VALKYRIE COMODO

Summary

File Name: GoToWebinar_Opener.exe

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

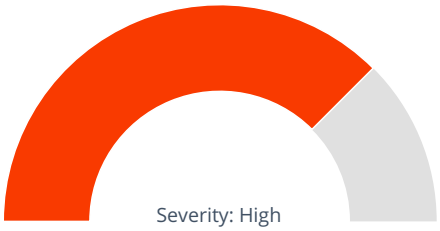
SHA1: 80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3

MD5: 6948c07a98c64a5ea68dab822e4fb6ab

MALWARE

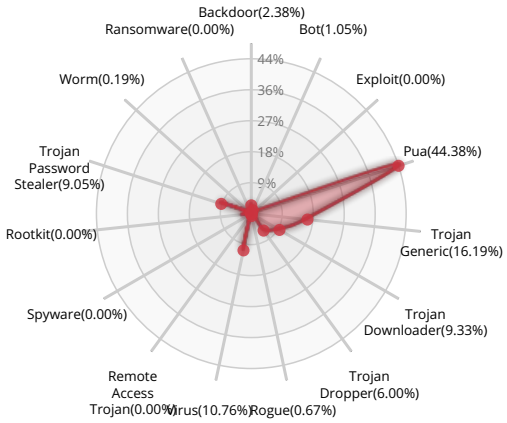
Valkyrie Final Verdict

DETECTION SECTION

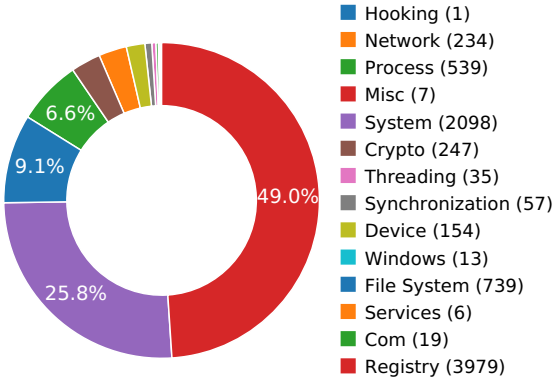


Verdict: Malware

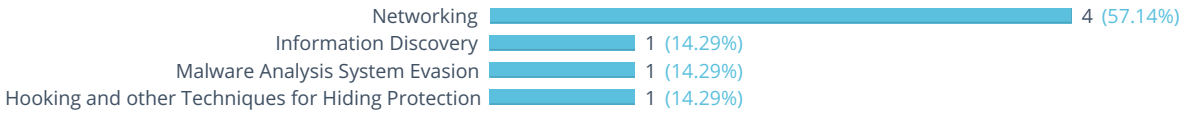
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

NETWORKING

Attempts to connect to a dead IP:Port (3 unique times) — Show sources

Performs some HTTP requests — Show sources

Network activity contains more than one unique useragent. — Show sources

A process sent information about the computer to a remote location. — Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task. — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

VALKYRIE COMODO

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\system\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\api-ms-win-core-fibers-l1-1-1.DLL
C:\ProgramData\Oracle\Java\javapath\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\wbem\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Universal Extractor\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-core-fibers-l1-1-1.DLL
C:\Python27\api-ms-win-core-fibers-l1-1-1.DLL
C:\Python27\Scripts\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\sysinternals\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\IDA_Pro_v6\python\api-ms-win-core-fibers-l1-1-1.DLL
C:\Users\user\AppData\Local\Temp\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\System32\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\system\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\api-ms-win-core-localization-l1-2-1.DLL
C:\ProgramData\Oracle\Java\javapath\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\System32\wbem\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-core-localization-l1-2-1.DLL
C:\Python27\api-ms-win-core-localization-l1-2-1.DLL
C:\Python27\Scripts\api-ms-win-core-localization-l1-2-1.DLL
C:\tools\sysinternals\api-ms-win-core-localization-l1-2-1.DLL
C:\tools\api-ms-win-core-localization-l1-2-1.DLL
C:\tools\IDA_Pro_v6\python\api-ms-win-core-localization-l1-2-1.DLL

\Device\KsecDD
C:\ProgramData\Comodo\CisDumps\
C:\ProgramData
C:\ProgramData\Comodo
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\SysWOW64\shell32.dll
C:\ProgramData\Comodo\CisDumps
C:\Users\user\AppData\Local\Temp\wrapped.sandboxed\
C:\Users\user\AppData\Local\Temp\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3.exe
C:\ProgramData\ComodoDome\cwsguard
C:\ProgramData\ComodoDome
C:\ProgramData\ComodoDome\cwsguard\GuardConfig.ini
C:\ProgramData\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\ProgramData\Microsoft\Network\Connections\Pbk*.pbk
C:\Windows\System32\ras*.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk*.pbk
C:\ProgramData\ComodoDome\cwsguard\cwsguard32.dll
C:\ProgramData\ComodoDome\cwsguard\cwsguard64.dll
C:\ProgramData\COMODOPSB\lib\wow64ext.dll
C:\ProgramData\COMODOPSB\lib
C:\ProgramData\COMODOPSB
C:\Windows\SysWOW64\kernel32.dll
C:\Windows\SysWOW64\KERNELBASE.dll
C:\Windows\SysWOW64\ntdll.dll
C:\Users\user\AppData\Local\Temp\wrapped.sandboxed\cis_temp_2511e80.exe
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\qagentrt.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\System32\en-US\dnsapi.DLL.mui
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates*
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
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\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_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoProxyDetectType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3_RASAPI32\FileDirectory
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3_RASMANCS\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3_RASMANCS\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3_RASMANCS\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3_RASMANCS\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3_RASMANCS\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3_RASMANCS\FileDirectory
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProgramData
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Hostname
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Domain
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{027947E1-D731-11CE-A357-000000000001}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{423EC01E-2E35-11D2-B604-00104B703EFD}\ProxyStubClsid32\(Default)

MODIFIED FILES

C:\ProgramData\COMODOPSB\lib\wow64ext.dll
C:\Users\user\AppData\Local\Temp\wrapped.sandboxed\cis_temp_2511e80.exe
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EA618097E393409AFA316F0F87E2C202_E950FDD8CC6997C1A810133CE1AFFEF3
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EA618097E393409AFA316F0F87E2C202_E950FDD8CC6997C1A810133CE1AFFEF3
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D84E548583BE1EE7DB5A935821009D26_5B98B6CD6E69202676965CF5B0E2A7A7
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\D84E548583BE1EE7DB5A935821009D26_5B98B6CD6E69202676965CF5B0E2A7A7

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsSetValue
kernel32.dll.FlsGetValue
kernel32.dll.LCMapStringEx
kernel32.dll.FlsFree
kernel32.dll.InitializeCriticalSectionEx

kernel32.dll.InitOnceExecuteOnce
kernel32.dll.CreateEventExW
kernel32.dll.CreateSemaphoreW
kernel32.dll.CreateSemaphoreExW
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.CreateSymbolicLinkW
kernel32.dll.GetTickCount64
kernel32.dll.GetFileInformationByHandleEx
kernel32.dll.SetFileInformationByHandle
kernel32.dll.InitializeConditionVariable
kernel32.dll.WakeConditionVariable
kernel32.dll.WakeAllConditionVariable
kernel32.dll.SleepConditionVariableCS
kernel32.dll.InitializeSRWLock
kernel32.dll.AcquireSRWLockExclusive
kernel32.dll.TryAcquireSRWLockExclusive
kernel32.dll.ReleaseSRWLockExclusive
kernel32.dll.SleepConditionVariableSRW
kernel32.dll.CreateThreadpoolWork
kernel32.dll.SubmitThreadpoolWork
kernel32.dll.CloseThreadpoolWork
kernel32.dll.CompareStringEx
kernel32.dll.GetLocaleInfoEx
ntdll.dll.RtlGetVersion
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook

user32.dll.IsProcessDPIAware
ole32.dll.CoTaskMemAlloc
ole32.dll.CoTaskMemFree
ole32.dll.CoInitializeEx
ole32.dll.CreateBindCtx
ole32.dll.CoGetApartmentType
ole32.dll.CoRegisterInitializeSpy
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
comctl32.dll.#236
oleaut32.dll.#6
ole32.dll.CoGetMalloc
comctl32.dll.#320
comctl32.dll.#324
comctl32.dll.#323
advapi32.dll.RegEnumKeyW
oleaut32.dll.#2
ole32.dll.CoUninitialize
rasapi32.dll.RasConnectionNotificationW
sechost.dll.NotifyServiceStatusChangeA
advapi32.dll.RegDeleteTreeA
advapi32.dll.RegDeleteTreeW
ole32.dll.CoCreateInstance
oleaut32.dll.#8
oleaut32.dll.#9
oleaut32.dll.DllGetClassObject
oleaut32.dll.DllCanUnloadNow
advapi32.dll.RegOpenKeyW
ole32.dll.StringFromIID
iphlpapi.dll.GetAdaptersAddresses
dhcpcsvc.dll.DhcpRequestParams
oleaut32.dll.#500
kernel32.dll.GetThreadPreferredUILanguages
kernel32.dll.SetThreadPreferredUILanguages

kernel32.dll.LocaleNameToLCID

DELETED FILES

C:\Users\user\AppData\Local\Temp\wrapped.sandboxed\cis_temp_2511e80.exe

C:\Users\user\AppData\LocalLow\VTRoot

REGISTRY KEYS

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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\App Paths\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3.exe

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\App Paths\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3.exe

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\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3.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_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_CURRENT_USER\Software\Classes
HKEY_CURRENT_USER\Software\Classes\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\TreatAs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\ThreadingModel

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocHandler32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocHandler
HKEY_LOCAL_MACHINE\Software\Microsoft\OleAut
HKEY_CURRENT_USER\Software\Classes\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Internet Settings\Wpad
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime

READ FILES

\Device\KsecDD
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\SysWOW64\shell32.dll
C:\Users\user\AppData\Local\Temp\80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3.exe
C:\ProgramData\ComodoDome\cwsguard\GuardConfig.ini
C:\Windows\SysWOW64\kernel32.dll
C:\Windows\SysWOW64\KERNELBASE.dll
C:\Windows\SysWOW64\ntdll.dll
C:\Users\user\AppData\Local\Temp\wrapped.sandboxed\cis_temp_2511e80.exe
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\en-US\dnsapi.DLL.mui
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\BAED8A8C5A147CFA78E686BB4A8E5829C2F934F5
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\C8A51E044BF5AF39158BB24E414E8FDCD2891C3A
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\FB45378AB288E369B22C860D123A809F530D5CC1
C:\Windows\System32\en-US\WINHTTP.dll.mui
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EA618097E393409AFA316F0F87E2C202_E950FDD8CC6997C1A810133CE1AFFEF3
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EA618097E393409AFA316F0F87E2C202_E950FDD8CC6997C1A810133CE1AFFEF3
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D84E548583BE1EE7DB5A935821009D26_5B98B6CD6E69202676965CF5B0E2A7A7
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\D84E548583BE1EE7DB5A935821009D26_5B98B6CD6E69202676965CF5B0E2A7A7
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.ver0x000000000000004a.db
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\LocalLow
C:\ProgramData\ComodoDome\recognizers\proto_v9\cmdscope.xml
C:\Users\user\AppData\Local\Temp\cfpver.dat

MUTEXES

DBWinMutex
IESQMMUTEX_0_208
mchMixCache$744

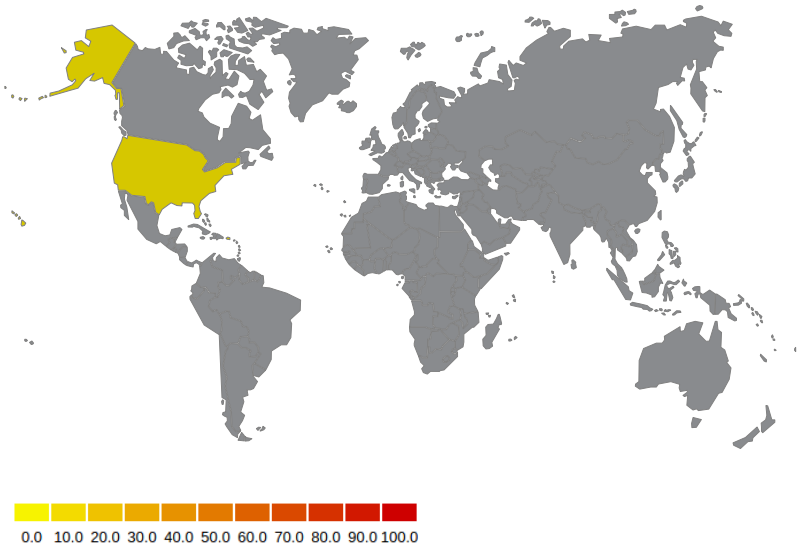
Mutex, mAH, Process $00000744, API $76fa103d
Mutex, mAH, Process $00000744, API $71ac0000
StartCleanUpVtRoot

MODIFIED REGISTRY KEYS

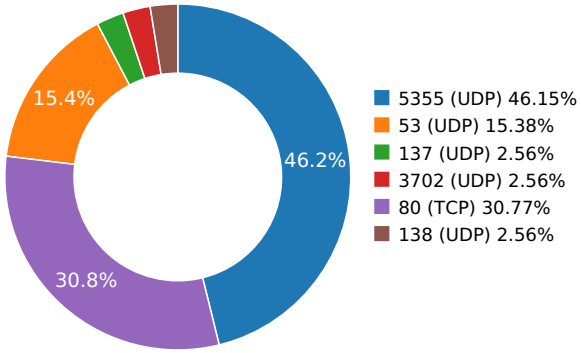
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	209.66.87.17	United States	6461	Zayo Bandwidth	OS Process
	23.35.171.27	United States	20940	Akamai Technologies, Inc.	Malware Process
	38.69.238.114	United States	174	PSINet, Inc.	OS Process
	104.28.16.56		13335	Cloudflare, Inc.	Malware Process
	104.91.166.216		20940	Akamai Technologies, Inc.	OS Process
	38.69.238.122		174	PSINet, Inc.	OS Process
	23.54.187.27		7843	Akamai Technologies, Inc.	Malware Process
	23.4.59.27		2914	Akamai Technologies, Inc.	Malware Process
	52.206.74.74		14618	Amazon Technologies Inc.	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	35.1765809059
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?4070b252bad529b2 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?4070b252bad529b2						
sv.symcd.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	40.6297719479
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQe6LNDJdqx%2BJOp7hVgTeaGFJ%2FCQgQUljtT8Hkzl699g%2B8uK8zKt4YecmYCEBxoP3uP%2B82s4ZJ9WI1JBs8%3D **URI:** http://sv.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQe6LNDJdqx%2BJOp7hVgTeaGFJ%2FCQgQUljtT8Hkzl699g%2B8uK8zKt4YecmYCEBxoP3uP%2B82s4ZJ9WI1JBs8%3D						
ts-ocsp.ws.symantec.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	45.9178678989
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBRi82PVYYKWGJWdgVNyePy5kYTdqQQUX5r1blzMzHSa1N197z%2Fb7EyALt0CEA7P9DjI%2Fr81bgTYapgbGlA%3D **URI:** http://ts-ocsp.ws.symantec.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRi82PVYYKWGJWdgVNyePy5kYTdqQQUX5r1blzMzHSa1N197z%2Fb7EyALt0CEA7P9DjI%2Fr81bgTYapgbGlA%3D						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	76.0003969669
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	81.1426169872
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	86.2987699509
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	91.4843039513
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
ec2-52-206-74-74.compute-1.amazonaws.com	A
Answers - 52.206.74.74 (A)	
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 38.69.238.122 (A) - a1621.g.akamai.net (CNAME) - 38.69.238.114 (A) - ctldl.windowsupdate.com.edgesuite.net (CNAME)	
sv.symcd.com	A
Answers - ocsp-ds.ws.symantec.com.edgekey.net (CNAME) - e8218.dscb1.akamaiedge.net (CNAME) - 23.35.171.27 (A)	
ts-ocsp.ws.symantec.com	A
Answers - 23.54.187.27 (A)	
crl.microsoft.com	A
Answers - 209.66.87.17 (A) - 209.66.87.25 (A) - crl.www.ms.akadns.net (CNAME) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 104.28.16.56 (A) - 104.28.17.56 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
35.1765809059	Sandbox	38.69.238.114	80
40.6297719479	Sandbox	23.35.171.27	80
45.9178678989	Sandbox	23.54.187.27	80
76.0003969669	Sandbox	209.66.87.17	80
91.4843039513	Sandbox	104.28.16.56	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.80230689049	Sandbox	192.168.56.255	137
6.84581589699	Sandbox	224.0.0.252	5355
6.8585498333	Sandbox	224.0.0.252	5355
6.86439299583	Sandbox	239.255.255.250	3702
7.80747485161	Sandbox	8.8.4.4	53
7.86062979698	Sandbox	224.0.0.252	5355
9.40842795372	Sandbox	224.0.0.252	5355
12.8451898098	Sandbox	192.168.56.255	138
29.9010338783	Sandbox	224.0.0.252	5355
32.4834728241	Sandbox	224.0.0.252	5355
35.0344338417	Sandbox	8.8.4.4	53
35.415792942	Sandbox	224.0.0.252	5355
37.9850637913	Sandbox	224.0.0.252	5355
40.5493218899	Sandbox	8.8.4.4	53
40.7219879627	Sandbox	224.0.0.252	5355
43.291634798	Sandbox	224.0.0.252	5355
45.8453369141	Sandbox	8.8.4.4	53
70.8367419243	Sandbox	224.0.0.252	5355
73.4192769527	Sandbox	224.0.0.252	5355
75.9710757732	Sandbox	8.8.4.4	53
76.02815485	Sandbox	224.0.0.252	5355
78.5850617886	Sandbox	224.0.0.252	5355
81.1737289429	Sandbox	224.0.0.252	5355
83.744260788	Sandbox	224.0.0.252	5355
86.3272819519	Sandbox	224.0.0.252	5355
88.8844349384	Sandbox	224.0.0.252	5355
91.4397988319	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EA618097E393409AFA316F0F87E2C202_E950FDD8CC6997C1A810133CE1AFFEF3	**Type :** data **MD5 :** 2448682b25fe60c396495da2f1574418 **SHA-1 :** 2bf302bf1f3029d99dcdba7f899bee0b255b39ea **SHA-256 :** 1e8933f40cfdcdb6c0511275919a90502600f3a4f **SHA-512 :** 35d1ec06a2a5d0b06222227c0f92a84ead6ebfb6 **Size :** 1.61 Kilobytes.
C:\ProgramData\COMODOPSB\Lib\Wow64ext.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 1d8d7898650685f96c2d4cac5434e1a8 **SHA-1 :** f726f4164436cdf0b2b908b78796483aba295c64 **SHA-256 :** 6a9edfab293a4390849f011e96ec8db02d6eabe8 **SHA-512 :** 48b953bfc23400f4121527551184f02a3d7d253d **Size :** 9.216 Kilobytes.
C:\Users\User\AppData\Local\Temp\Wrapped.Sandboxed\Cis_temp_2511e80.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** d0ee527b5c2669df35c509639a3a45ae **SHA-1 :** 873a8ec3f7a38b2397bfefb3066b0a2b37caeee9 **SHA-256 :** 391dad2a7b3247437d639df7064d93e963f929b4 **SHA-512 :** b4357ebf259725c196fb13c076356af0d49ad2e6a **Size :** 300.984 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\D84E548583BE1EE7DB5A935821009D26_5B98B6CD6E69202676965CF5B0E2A7A7	**Type :** data **MD5 :** 7c89102b7799dbd11341996e51f22536 **SHA-1 :** 2432a0d55fcca5e77d94bfc2122d751b507f9a72 **SHA-256 :** ce040a1fd05cd0f272ae6120048412bbb4055236 **SHA-512 :** ae9a468df7839723041d0167b6150344c60b516(**Size :** 1.469 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6564 bytes, 1 file **MD5 :** 16e8e953c65d610c3bfc595240f3f5b7 **SHA-1 :** 231a802e6ff1fae42f2b12561fff2767d473210b **SHA-256 :** 048846ed8ed185a26394adeb3f63274d1029bbd **SHA-512 :** 8cf223f68cd118be6bef746d4ccef2bc293e7e0f44 **Size :** 6.564 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EA618097E393409AFA316F0F87E2C202_E950FDD8CC6997C1A810133CE1AFFEF3	**Type :** data **MD5 :** 94a697c80122ef6fc18f74c4e697996e **SHA-1 :** 1d76f3e77f832b162c4ff72894d47b7dfe01c3f3 **SHA-256 :** d5e9488a7c2efe50107349928a56c53f79df3542(**SHA-512 :** cf1ca35a4e71c89b4ca37dd1038c6183498b1880 **Size :** 0.402 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D84E548583BE1EE7DB5A935821009D26_5B98B6CD6E69202676965CF5B0E2A7A7	**Type :** data **MD5 :** a1fc6515961ee758188aefd46954f6a8 **SHA-1 :** fa4388dce42038f8b40a84b2c328479c74d22900 **SHA-256 :** 1539276838fe642baf4c6875de45d9d113ed1b6(**SHA-512 :** c9a53392d6e67906985a7aaa4374bfc878dd3744 **Size :** 0.416 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** ccfa20b483c5541f1da2027368e4cdbc **SHA-1 :** fe356f293dffe1d6da08328f9d6058eb0d070891 **SHA-256 :** 6b42e24550dacafcfd8699dcd388342c07361f327 **SHA-512 :** 1bd46a3bc71b30895929de4caa63886c05c0f863 **Size :** 0.34 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	GoToWebinar_Opener.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3
MD5:	6948c07a98c64a5ea68dab822e4fb6ab
First Seen Date:	2018-02-23 18:07:42.418650 (11 months ago)
Number Of Clients Seen:	4
Last Analysis Date:	2018-02-23 18:07:42.418650 (11 months ago)
Human Expert Analysis Date:	2018-02-23 19:55:28.130883 (11 months 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	[{u'Path': u'D:\\Haibo\\COMODOCloudAntivirus\\PortableSandbox\\guard\\Release\\x32\\Symbols\\cwsLauncher.pdb\x00', u'GUID': u'{bbe5a357-b1e9-46ff-a27a-f5e3de6f409c}', u'timestamp': u'2017-09-13 01:36:35'}]
Number Of Sections	7
Trid	[[52.9, u'Windows ActiveX control'], [18.8, u'Win32 EXE PECompact compressed (generic)'], [12.2, u'UPX compressed Win32 Executable'], [12.0, u"Win32 EXE Yoda's Crypter"], [2.0, u'Win32 Executable (generic)']]
Compilation Time Stamp	0x59B88BA3 [Wed Sep 13 01:36:35 2017 UTC]
LegalCopyright	Copyright \xa9 2012-2017 LogMeIn, Inc.
InternalName	GoToOpener
FileVersion	1.0.0.473
CompanyName	LogMeIn, Inc.
ProductName	GoTo Opener
ProductVersion	1.0.0.473
FileDescription	GoTo Opener
OriginalFilename	GoToOpener.exe
Translation	0x0409 0x04e4
Entry Point	0x495fe2 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	2166664
Ssdeep	49152:HJaY/26sKgD/+fCbWQh6WTPZ+CFtNw5KBc838WFNXJssnsDEkNk8w5M0:HJP/2AO/b/WKBcXVV8M0
Sha256	f01372c75b0aa24f9ab961b64403cda9b69e40a660ca7a052e21350d43f5b95a
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/8/0/d/1/80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3', u'EXE:OriginalFileName': u'GoToOpener.exe', u'EXE:ProductName': u'GoTo Opener', u'EXE:InternalName': u'GoToOpener', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:02:23 18:07:04+00:00', u'EXE:InitializedDataSize': 623104, u'File:FileModifyDate': u'2018:02:23 16:53:12+00:00', u'EXE:FileVersionNumber': u'1.0.0.473', u'EXE:FileVersion': u'1.0.0.473', u'File:FileSize': u'2.1 MB', u'EXE:CharacterSet': u'Windows, Latin1', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Windows NT 32-bit', u'EXE:ProductVersion': u'1.0.0.473', u'EXE:ObjectFileType': u'Dynamic link library', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'LogMeIn, Inc.', u'File:FileName': u'80d11333708f5ef3fbdabac6ae7bef3cdbcb37f3', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.1, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2017:09:13 01:36:35+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright \xa9 2012-2017 LogMeIn, Inc.', u'EXE:LinkerVersion': 14.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/8/0/d/1', u'EXE:FileDescription': u'GoTo Opener', u'EXE:EntryPoint': u'0x95fe2', u'EXE:SubsystemVersion': 5.1, u'EXE:CodeSize': 1209856, u'File:FileInodeChangeDate': u'2018:02:23 16:53:12+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.0.0.473'}]
Mime Type	application/x-dosexec
Imphash	4b875ab535b4029e573a29899b193291

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1275b9	0x127600	6.67619427067	49161b38d3aa03bae7ec4a0f84b06340
.rdata	0x129000	0x59936	0x59a00	4.81738869006	0f05c9e23d654791fa12129dec84be9b
.data	0x183000	0x13dd4	0xc000	6.33651753179	d4da40405b6715272cec3039568f422b
.gfids	0x197000	0xbe8	0xc00	3.95166640902	c9a4eeab02b94b530ecb7bce5e6c8cf0
.tls	0x198000	0x9	0x200	0.0203931352361	1f354d76203061bfdd5a53dae48d5435
.rsrc	0x199000	0x26f9a	0x27000	6.79273724603	faf9226682327865e8c9c8e677976684
.reloc	0x1c0000	0x12208	0x12400	6.60237683542	aa052a68948314abbbed5b6a43990b8e

PE Imports

- ntdll.dll
  - NtQueryVirtualMemory
  - isdigit
  - NtOpenSymbolicLinkObject
  - RtlAppendUnicodeToString
  - RtlCopyUnicodeString
  - _wcsnicmp
  - NtClose
  - NtCreateFile
  - NtQueryObject
  - wcspbrk
  - _itow
  - strchr
  - strncmp
  - _aullshr
  - _allshl
  - _alldvrm
  - _aullrem
  - wcsncpy
  - wcschr
  - isspace
  - wcstoul
  - RtlUnwind
  - toupper
  - tolower
  - strrchr
  - wcsncmp
  - memcmp
  - NtCreateKey
  - _wtoi
  - atoi
  - wcstol
  - _wcsicmp
  - _chkstk
  - _alldiv
  - strncpy
  - wcsstr
  - _stricmp
  - memset
  - ZwCreatePort
  - ZwAcceptConnectPort
  - ZwCompleteConnectPort
  - wcsrchr
  - memmove
  - ZwReplyWaitReceivePortEx
  - memcpy
- KERNEL32.dll
  - CreateFileMappingW
  - GetModuleHandleA
  - GetCurrentThreadId
  - SetEvent
  - ResetEvent
  - ReleaseMutex
  - WaitForMultipleObjects
  - CreateMutexW

- CreateEventW
- DecodePointer
- FreeResource
- LockResource
- FreeLibrary
- LocalAlloc
- LocalFree
- InitializeCriticalSectionAndSpinCount
- LoadResource
- SizeofResource
- LoadLibraryW
- FindResourceW
- FindResourceExW
- MultiByteToWideChar
- WideCharToMultiByte
- LocalFileTimeToFileTime
- lstrlenW
- OutputDebugStringA
- GetComputerNameA
- WriteFile
- GetTickCount
- CreateFileW
- GetSystemDirectoryW
- HeapCreate
- GetFileSize
- ReadFile
- SetFilePointer
- VirtualAlloc
- VirtualFree
- SuspendThread
- OpenMutexW
- OpenEventW
- GetModuleFileNameA
- GetModuleFileNameW
- GetTempPathW
- DeleteFileW
- MoveFileExW
- OpenProcess
- GetCurrentProcessId
- SetEndOfFile
- SetFileAttributesW
- MoveFileW
- GetVersionExW
- FlushInstructionCache
- ExitProcess
- DuplicateHandle
- GetEnvironmentVariableW
- GetDriveTypeW
- GetVolumeInformationW
- CreateToolhelp32Snapshot
- Process32FirstW
- Process32NextW
- ExitThread
- GetLocalTime
- MapViewOfFile
- OpenFileMappingW
- GetPrivateProfileStringW
- WritePrivateProfileStringW
- CreateDirectoryW
- CopyFileW
- LoadLibraryExW
- EnumResourceNamesW
- GlobalAlloc
- GlobalLock
- GlobalUnlock
- GlobalFree
- FormatMessageA
- LoadLibraryA
- ReleaseSemaphore
- CreateSemaphoreW
- FindClose
- FindFirstFileW
- FindNextFileW
- RemoveDirectoryW
- GetSystemTimeAsFileTime

- GetFileInformationByHandle
- GetFileTime
- InterlockedCompareExchange
- InterlockedExchangeAdd
- ExpandEnvironmentStringsW
- SearchPathW
- SetCriticalSectionSpinCount
- FileTimeToSystemTime
- MapViewOfFileEx
- UnmapViewOfFile
- CreateMutexA
- CreateEventA
- GetCurrentDirectoryW
- GetTempFileNameW
- VerSetConditionMask
- VerifyVersionInfoW
- QueryDosDeviceW
- CreateWaitableTimerW
- SetWaitableTimer
- GetSystemWindowsDirectoryW
- InterlockedIncrement
- DeleteCriticalSection
- GetCurrentThread
- SetLastError
- VirtualProtectEx
- VirtualQueryEx
- ReadProcessMemory
- lstrcpyW
- CreateProcessA
- CreateFileMappingA
- GetVersion
- GetWindowsDirectoryW
- lstrcpyA
- lstrcatA
- lstrlenA
- VirtualQuery
- TlsAlloc
- TlsGetValue
- TlsSetValue
- TlsFree
- VirtualProtect
- VirtualFreeEx
- DeviceIoControl
- GetThreadContext
- IsDebuggerPresent
- FreeEnvironmentStringsW
- GetOEMCP
- IsValidCodePage
- FindFirstFileExW
- FlushFileBuffers
- GetConsoleCP
- SetFilePointerEx
- ReadConsoleW
- GetConsoleMode
- EnumSystemLocalesW
- GetUserDefaultLCID
- IsValidLocale
- GetACP
- GetFileAttributesExW
- WriteConsoleW
- GetFileType
- GetStdHandle
- GetModuleHandleExW
- GetCommandLineW
- GetCommandLineA
- CreateTimerQueue
- UnregisterWaitEx
- QueryDepthSList
- InterlockedFlushSList
- InterlockedPushEntrySList
- InterlockedPopEntrySList
- FreeLibraryAndExitThread
- GetThreadTimes
- UnregisterWait
- RegisterWaitForSingleObject

    - SetThreadAffinityMask
    - GetProcessAffinityMask
    - GetNumaHighestNodeNumber
    - DeleteTimerQueueTimer
    - ChangeTimerQueueTimer
    - CreateTimerQueueTimer
    - GetLogicalProcessorInformation
    - GetThreadPriority
    - SetThreadPriority
    - GetExitCodeThread
    - CreateRemoteThread
    - RaiseException
    - GetEnvironmentStringsW
    - TerminateProcess
    - GetCurrentProcess
    - GetProcessHeap
    - HeapSize
    - HeapFree
    - HeapReAlloc
    - HeapAlloc
    - HeapDestroy
    - VirtualAllocEx
    - GetProcAddress
    - SwitchToThread
    - SignalObjectAndWait
    - InitializeSListHead
    - GetStartupInfoW
    - IsProcessorFeaturePresent
    - SetUnhandledExceptionFilter
    - UnhandledExceptionFilter
    - WaitForSingleObjectEx
    - GetCPInfo
    - GetStringTypeW
    - GetLocaleInfoW
    - LCMapStringW
    - EncodePointer
    - QueryPerformanceCounter
    - TryEnterCriticalSection
    - GetFileAttributesW
    - OutputDebugStringW
    - CreateProcessW
    - GetModuleHandleW
    - LeaveCriticalSection
    - EnterCriticalSection
    - InitializeCriticalSection
    - GetSystemInfo
    - CloseHandle
    - Sleep
    - WaitForSingleObject
    - ResumeThread
    - WriteProcessMemory
    - TerminateThread
    - CreateThread
    - InterlockedDecrement
    - SetStdHandle
    - SetFileTime
    - GetLastError
- USER32.dll
    - DefWindowProcW
    - PostQuitMessage
    - RegisterClassExW
    - CreateWindowExW
    - IsWindow
    - DestroyWindow
    - ShowWindow
    - MoveWindow
    - SetTimer
    - KillTimer
    - UpdateWindow
    - GetDC
    - BeginPaint
    - EndPaint
    - GetWindowRect
    - GetWindowLongW
    - SetWindowLongW

    - LoadCursorW
    - SystemParametersInfoW
    - PostMessageW
    - GetSysColor
    - DestroyIcon
    - LoadImageW
    - FindWindowW
    - SendMessageTimeoutW
    - RegisterWindowMessageW
    - OpenInputDesktop
    - CloseDesktop
    - GetThreadDesktop
    - GetUserObjectInformationA
    - SendMessageW
    - SetForegroundWindow
    - TranslateMessage
    - GetMessageW
    - wsprintfW
    - GetSystemMetrics
    - DispatchMessageW
- ADVAPI32.dll
    - DeleteService
    - CreateServiceW
    - ControlService
    - RegEnumKeyW
    - GetKernelObjectSecurity
    - OpenThreadToken
    - DuplicateTokenEx
    - InitializeSid
    - AdjustTokenPrivileges
    - LookupPrivilegeValueW
    - RevertToSelf
    - ImpersonateLoggedOnUser
    - GetTokenInformation
    - RegEnumValueW
    - RegQueryInfoKeyW
    - RegDeleteKeyW
    - AddAccessAllowedAceEx
    - InitializeAcl
    - GetLengthSid
    - OpenProcessToken
    - RegSetValueExW
    - RegOpenKeyW
    - RegDeleteValueW
    - RegCreateKeyExW
    - CheckTokenMembership
    - StartServiceW
    - QueryServiceStatus
    - QueryServiceConfigW
    - OpenServiceW
    - OpenSCManagerW
    - CloseServiceHandle
    - ChangeServiceConfigW
    - RegQueryValueExW
    - RegOpenKeyExW
    - RegCloseKey
    - SetSecurityDescriptorDacl
    - InitializeSecurityDescriptor
    - FreeSid
    - AllocateAndInitializeSid
- ole32.dll
    - GetHGlobalFromStream
    - StringFromGUID2
    - StringFromCLSID
    - CLSIDFromProgID
    - CLSIDFromString
    - CoInitializeEx
    - CoTaskMemAlloc
    - CoFreeUnusedLibrariesEx
    - CreateStreamOnHGlobal
    - CoTaskMemFree
    - CoCreateInstance
    - CoSetProxyBlanket
    - CoInitializeSecurity
    - CoUninitialize

    - CoInitialize
- SHELL32.dll
    - SHCreateDirectoryExW
    - None
    - SHGetFolderPathW
    - SHGetSpecialFolderPathW
    - SHFileOperationW
    - ShellExecuteW
- OLEAUT32.dll
    - SysFreeString
    - VariantInit
    - VariantClear
    - SysAllocStringLen
    - SysAllocStringByteLen
    - SysStringByteLen
    - VariantChangeType
    - SysStringLen
    - SysAllocString
- SHLWAPI.dll
    - PathRemoveExtensionW
    - SHCreateStreamOnFileEx
    - PathIsNetworkPathW
    - PathAddBackslashW
    - PathRemoveBackslashW
    - UrlUnescapeW
    - PathFileExistsW
    - PathFindExtensionW
    - PathFindFileNameW
    - SHDeleteKeyW
    - PathAppendW
    - PathIsFileSpecW
    - PathCombineW
    - PathStripPathW
    - PathRemoveFileSpecW
    - PathStripToRootW
- gdiplus.dll
    - GdipCreateBitmapFromHICON
    - GdipFree
    - GdiplusStartup
    - GdiplusShutdown
    - GdipCloneBrush
    - GdipDeleteBrush
    - GdipCreateSolidFill
    - GdipCreatePen1
    - GdipDeletePen
    - GdipGetImageWidth
    - GdipGetImageHeight
    - GdipCreateFromHDC
    - GdipDeleteGraphics
    - GdipSetSmoothingMode
    - GdipDrawLines
    - GdipFillRectangle
    - GdipFillRectangleI
    - GdipDrawImageRect
    - GdipCreateFontFamilyFromName
    - GdipDeleteFontFamily
    - GdipGetGenericFontFamilySansSerif
    - GdipCreateFont
    - GdipDeleteFont
    - GdipDrawString
    - GdipCreateStringFormat
    - GdipDeleteStringFormat
    - GdipSetStringFormatAlign
    - GdipSetStringFormatLineAlign
    - GdipSetStringFormatTrimming
    - GdipCloneImage
    - GdipDisposeImage
    - GdipLoadImageFromStream
    - GdipLoadImageFromStreamICM
    - GdipGetImageThumbnail
    - GdipAlloc
- WININET.dll
    - HttpSendRequestW
    - HttpQueryInfoW
    - InternetReadFile

    - InternetQueryOptionW
    - InternetGetLastResponseInfoW
    - HttpSendRequestA
    - HttpOpenRequestW
    - InternetCloseHandle
    - InternetOpenW
    - InternetOpenA
    - InternetCanonicalizeUrlW
    - InternetCrackUrlW
    - InternetSetOptionW
    - InternetConnectW
- WTSAPI32.dll
    - WTSOpenServerW
    - WTSCloseServer
    - WTSEnumerateSessionsW
    - WTSQuerySessionInformationA
    - WTSFreeMemory
    - WTSQueryUserToken
- IPHLPAPI.DLL
    - GetAdaptersInfo
    - GetIfEntry
    - GetNetworkParams
- imagehlp.dll
    - ImageGetCertificateHeader
    - ImageGetCertificateData
- CRYPT32.dll
    - CryptVerifyMessageSignature
    - CertGetNameStringW
    - CertFreeCertificateContext
- WINTRUST.dll
    - WTHelperGetProvCertFromChain
    - WTHelperGetProvSignerFromChain
    - WTHelperProvDataFromStateData
    - WinVerifyTrust
- USERENV.dll
    - DestroyEnvironmentBlock
    - CreateEnvironmentBlock
- GDI32.dll
    - DeleteObject
- WS2_32.dll
    - socket
    - WSAEventSelect
    - WSAEnumNetworkEvents
    - WSAIoctl
    - recvfrom
    - getsockopt
    - sendto
    - ioctlsocket
    - __WSAFDIsSet
    - select
    - recv
    - htonl
    - inet_ntoa
    - closesocket
    - connect
    - htons
    - inet_addr
    - ntohl
    - send
    - setsockopt
    - gethostbyname
    - gethostname
    - getservbyname
    - WSAStartup
    - WSAGetLastError
    - WSACleanup
    - getprotobynumber
- WINMM.dll
    - timeGetTime
- VERSION.dll
    - GetFileVersionInfoW
    - VerQueryValueW
    - GetFileVersionInfoSizeW
- MPR.dll
    - WNetGetUniversalNameW

- XmlLite.dll
  - CreateXmlWriterOutputWithEncodingName
  - CreateXmlWriter
- COMDLG32.dll
  - GetOpenFileNameW
- PSAPI.DLL
  - GetMappedFileNameW

PE Exports

fvParseFullPathName
g_SandboxId

PE Resources

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 1679624, u'sha256': u'46146218e1ce4ae1cad015ace6bcdb788b89c503711dd63590e6682ea928084f', u'type': u'PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced', u'size': 4332}
{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 1683960, u'sha256': u'57ea7d50cdcda7e1331b78c839e95220c3b86c85434b93b747e9f5ac57527ea9', u'type': u'PNG image data, 13 x 13, 8-bit/color RGBA, non-interlaced', u'size': 3014}
{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 1686976, u'sha256': u'fe9d526fa11241a1db4565e2ab108bf119941493a2ed0acf81cc8e29c4d6dc90', u'type': u'PNG image data, 113 x 19, 8-bit/color RGBA, non-interlaced', u'size': 5137}
{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 1692120, u'sha256': u'a357e4485d539e182a87a928e5fe6f562d6ad82804375652e6ae4af7ed79c63f', u'type': u'PNG image data, 44 x 44, 8-bit/color RGBA, non-interlaced', u'size': 3604}
{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 1695728, u'sha256': u'fc4cce1e28d8c7d4162e380bb5654c5c78a24e715084d0659fc7229182332abb', u'type': u'PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced', u'size': 4490}
{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 1700224, u'sha256': u'747a8eaa62cdd62a7a84ffd955a34fced81147550a6b5d7e9317e0c52fd86b8a', u'type': u'PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced', u'size': 4400}
{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 1704624, u'sha256': u'1ffe11c728b14502eab303c475076549a815472281d0aa55b6a09689a6527241', u'type': u'PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced', u'size': 4281}
{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 1708912, u'sha256': u'85d1b3079025ee47c5e32e20a4cefa3ffeaefcdf4701bba38a1f9ab6ba051f07', u'type': u'PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced', u'size': 4267}
{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 1713184, u'sha256': u'8e1eb7d418fc601f322f65e60e3a348ae76c2bd0e5d68c035ac8f917dda116d5', u'type': u'PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced', u'size': 4517}
{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 1717704, u'sha256': u'a1d1d41eff0c4a3fe46a9069767ee0b06ae760ed51208a70a986459faba4ff9f', u'type': u'PNG image data, 8 x 2, 8-bit/color RGBA, non-interlaced', u'size': 2797}
{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 1720504, u'sha256': u'66df770bf5a8c738fc165c68bd691d31b87384f1b7b2c3797eda040a8e316d70', u'type': u'PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced', u'size': 4502}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1725008, u'sha256': u'fbeb3be87e80cb8e1d2af3d8140796c1bb80c6c7056f60897088ff9e355c3867', u'type': u'data', u'size': 308}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1725320, u'sha256': u'f64ccc0582bc7c66af8b40049e485e8e241335261ec95ace909293ba50b2e4a3', u'type': u'data', u'size': 180}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1725504, u'sha256': u'652988945185cf5d604d9b48de66288d82d8ed0acdd134398e90d002d2d9fc72', u'type': u'AmigaOS bitmap font', u'size': 308}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1725816, u'sha256': u'0b0e16c38a3d5a85566e67b1d9a7e720e4dee27e163b06099d3d7dfa5dbed9ee', u'type': u'data', u'size': 308}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1726128, u'sha256': u'368f9cb089d206a8b61251f0c85eeda97ee08a56b33be8579246e964d3af6169', u'type': u'data', u'size': 308}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1726440, u'sha256': u'6440c3a38dcfb81d45bc6be31b776fdae116dd7a2933b407b67132f6cfa0e6eb', u'type': u'data', u'size': 308}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1726752, u'sha256': u'9882a8462ce9de3cc9a5d0ca48c8c4f7ca97f1f846f0c10e6655e33c9734b152', u'type': u'data', u'size': 308}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1727064, u'sha256': u'322e92d75b3fec9e16b81466f4cf111d298b80812d5b238f4ee032c025a02050', u'type': u'data', u'size': 308}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1727376, u'sha256': u'8db6df648274a0fc3d28430367216e1c17c364ca613066cbb0e133637e92ba62', u'type': u'data', u'size': 308}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1727688, u'sha256': u'f9c81ce9b4176b305c554a15f0ca2b98b11be76c1f13ef22169999aa07e9612f', u'type': u'data', u'size': 308}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1728000, u'sha256': u'601635482a9b1864ea0c61ce0282c5c9fe1d014aa95dbb4f60770f1c2b6df3da', u'type': u'data', u'size': 308}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1728312, u'sha256':

u'2bf742d2beb4c56dd6eb68347dd8ee28da85bed9e6d165b36c6edb91da01d5d6', u'type': u'data', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1728624, u'sha256': u'cfc4ff9e46fbb61f61b68f36adc6593b137233d1cbaa50fe37e5653f0cb20396', u'type': u'AmigaOS bitmap font', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1728936, u'sha256': u'c4a6e3a7a346baecb09a0c49268eb44f388382a7866a4e912b53d48fa3b34c26', u'type': u'data', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1729248, u'sha256': u'f273e554605a89aa0994c9d42bc2569be3db5b19b2900dacb30f3218ed1174a0', u'type': u'data', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 1729560, u'sha256': u'ebaf4bcc0f0d7ca9a3458ea52520d2dd10811069241940b9b2e79ac1a4c3ca5c', u'type': u'data', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 1729872, u'sha256': u'e7c0005285d1ab59732d5f99f77a9bdd6342b01cf44437ebd7a07611a227e272', u'type': u'data', u'size': 184}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 1730056, u'sha256': u'abdf36bde89a26349f5741c17c235dacea88d441d8662ba16a598dc50c3c4864', u'type': u'data', u'size': 324}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 1730384, u'sha256': u'b4b2f722234d9e7f31ff4facd631adcc0482b81c4ad1eb1458fc822175277c21', u'type': u'data', u'size': 744}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 1731128, u'sha256': u'803572ed52c34a6b6c2efa70c0f7a5279e21bad55a4d5d18744b270937404fe2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 1731424, u'sha256': u'0a4938500c6f3d33430c7fed3c2271a78b34ee727a78475eb6d1a435f4a00bdb', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 1735176, u'sha256': u'2ae3c5d4d767d49adf27595ac6e6c282cba327b4cdb89f9dc2a735c314eb7d18', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 1737392, u'sha256': u'b1f2927559496473b1bd7ca8d8cb21b67e56eefa87fc06945eba67c71d268645', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 1738776, u'sha256': u'10f2dfcb31c0f0816447923633e79ef4ff7ca1bf89d5f6984e4cce62615ea729', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 9640}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 1748416, u'sha256': u'aec3c266b0f119a982069893611ffd2cdd271fdbcf915b17fdf9b00d445676c9', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 1752680, u'sha256': u'7ad7dd241cc84dad41c3f1ee55c9272bd835e6172e6144423af4be38ce3fe2a1', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1753808, u'sha256': u'1db292b8a589c9ad9b187bbc49e873100345b5547ee39508ba3a410ac68a06d7', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 1640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1755448, u'sha256': u'feaccf5b4849780a43c03f9004a3cdd46c99c2b4f85af24003514d28309e93f7', u'type': u'data', u'size': 744}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1756192, u'sha256': u'6b900485ef52ecbb4e29de3d42f9455cb70bc633ec8e7669ace6318cb2a0feb2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1756488, u'sha256': u'cea5e1c45eea1d3e5c06b07a313c011a428e8ce8e1e74686eafa370cc3a4a207', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1760240, u'sha256': u'499bf019d6c6d85672cf6dd4a93e202460125a4fcad47fdb2a1d2986f7b00f7b', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1762456, u'sha256': u'2ebc8da746fd3765dd10a82990cc58b20e19a61ca5927ac3d16f47f5306aa408', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1763840, u'sha256': u'512fb3be3926b37d0b45a89ea0e5632e5004c94150d92e613e142a1664ef35b6', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 36411}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1800256, u'sha256': u'402a302a3ac7b7b939331bfd6ae6c0ec9e61a835213d4de61fbd8cdb7d03612f', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1809896, u'sha256': u'c386c938ff8e0c0349696f63602f05028706a96a43ea5f8e880c6c1408d555b6', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1814160, u'sha256': u'f25c5b0ef9ca4c79124fdc9070eebf727d07992fd58a7f7010726028d298c89c', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 1815288, u'sha256': u'0a499d64718a0381a46280ddc2197bb340a07e95c55e3e1eed1ee472aa7fd7e6', u'type': u'data', u'size': 392}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 1815680, u'sha256': u'6e113fd8e9f3156ae68251c6076beb9b59fe29e589d06398e7019802521f69d3', u'type': u'data', u'size': 232}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 1815912, u'sha256': u'4cf716efaf68e0cb2ec45ec55d291050b5712b05653cae68edbb999f803d2a98', u'type': u'data', u'size': 52}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 1815968, u'sha256': u'd91dc4e26fd86def5ee907c72f32457bea07d21fa618012245f641d08501548d', u'type': u'data', u'size': 130}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 1816104, u'sha256': u'05e0d5787611ed4f643733e3e6e62d00f426422b5d3e443ceebac22e9d294bc4', u'type': u'data', u'size': 42}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 1816152, u'sha256': u'9665348f07508c6c2a568fc90ec4c04736668adc3521e311a4c7659973d92313', u'type': u'data', u'size': 388}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 1816544, u'sha256': u'fcb87f4b1b4178dae839137498027a0cfdf4247d1b49e741b5015313a2cd6a2d', u'type': u'data', u'size': 1262}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 1817808, u'sha256': u'eaa0b4fe4704e193dd2ed1f8de1cb20e1001034fdb30307ee44aa664966d4ffc', u'type': u'data', u'size': 612}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 1818424, u'sha256': u'cffcd4956911b3d50eef378cb051e598baba0db48246b07780af03b01c67c64d', u'type': u'data', u'size': 730}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 1819160, u'sha256': u'35b5abb90316b4017d5531e031cbf15bae6e8dd46f6dd221701693a22a7795be', u'type': u'data', u'size': 138}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 1819304, u'sha256': u'1b8660b0c53b94f3e029de58e56d08c8097a080244e9dc65d4155a9b603820d8', u'type': u'data', u'size': 172}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 1819480, u'sha256': u'31bff9afbf08a8869318cd946a1d73a4425afefc5693c6e06671bde1e86de1dc', u'type': u'data', u'size': 222}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 1819704, u'sha256': u'2b5551644093e58a4af74928fb744bd735fa2ef5f99824e6918ff9f6a33a3803', u'type': u'data', u'size': 1192}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 1820896, u'sha256': u'e9212b16f2d3292d0b0eb67134a70778ff1b0aede4918831e5bdba3f950db2a7', u'type': u'data', u'size': 552}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 1821448, u'sha256': u'0714c554acd308b38c3d6319f7e470f76a16d712f696545eacac2bdc725dfb95', u'type': u'data', u'size': 44}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 1821496, u'sha256': u'a5e23c6071b4faf115605493d1fd2e238c1d915b412f869aa6a7a77726f56082', u'type': u'data', u'size': 1342}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_RCDATA', u'offset': 1822840, u'sha256': u'01d4eb943f707b6a0d62ba9ea3ad58320f1ccd9dd0db66bc028859db0abbafc1', u'type': u'ASCII text', u'size': 778}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823624, u'sha256': u'04af5d91ca460ae8eb8f2a5149cb13d682f04e801101bfc367d015485dadf206', u'type': u'MS Windows cursor resource - 2 icons, 32x256, hotspot @1x1', u'size': 34}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823664, u'sha256': u'12a5b9052dd16bed260343bc4352d436167c991c54497c5af441304646549386', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823688, u'sha256': u'28b8110695851e5280ff55cb78507b03e8b74dd370b8e122179c82b56f7e5f37', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823712, u'sha256': u'4ecc7f2578fd7b137c04f85ffcbd67d6eab0bc8b1df4246cebd2a2aa517f3c60', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823736, u'sha256': u'ef309b720f166673cad840a88e7636e9161ad91415cc7c176010cebba07757e5', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823760, u'sha256': u'8f51832638675f16ec5f251ab59251b3f85d84e5129025d44c45b3191b331c58', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823784, u'sha256': u'a2f0549cca7170ae03ba042464efe62365fba38c20049e439871c9e5ce0f914f', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823808, u'sha256': u'da738753c27f2708bd2257f8cac3385a4ccb0df1341b76acfda07fa980cfb4bd', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823832, u'sha256': u'8a495f17bc472bfc5e6923d9efa687848fac027ad60694f9c3f10a4f7b194924', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823856, u'sha256': u'ee63d4681e7622067fd29005c6cc67b456031eb723c7239f05f1cb097af0ef98', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823880, u'sha256': u'3f02dcac38fffe306e1825846e2bc0458ee712696310d051e3a69ebda8330cc3', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823904, u'sha256': u'b328fe22a904a2e7e1341a95dbf00e2fdffc9ab350bc64c5ee348d3007c2b479', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823928, u'sha256': u'6c2ef97bca5cdc6aa6de65b1f1ae8328bcb3494a16025eee870231d991e2cd56', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823952, u'sha256': u'1085b7390dbd2b2006f85619521047c6ca58a8b274196eeed48e74ad8a1b746a', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 1823976, u'sha256': u'60a0a8bc0169228c8af42c377d93a218ccc9712a17b76ef014f81e156a36c66f', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 1824000, u'sha256': u'e596181dd132ce3d343c70f76e868e4a9dca9a69dd9e3265bf8cbe83d683f2ca', u'type': u'MS Windows icon resource - 10 icons, 48x48, 16 colors', u'size': 146}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_ICON', u'offset': 1824152, u'sha256': u'0f8e66b41e930335fa661b03299b12d6e7d8f04e7e35a117cb6966b9d1258497', u'type': u'MS Windows icon resource - 8 icons, 32x32, 16 colors', u'size': 118}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 1824272, u'sha256': u'840c802c2383fc3c87b005502685f5c534888547b8b690da6204ee6fd1f732fd', u'type': u'data', u'size': 748}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 1825024, u'sha256': u'6f35c0504f9088199d817f4ab0a630d5a3822d724a42b6968593b744a037ae86', u'type': u'XML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators', u'size': 663}

{u'lang': u'LANG_CHINESE', u'name': u'102', u'offset': 1825688, u'sha256': u'6a9edfab293a4390849f011e96ec8db02d6eabe867d4d079dff5b9d1006a735b', u'type': u'PE32 executable (DLL) (GUI) Intel 80386, for MS Windows', u'size': 9216}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS