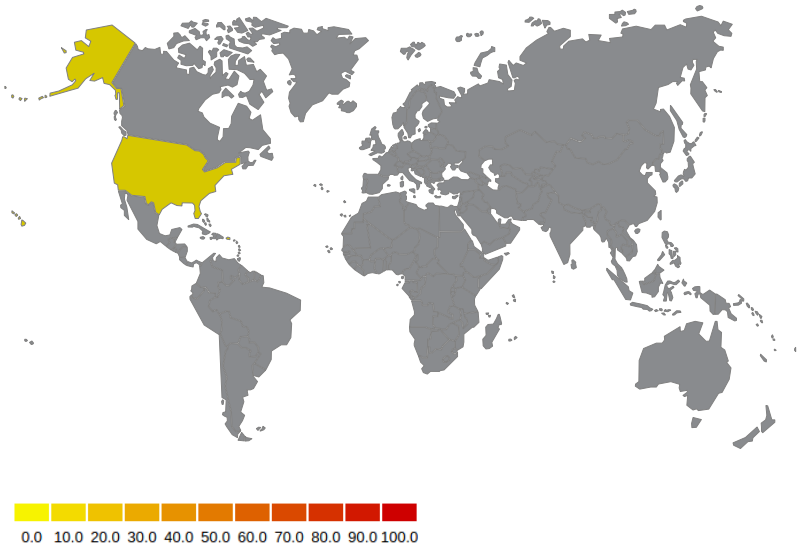
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\NoNetCrawling
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AutoCheckSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\IconsOnly
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowTypeOverlay

READ FILES

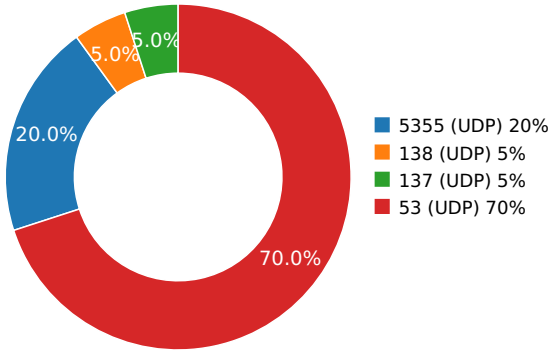
C:\Users\user\AppData\Local\Temp\b2965a7783b66b66618be73bf8115e92dab29b57.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\SysWOW64\shell32.dll
C:\
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
\Device\KsecDD
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\Countee
C:\Windows\SysWOW64\ntdll.dll

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Google LLC	Malware Process
	8.8.8.8	United States	15169	Google LLC	Malware Process
					Malware Process
www.aieov.com	45.33.23.183	United States	63949	Akamai Technologies, Inc.	Malware Process

DNS QUERIES

Request	Type
5isohu.com	A
www.aieov.com	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.04993700981	Sandbox	224.0.0.252	5355
3.05028891563	Sandbox	224.0.0.252	5355
3.07848381996	Sandbox	192.168.56.255	137
3.70192193985	Sandbox	224.0.0.252	5355
5.61064887047	Sandbox	224.0.0.252	5355
6.38971090317	Sandbox	8.8.4.4	53
7.4063668251	Sandbox	8.8.8.8	53
9.17302203178	Sandbox	192.168.56.255	138
20.9227809906	Sandbox	8.8.8.8	53
21.9220399857	Sandbox	8.8.4.4	53
35.363049984	Sandbox	8.8.8.8	53
36.3599069118	Sandbox	8.8.4.4	53
50.1605148315	Sandbox	8.8.8.8	53
51.1563799381	Sandbox	8.8.4.4	53
64.5790839195	Sandbox	8.8.8.8	53
65.5782499313	Sandbox	8.8.4.4	53
79.0635929108	Sandbox	8.8.8.8	53
80.0642268658	Sandbox	8.8.4.4	53
97.3765239716	Sandbox	8.8.8.8	53
98.3755748272	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Countee	**Type :** data **MD5 :** 2d8cc9f55048e791ceb27994ab65e768 **SHA-1 :** 5697d2fb44339dde5b097138c994fce26f3a0e8d **SHA-256 :** 9985b902235d4c4692e8e3ae0946864f9d7b464! **SHA-512 :** 2d352ead6150360867a0acf69e58d9aa265bc5f0 **Size :** 286.72 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	Odeme_Onay_Kopyas.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	b2965a7783b66b66618be73bf8115e92dab29b57
MD5:	706aa6e6ec6c73d221f82bd4ab0d12c8
First Seen Date:	2024-10-17 07:57:47.342496 (11 days ago)
Number Of Clients Seen:	4
Last Analysis Date:	2024-10-17 07:57:47.342496 (11 days ago)
Human Expert Analysis Date:	2024-10-18 15:44:21.312619 (10 days 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	4
Trid	[[92.2, u'AutoIt3 compiled script executable'], [4.9, u'Win64 Executable (generic)'], [1.1, u'Win32 Dynamic Link Library (generic)'], [0.8, u'Win32 Executable (generic)'], [0.3, u'Generic Win/DOS Executable']]
Compilation Time Stamp	0x4B93CF87 [Sun Mar 7 16:08:39 2010 UTC]
CompiledScript	AutoIt v3 Script: 3, 3, 6, 0
FileVersion	3, 3, 6, 0
FileDescription	
Translation	0x0809 0x04b0
Entry Point	0x416310 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	1345613
Ssdeep	24576:ffmMv6Ckr7Mny5QLocrS5yyr/yqQP47WkyWu3bGldnfWg2W3df4UEZ:f3v+7/5QLop5Rzs47flu6lZfT2WhXEZ
Sha256	a70f2a55eaca82a3a62eeb3a9d0273dd637b43c3697ed9dac1c0a5e0d708e093
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/b/2/9/6/b2965a7783b66b66618be73bf8115e92dab29b57', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2024:10:17 07:57:07+00:00', u'EXE:InitializedDataSize': 120320, u'File:FileModifyDate': u'2024:10:17 07:56:45+00:00', u'EXE:FileVersionNumber': u'3.3.6.0', u'EXE:FileVersion': u'3, 3, 6, 0', u'File:FileSize': u'1314 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:CompiledScript': u'AutoIt v3 Script: 3, 3, 6, 0', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ObjectFileType': u'Unknown', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 0, u'File:FileName': u'b2965a7783b66b66618be73bf8115e92dab29b57', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2010:03:07 16:08:39+00:00', u'EXE:FileFlagsMask': u'0x0017', u'EXE:LinkerVersion': 9.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/b/2/9/6', u'EXE:FileDescription': u'', u'EXE:EntryPoint': u'0x16310', u'EXE:SubsystemVersion': 5.0, u'EXE:CodeSize': 524800, u'File:FileInodeChangeDate': u'2024:10:17 07:57:06+00:00', u'EXE:LanguageCode': u'English (British)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'3.3.6.0'}]
Mime Type	application/x-dosexec
Imphash	aaaa8913c89c8aa4a5d93f06853894da

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x80017	0x80200	6.63468823026	6c20c6bf686768b6f134f5bd508171bc
.rdata	0x82000	0xd95c	0xda00	4.88004082412	f979966509a93083729d23cdfd2a6f2d
.data	0x90000	0x1a518	0x6800	2.20176498963	e5d77411f751d28c6eee48a743606795
.rsrc	0xab000	0x9298	0x9400	5.53030308978	f6be76de0ef2c68f397158bf01bdef3e

PE Imports

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

    - InternetQueryOptionW
    - InternetQueryDataAvailable
- PSAPI.DLL
    - EnumProcesses
    - GetModuleBaseNameW
    - GetProcessMemoryInfo
    - EnumProcessModules
- USERENV.dll
    - CreateEnvironmentBlock
    - DestroyEnvironmentBlock
    - UnloadUserProfile
    - LoadUserProfileW
- KERNEL32.dll
    - HeapAlloc
    - Sleep
    - GetCurrentThreadId
    - RaiseException
    - MulDiv
    - GetVersionExW
    - GetSystemInfo
    - MultiByteToWideChar
    - WideCharToMultiByte
    - GetModuleHandleW
    - QueryPerformanceCounter
    - VirtualFreeEx
    - OpenProcess
    - VirtualAllocEx
    - WriteProcessMemory
    - ReadProcessMemory
    - CreateFileW
    - SetFilePointerEx
    - ReadFile
    - WriteFile
    - FlushFileBuffers
    - TerminateProcess
    - CreateToolhelp32Snapshot
    - Process32FirstW
    - Process32NextW
    - SetFileTime
    - GetFileAttributesW
    - FindFirstFileW
    - FindClose
    - DeleteFileW
    - FindNextFileW
    - lstrcmpiW
    - MoveFileW
    - CopyFileW
    - CreateDirectoryW
    - RemoveDirectoryW
    - SetSystemPowerState
    - QueryPerformanceFrequency
    - FindResourceW
    - LoadResource
    - LockResource
    - SizeofResource
    - GetProcessHeap
    - OutputDebugStringW
    - GetLocalTime
    - CompareStringW
    - CompareStringA
    - InterlockedIncrement
    - InterlockedDecrement
    - DeleteCriticalSection
    - EnterCriticalSection
    - LeaveCriticalSection
    - InitializeCriticalSectionAndSpinCount
    - GetStdHandle
    - CreatePipe
    - InterlockedExchange
    - TerminateThread
    - GetTempPathW
    - GetTempFileNameW
    - VirtualFree
    - FormatMessageW
    - GetExitCodeProcess

- SetErrorMode
- GetPrivateProfileStringW
- WritePrivateProfileStringW
- GetPrivateProfileSectionW
- WritePrivateProfileSectionW
- GetPrivateProfileSectionNamesW
- FileTimeToLocalFileTime
- FileTimeToSystemTime
- SystemTimeToFileTime
- LocalFileTimeToFileTime
- GetDriveTypeW
- GetDiskFreeSpaceExW
- GetDiskFreeSpaceW
- GetVolumeInformationW
- SetVolumeLabelW
- CreateHardLinkW
- DeviceIoControl
- SetFileAttributesW
- GetShortPathNameW
- CreateEventW
- SetEvent
- GetEnvironmentVariableW
- SetEnvironmentVariableW
- GlobalLock
- GlobalUnlock
- GlobalAlloc
- GetFileSize
- GlobalFree
- GlobalMemoryStatusEx
- Beep
- GetComputerNameW
- GetWindowsDirectoryW
- GetSystemDirectoryW
- GetCurrentProcessId
- GetCurrentThread
- GetProcessIoCounters
- CreateProcessW
- SetPriorityClass
- LoadLibraryW
- VirtualAlloc
- LoadLibraryExW
- HeapFree
- WaitForSingleObject
- CreateThread
- DuplicateHandle
- GetLastError
- CloseHandle
- GetCurrentProcess
- GetProcAddress
- LoadLibraryA
- FreeLibrary
- GetModuleFileNameW
- GetFullPathNameW
- ExitProcess
- ExitThread
- GetSystemTimeAsFileTime
- SetCurrentDirectoryW
- IsDebuggerPresent
- GetCurrentDirectoryW
- ResumeThread
- GetStartupInfoW
- TlsGetValue
- TlsAlloc
- TlsSetValue
- TlsFree
- SetLastError
- HeapSize
- GetCPInfo
- GetACP
- GetOEMCP
- IsValidCodePage
- UnhandledExceptionFilter
- SetUnhandledExceptionFilter
- GetModuleFileNameA
- HeapReAlloc

    - HeapCreate
    - SetHandleCount
    - GetFileType
    - GetStartupInfoA
    - SetStdHandle
    - GetConsoleCP
    - GetConsoleMode
    - LCMapStringW
    - LCMapStringA
    - RtlUnwind
    - SetFilePointer
    - GetTimeZoneInformation
    - GetTimeFormatA
    - GetDateFormatA
    - FreeEnvironmentStringsW
    - GetEnvironmentStringsW
    - GetCommandLineW
    - GetTickCount
    - GetStringTypeA
    - GetStringTypeW
    - GetLocaleInfoA
    - GetModuleHandleA
    - WriteConsoleA
    - GetConsoleOutputCP
    - WriteConsoleW
    - CreateFileA
    - SetEndOfFile
    - EnumResourceNamesW
    - SetEnvironmentVariableA
- USER32.dll
    - 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

- ReleaseCapture
- SetCapture
- WindowFromPoint
- CreateIconFromResourceEx
- mouse_event
- ExitWindowsEx
- SetActiveWindow
- FindWindowExW
- EnumThreadWindows
- SetMenuDefaultItem
- InsertMenuItemW
- IsMenu
- TrackPopupMenuEx
- GetCursorPos
- DeleteMenu
- CheckMenuRadioItem
- CopyImage
- GetMenuItemCount
- SetMenuItemInfoW
- GetMenuItemInfoW
- SetForegroundWindow
- IsIconic
- FindWindowW
- SystemParametersInfoW
- PeekMessageW
- 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
- GetWindowThreadProcessId
- AttachThreadInput
- GetFocus
- GetWindowTextW
- ScreenToClient
- SendMessageTimeoutW
- EnumChildWindows
- CharUpperBuffW
- GetClassNameW
- GetParent
- GetDlgCtrlID
- SendMessageW
- MapVirtualKeyW
- PostMessageW
- GetWindowRect
- SetUserObjectSecurity
- GetUserObjectSecurity
- CloseDesktop
- CloseWindowStation
- OpenDesktopW
- SetProcessWindowStation
- GetProcessWindowStation

    - OpenWindowStationW
    - MessageBoxW
    - DefWindowProcW
    - MoveWindow
    - AdjustWindowRectEx
    - SetRect
    - SetClipboardData
    - EmptyClipboard
    - CountClipboardFormats
    - CloseClipboard
    - GetClipboardData
    - IsClipboardFormatAvailable
    - OpenClipboard
    - BlockInput
    - GetMessageW
    - LockWindowUpdate
    - DispatchMessageW
    - GetMenuItemID
    - TranslateMessage
    - SetFocus
    - PostQuitMessage
    - KillTimer
    - CreatePopupMenu
    - RegisterWindowMessageW
    - SetTimer
    - ShowWindow
    - CreateWindowExW
    - RegisterClassExW
    - LoadIconW
    - LoadCursorW
    - GetSysColorBrush
    - GetForegroundWindow
    - MessageBoxA
    - DestroyIcon
    - UnregisterHotKey
    - CharLowerBuffW
    - MonitorFromRect
    - keybd_event
    - LoadImageW
    - GetWindowLongW
- GDI32.dll
    - DeleteObject
    - GetObjectW
    - GetTextExtentPoint32W
    - ExtCreatePen
    - StrokeAndFillPath
    - StrokePath
    - EndPath
    - SetPixel
    - CloseFigure
    - CreateCompatibleBitmap
    - CreateCompatibleDC
    - SelectObject
    - StretchBlt
    - GetDIBits
    - LineTo
    - AngleArc
    - MoveToEx
    - Ellipse
    - PolyDraw
    - BeginPath
    - Rectangle
    - GetDeviceCaps
    - SetBkMode
    - RoundRect
    - SetBkColor
    - CreatePen
    - CreateSolidBrush
    - SetTextColor
    - CreateFontW
    - GetTextFaceW
    - GetStockObject
    - CreateDCW
    - GetPixel
    - DeleteDC

    - SetViewportOrgEx
- COMDLG32.dll
    - GetSaveFileNameW
    - GetOpenFileNameW
- ADVAPI32.dll
    - RegEnumValueW
    - RegDeleteValueW
    - RegDeleteKeyW
    - RegSetValueExW
    - RegCreateKeyExW
    - GetUserNameW
    - RegConnectRegistryW
    - RegEnumKeyExW
    - CloseServiceHandle
    - UnlockServiceDatabase
    - LockServiceDatabase
    - OpenSCManagerW
    - InitiateSystemShutdownExW
    - AdjustTokenPrivileges
    - RegCloseKey
    - RegQueryValueExW
    - RegOpenKeyExW
    - OpenThreadToken
    - OpenProcessToken
    - LookupPrivilegeValueW
    - DuplicateTokenEx
    - CreateProcessAsUserW
    - CreateProcessWithLogonW
    - InitializeSecurityDescriptor
    - InitializeAcl
    - GetLengthSid
    - SetSecurityDescriptorDacl
    - CopySid
    - LogonUserW
    - GetTokenInformation
    - GetAclInformation
    - GetAce
    - AddAce
    - GetSecurityDescriptorDacl
- SHELL32.dll
    - DragQueryPoint
    - ShellExecuteExW
    - SHGetFolderPathW
    - DragQueryFileW
    - SHEmptyRecycleBinW
    - SHBrowseForFolderW
    - SHFileOperationW
    - SHGetPathFromIDListW
    - SHGetDesktopFolder
    - SHGetMalloc
    - ExtractIconExW
    - Shell_NotifyIconW
    - ShellExecuteW
    - DragFinish
- ole32.dll
    - OleSetMenuDescriptor
    - MkParseDisplayName
    - OleSetContainedObject
    - CoInitialize
    - CoUninitialize
    - CoCreateInstance
    - CreateStreamOnHGlobal
    - CoTaskMemAlloc
    - CoTaskMemFree
    - CLSIDFromString
    - StringFromCLSID
    - IIDFromString
    - StringFromIID
    - OleInitialize
    - CreateBindCtx
    - CLSIDFromProgID
    - CoInitializeSecurity
    - CoCreateInstanceEx
    - CoSetProxyBlanket
    - OleUninitialize

- OLEAUT32.dll
  - SafeArrayAllocData
  - SafeArrayAllocDescriptorEx
  - SysAllocString
  - OleLoadPicture
  - SafeArrayGetVartype
  - SafeArrayDestroyData
  - SafeArrayAccessData
  - VarR8FromDec
  - VariantTimeToSystemTime
  - VariantClear
  - VariantCopy
  - VariantInit
  - SafeArrayDestroyDescriptor
  - LoadRegTypeLib
  - GetActiveObject
  - SafeArrayUnaccessData

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 701896, u'sha256': u'08bcba5aa989c988ea18f8101c84daaee58d4f0b584535a85186c8b98b66147e', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 702192, u'sha256': u'62ba0b2575098d4428c9a99bd060ef7572071698bf9d03b4bd430f5f691378e5', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 702488, 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': 702784, u'sha256': u'7ed6c1961c0af686116a20a9af1749b250855cde0dbb6d22709769d78856f47a', u'type': u'data', u'size': 1640}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 704424, u'sha256': u'b1536ed3ce7dd68c4aff2a50b0b7b94a41461ee59a1bc1a5db852915311bd6bd', u'type': u'dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2005399800, next used block 8452216', u'size': 744}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 705168, u'sha256': u'9803deebb424e82f73c26dc00c0b8df765ebde020e673fab8a6ff6faa38588e2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 705464, u'sha256': u'3beadf2cf64cbd321f31a554775f7839eebc911a695a7815731f9933cd873a71', u'type': u'data', u'size': 3752}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 709216, u'sha256': u'79db4f9306690bfd5e7b8b11f38a5629e24910bd5d0fa535404368b371ff0e5b', u'type': u'dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 13490662, next used block 13885161', u'size': 2216}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 711432, u'sha256': u'ebfd43bb200d33cf702cbaf6824cbb4a9e5f75d52470d805370b316bc2622710', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 712816, u'sha256': u'4c78e116fb08293b0883a8d1fa1a8b58c1c08fbd1c2aa89d1a41951632d18c0e', u'type': u'data', u'size': 9640}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 722456, u'sha256': u'cb11fa807d0d7258941541d7ed11e2866330f9c487de2dc3ffde68ff054672f3', u'type': u'data', u'size': 4264}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 726720, u'sha256': u'10d8d1d5d34a6d375fe241ef289d303f40e59680b8c33b0307325f03a3f2185e', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_MENU', u'offset': 727848, u'sha256': u'54f5e2ecbfc4f87380ca7466337676b99d0c4a21f806cf83f69fd48934c857ab', u'type': u'data', u'size': 80}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 727928, u'sha256': u'7de7438fb4425f608109111fdce25be7d2381938f6c5984bcfb14b3b88e9c883', u'type': u'data', u'size': 252}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 728184, u'sha256': u'ff841c2dd3b09d5a11dd9b16d09268adc0ac3562eb0dc79cc5044dc531de6477', u'type': u'data', u'size': 1328}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 729512, u'sha256': u'3f37dba0277dc704f072aaf3e740c2bee9ac04f79982fd41662dfc94e7bfda2e', u'type': u'data', u'size': 1680}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 731192, u'sha256': u'322afa4fa7a6e6cb4eb0b276d8feeeee558ec0df828e3ed8859b0506d39a38b4', u'type': u'data', u'size': 1082}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 732280, u'sha256': u'4854e5abce2237256df24b69c9759fc1e8caa423a54bfe661ba7031afd8375eb', u'type': u'data', u'size': 1532}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 733816, u'sha256': u'd38369002e36f73866a0d40b13e069b9ffdbda50957f4c88d52a72fecb9b4e45', u'type': u'data', u'size': 1628}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 735448, u'sha256': u'ae9b084978e14d5bfa296e256820765b30a7b3e411cdccc67c91e146f053e815', u'type': u'data', u'size': 904}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 736352, u'sha256': u'b3711acbe8e01fee7fd362112b4e42da05c728e98b85c0a3b4cb075977849cee', u'type': u'data', u'size': 344}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 736696, u'sha256': u'5d62d392a0f454a05c957c41003db41c4faabf09156725ca8ce9d6622b22ca71', u'type': u'MS Windows icon resource - 9 icons, 48x48, 16 colors', u'size': 132}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 736832, 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_GROUP_ICON', u'offset': 736856, u'sha256':

u'6bcce1250099cc08d574211b3debabb0244cd2641f6d960538e7ddc97d319164', u'type': u'MS Windows icon resource - 1 icon, 16x16, 16 colors', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 736880, u'sha256': u'7698ef362b288a7e3b96304ca50814b42518cba38598db9dbb36d8b90212d76a', 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': 736904, u'sha256': u'81f4d0ba1102bc1ecb247be3241bfaef9045aaff2aaf84db50f135c57ae23f58', u'type': u'data', u'size': 412}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 737320, u'sha256': u'6fb2f428ceb740481a982bfa8d6718e01c1cac512f6848fcd78ddf56df9ec877', u'type': u'ASCII text, with CRLF line terminators', u'size': 620}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS