VALKYRIE COMODO

Summary

File Name: PFXServer.exe

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

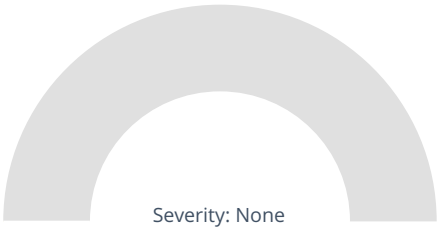
SHA1: 607a45a0d2ba7e53249570ec9b1acada710aafd9

MD5: b9456922590d0a1f3304d04502056e90

CLEAN

Valkyrie Final Verdict

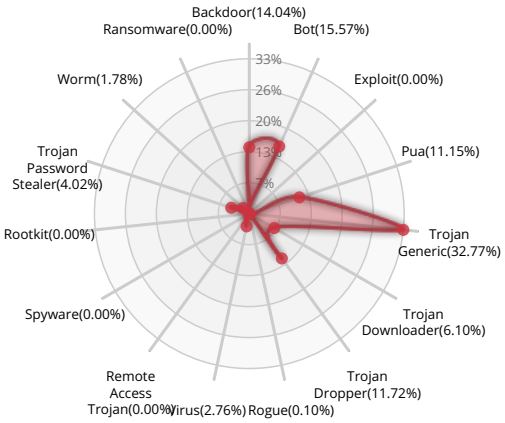
DETECTION SECTION



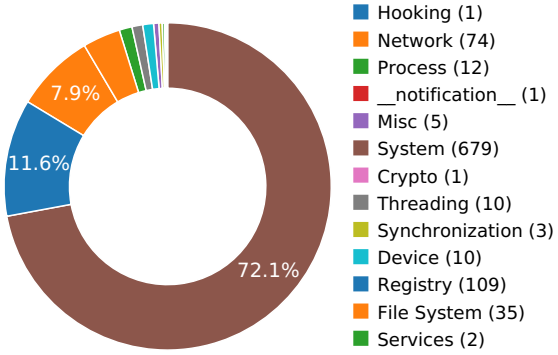
Severity: None

Verdict: Clean

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

NETWORKING

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

Performs some HTTP requests — Show sources

MALWARE ANALYSIS SYSTEM EVASION

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

Tries to unhook or modify Windows functions monitored by Cuckoo — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

VALKYRIE COMODO

Behavior Graph

Behavior Summary

ACCESSED FILES

\Device\KsecDD
C:\Windows\System32\tzres.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Program Files\Common Files\System\symsrv.dll
C:\Users\user\AppData\Local\Temp\A1D26E2
C:\Program Files\Common Files\System\symsrv.dll.dat
C:\Program Files\Common Files\System\symsrv.dll.000

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3\Com+Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
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 NT\CurrentVersion\Windows\AppInit_DLLs
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\AppCompat\RaiseDefaultAuthnLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\DefaultAccessPermission
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{00000134-0000-0000-C000-000000000046}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\NdrOleExtDLL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\RemoteRpcDll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\BD5F5ADB
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\MaxSxSHashCount

RESOLVED APIS

kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.FlsAlloc
kernel32.dll.FlsSetValue
kernel32.dll.FlsGetValue
kernel32.dll.LCMapStringEx
api-ms-win-core-synch-l1-2-0.dll.InitializeConditionVariable
api-ms-win-core-synch-l1-2-0.dll.SleepConditionVariableCS
api-ms-win-core-synch-l1-2-0.dll.WakeAllConditionVariable

cryptbase.dll.SystemFunction036
ole32.dll.CLSIDFromOle1Class
clbcatq.dll.GetCatalogObject
clbcatq.dll.GetCatalogObject2
kernel32.dll.OpenProcess
kernel32.dll.TerminateProcess
kernel32.dll.WriteProcessMemory
kernel32.dll.VirtualAllocEx
sechost.dll.LookupAccountNameLocalW
advapi32.dll.AdjustTokenPrivileges
user32.dll.MessageBoxTimeoutW
wintrust.dll.WinVerifyTrust
kernel32.dll.CreateProcessInternalW
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
ws2help.dll.WahReferenceContextByHandle
ntdll.dll.KiUserExceptionDispatcher
advapi32.dll.LookupAccountSidW
sechost.dll.LookupAccountSidLocalW
cryptsp.dll.CryptAcquireContextW
cryptsp.dll.CryptGenRandom
ole32.dll.NdrOleInitializeExtension
ole32.dll.CoGetClassObject
ole32.dll.CoGetMarshalSizeMax
ole32.dll.CoMarshalInterface
ole32.dll.CoUnmarshalInterface
ole32.dll.StringFromIID
ole32.dll.CoGetPSClsid
ole32.dll.CoTaskMemAlloc
ole32.dll.CoTaskMemFree
ole32.dll.CoCreateInstance
ole32.dll.CoReleaseMarshalData
ole32.dll.DcomChannelSetHResult
rpcrtremote.dll.I_RpcExtInitializeExtensionPoint
wininet.dll.InternetOpenA

wininet.dll.InternetOpenUrlA
rasapi32.dll.RasConnectionNotificationW
sechost.dll.NotifyServiceStatusChangeA
ole32.dll.CoInitializeEx
advapi32.dll.RegDeleteTreeA
advapi32.dll.RegDeleteTreeW
wininet.dll.InternetCloseHandle
wininet.dll.InternetReadFile
ws2_32.dll.connect
ole32.dll.CoUninitialize
oleaut32.dll.#500

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Classes
HKEY_LOCAL_MACHINE\Software\Microsoft\COM3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3\Com+Enabled
HKEY_CURRENT_USER\Software\Classes\CLSID\{E895F6DF-5FE2-4029-950F-359E556C1221}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
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 nt\currentversion\windows
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
HKEY_CURRENT_USER\Software\Classes\AppID\607a45a0d2ba7e53249570ec9b1acada710aafd9.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\OLE\AppCompat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\AppCompat\RaiseDefaultAuthnLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\DefaultAccessPermission
HKEY_CURRENT_USER\Software\Classes\Interface\{00000134-0000-0000-C000-000000000046}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{00000134-0000-0000-C000-000000000046}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{00000134-0000-0000-C000-000000000046}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Extensions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\NdrOleExtDLL

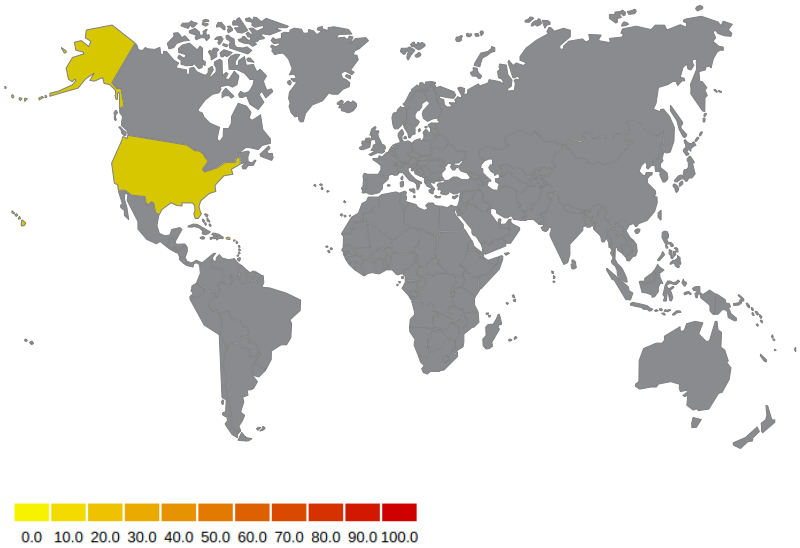
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\RemoteRpcDll
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BFE
HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows\DisabledProcesses\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\BD5F5ADB
HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows\DisabledSessions\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_LOCAL_MACHINE\Software\Microsoft\OLE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\MaxSxSHashCount
HKEY_CURRENT_USER\Software\Classes\CLSID\{9EF91B74-82BB-42B4-8C6A-4837200020B3}
HKEY_CURRENT_USER\Software\Classes\CLSID\{8C3EDBE5-AC14-4E5C-B10A-CA0764261365}
HKEY_CURRENT_USER\Software\Classes\CLSID\{142DE38F-16F5-4DE7-8D66-EEC56738446C}
HKEY_CURRENT_USER\Software\Classes\CLSID\{F6A711DA-46F1-4086-8DC2-9A2FD56A8E5E}
HKEY_CURRENT_USER\Software\Classes\CLSID\{2CD257FE-A9BA-4C39-9817-FD00B2FE4882}
HKEY_CURRENT_USER\Software\Classes\CLSID\{2B8BC88C-28AE-4D68-A583-A53677678741}
HKEY_CURRENT_USER\Software\Classes\CLSID\{AC1B4665-674E-4646-B42B-22713CB4D1F4}
HKEY_CURRENT_USER\Software\Classes\CLSID\{8A3FE424-D9E7-4D7E-A3F2-1CE0666FB589}
HKEY_CURRENT_USER\Software\Classes\CLSID\{4675F3AB-682A-4DCB-B448-BA5FF29FC5FA}
HKEY_CURRENT_USER\Software\Classes\CLSID\{B6B899EF-5338-44CE-9C05-41E61140C2E9}
HKEY_CURRENT_USER\Software\Classes\CLSID\{F3DB2FAC-AE70-49E9-A02A-FC9A7078DA97}
HKEY_CURRENT_USER\Software\Classes\CLSID\{EB357C55-ED0F-4F81-98A1-03C01251C1A7}
HKEY_CURRENT_USER\Software\Classes\CLSID\{B2412A08-204D-4AEE-9F30-D4D856497C6D}
HKEY_CURRENT_USER\Software\Classes\CLSID\{3CFE6C77-4C1C-4280-88DA-A5A843443B9C}
HKEY_CURRENT_USER\Software\Classes\CLSID\{6E8D13C2-83BD-489C-841C-C4FCA5700D24}

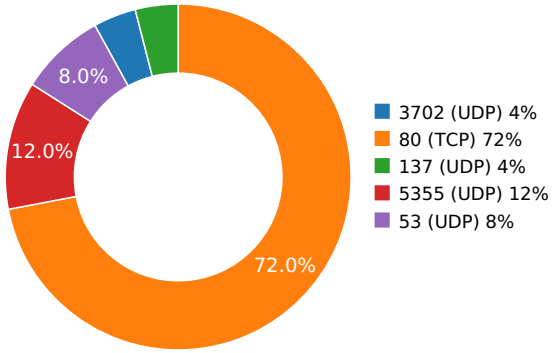
READ FILES

\Device\KsecDD
C:\Windows\System32\tzres.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Program Files\Common Files\System\symsrv.dll

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
	104.200.23.95		63949	Linode	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
www.aieov.com	80	GET	1.1		2	6.44032406807
Path: /setup.exe **URI:** http://www.aieov.com/setup.exe						
www.aieov.com	80	GET	1.1		12	10.6005051136
Path: /logo.gif **URI:** http://www.aieov.com/logo.gif						
www.aieov.com	80	GET	1.1		1	185.17839098
Path: /so.gif **URI:** http://www.aieov.com/so.gif						

DNS QUERIES

Request	Type
5isohu.com	A
www.aieov.com	A
Answers - 104.200.22.130 (A) - 104.200.23.95 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.44032406807	Sandbox	104.200.23.95	80
10.6005051136	Sandbox	104.200.23.95	80
11.7099149227	Sandbox	104.200.23.95	80
19.3966009617	Sandbox	104.200.23.95	80
20.490762949	Sandbox	104.200.23.95	80
28.1939520836	Sandbox	104.200.23.95	80
29.2714350224	Sandbox	104.200.23.95	80
36.9905850887	Sandbox	104.200.23.95	80
38.0526969433	Sandbox	104.200.23.95	80
45.78738904	Sandbox	104.200.23.95	80
46.8342180252	Sandbox	104.200.23.95	80
54.5842030048	Sandbox	104.200.23.95	80
55.6152219772	Sandbox	104.200.23.95	80
60.3967399597	Sandbox	104.200.23.95	80
185.17839098	Sandbox	104.200.23.95	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.03014206886	Sandbox	224.0.0.252	5355
3.07230901718	Sandbox	224.0.0.252	5355
3.10205197334	Sandbox	192.168.56.255	137
3.15815401077	Sandbox	239.255.255.250	3702
4.02451014519	Sandbox	8.8.4.4	53
5.62926912308	Sandbox	224.0.0.252	5355
6.3922970295	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Program Files\Common Files\System\Symsrv.Dll.000	**Type :** Non-ISO extended-ASCII text, with no line terminators **MD5 :** a33fe6ffe32a780b02447b9560b0c39a **SHA-1 :** a5ebc92cf88b7859034b2cdef1ec46ae92dbc71e **SHA-256 :** fb5e0064049ed6427348adbc1c4fe6c2fdeafe1fe(**SHA-512 :** 78a2f6e48f513c727810157721118c389870ae5al **Size :** 0.014 Kilobytes.

MATCH YARA RULES

MATCH RULES
anti_dbg
win_registry
win_files_operation

STATIC FILE INFO

File Name:	PFXServer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	607a45a0d2ba7e53249570ec9b1acada710aafd9
MD5:	b9456922590d0a1f3304d04502056e90
First Seen Date:	2018-10-12 19:00:26.198856 (8 months ago)
Number Of Clients Seen:	8
Last Analysis Date:	2019-05-29 19:21:13.339168 (about 14 hours ago)
Human Expert Analysis Date:	2018-10-12 22:58:08.075795 (8 months ago)
Human Expert Analysis Result:	Clean

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'C:\\Mainline\\Main\\Common\\Source\\ProductIntegration\\PSI\\Misc\\CCH.Pfx.PSI.ComServer\\Source\\PFXServer\\Rel u'GUID': u'{c003468c-1141-4589-8e7f-d81f067edade}', u'timestamp': u'2018-09-21 03:39:07'}]
Number Of Sections	4
Trid	[[64.6, u'Win64 Executable (generic)'], [15.4, u'Win32 Dynamic Link Library (generic)'], [10.5, u'Win32 Executable (generic)'] Executable'], [4.6, u'DOS Executable Generic']]
Compilation Time Stamp	0x5BA467DB [Fri Sep 21 03:39:07 2018 UTC]
LegalCopyright	CCH, A WoltersKluwer Business. All rights reserved.
InternalName	PFXServer.exe
FileVersion	1.0.20.1670
CompanyName	CCH, A WoltersKluwer Business
ProductName	NextGen
ProductVersion	1.0.0.1
FileDescription	CCH.Pfx.PSI.Tax
OriginalFilename	PFXServer.exe
Translation	0x0409 0x04e4
Entry Point	0x43ff8d (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	605184
Ssdeep	12288:4Da75Af0gmIsNRy91tC9xpXmYa7ctcCLgrh7g:JIs+4A7tC
Sha256	092e278082b4312e5a5f0d6c0652219a6e08a0b14489bb5ef3eea20c0970c0f1
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/6/0/7/a/607a45a0d2ba7e53249570ec9b1acada710aafd9', u'EXE:OriginalFileN u'EXE:ProductName': u'NextGen', u'EXE:InternalName': u'PFXServer.exe', u'File:MIMEType': u'application/octet-stream', u'F u'2019:05:29 19:20:58+00:00', u'EXE:InitializedDataSize': 258048, u'File:FileModifyDate': u'2019:05:29 19:20:58+00:00', u'EX u'1.0.20.1670', u'EXE:FileVersion': u'1.0.20.1670', u'File:FileSize': u'591 kB', u'EXE:CharacterSet': u'Windows, Latin1', u'EXE:M or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'1.0.0.1', u'EXE:ObjectFileType': u'Executable ap u'Win32 EXE', u'EXE:CompanyName': u'CCH, A WoltersKluwer Business', u'File:FileName': u'607a45a0d2ba7e53249570ec9 u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 6.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp' 03:39:07+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'CCH, A WoltersKluwer Business. All rights reserv 14.14, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valky u'EXE:FileDescription': u'CCH.Pfx.PSI.Tax', u'EXE:EntryPoint': u'0x3ff8d', u'EXE:SubsystemVersion': 6.0, u'EXE:CodeSize': 367 u'File:FileInodeChangeDate': u'2019:05:29 19:20:58+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.0.0.1'}]
Mime Type	application/x-dosexec
Imphash	9390d3daa350805ff51cd64eaaa9658a

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x598bc	0x59a00	6.47541984958	672beeecadd17ddcfa4a024c81ade4e6
.rdata	0x5b000	0x23176	0x23200	5.12788576561	da5fdc66e869f40f0e5961b423091ff6
.data	0x7f000	0xdeb4	0x8e00	5.26746387809	b091ff52712d0b2ad134fdb934783d68
.rsrc	0x8d000	0xdda8	0xde00	5.22427974778	9a2ab8c0274b112acd30c4431a077b9d

PE Imports

- RPCRT4.dll
  - UuidToStringA
- WTSAPI32.dll
  - WTSFreeMemory
  - WTSEnumerateProcessesA
- KERNEL32.dll
  - GetModuleFileNameA
  - GetModuleHandleA
  - GetProcAddress
  - LoadLibraryExA
  - LoadResource
  - SizeofResource
  - lstrcmpiA
  - FindResourceA
  - MultiByteToWideChar
  - WideCharToMultiByte
  - IsDBCSLeadByte
  - SetLastError
  - Sleep
  - GetCurrentThreadId
  - CloseHandle
  - HeapDestroy
  - HeapAlloc
  - HeapReAlloc
  - HeapFree
  - HeapSize
  - GetProcessHeap
  - InitializeCriticalSectionEx
  - CreateProcessA
  - FindResourceExW
  - LockResource
  - FindResourceW
  - LocalAlloc
  - LocalSize
  - LocalFree
  - FormatMessageA
  - lstrlenA
  - CreateFileA
  - SetFilePointer
  - WriteFile
  - InitializeCriticalSection
  - FreeLibrary
  - SetEvent
  - WaitForSingleObject
  - CreateEventA
  - LoadLibraryA
  - GetCommandLineA
  - CreateThread
  - GetModuleHandleW
  - CreateTimerQueueTimer
  - UnhandledExceptionFilter
  - SetFilePointerEx
  - GetConsoleMode
  - GetConsoleCP
  - FlushFileBuffers
  - GetStringTypeW
  - SetStdHandle
  - FreeEnvironmentStringsW
  - GetEnvironmentStringsW
  - GetCommandLineW
  - GetCPInfo

    - GetOEMCP
    - GetACP
    - IsValidCodePage
    - FindNextFileW
    - FindFirstFileExW
    - FindClose
    - GetFileType
    - SetUnhandledExceptionFilter
    - LCMapStringW
    - GetStdHandle
    - GetModuleFileNameW
    - DeleteCriticalSection
    - InitializeCriticalSectionAndSpinCount
    - LeaveCriticalSection
    - EnterCriticalSection
    - GetLastError
    - RaiseException
    - DecodePointer
    - CreateFileW
    - WriteConsoleW
    - GetLocalTime
    - ExitProcess
    - GetModuleHandleExW
    - FreeLibraryAndExitThread
    - CreateEventW
    - ExitThread
    - VirtualQuery
    - VirtualProtect
    - GetSystemInfo
    - LoadLibraryExW
    - TlsFree
    - TlsSetValue
    - TlsGetValue
    - TlsAlloc
    - RtlUnwind
    - GetSystemTimeAsFileTime
    - GetCurrentProcessId
    - QueryPerformanceCounter
    - WaitForSingleObjectEx
    - ResetEvent
    - VirtualFree
    - VirtualAlloc
    - IsProcessorFeaturePresent
    - FlushInstructionCache
    - GetCurrentProcess
    - InterlockedPushEntrySList
    - InterlockedPopEntrySList
    - InitializeSListHead
    - EncodePointer
    - OutputDebugStringW
    - IsDebuggerPresent
    - TerminateProcess
    - GetStartupInfoW
- USER32.dll
    - CharNextA
    - PostMessageA
    - DefWindowProcA
    - CallWindowProcA
    - RegisterClassExA
    - UnregisterClassA
    - CreateWindowExA
    - IsWindow
    - DestroyWindow
    - GetWindowLongA
    - SetWindowLongA
    - LoadCursorA
    - SendMessageA
    - LoadStringA
    - GetClassInfoExA
    - AttachThreadInput
    - SendMessageTimeoutA
    - CharNextW
    - CharUpperA
    - PostThreadMessageA
    - DispatchMessageA

    - TranslateMessage
    - GetMessageA
    - GetWindowThreadProcessId
    - GetTopWindow
    - GetClassNameA
    - FindWindowA
    - GetForegroundWindow
    - SetWindowPos
- ADVAPI32.dll
    - RegQueryValueExA
    - RegQueryInfoKeyA
    - GetUserNameA
    - LookupAccountSidA
    - RegSetValueExA
    - RegQueryInfoKeyW
    - RegOpenKeyExA
    - RegEnumKeyExA
    - RegDeleteValueA
    - RegDeleteKeyA
    - RegCreateKeyExA
    - RegCloseKey
- SHELL32.dll
    - SHGetFolderPathA
- ole32.dll
    - CoCreateInstance
    - CLSIDFromProgID
    - CoUninitialize
    - CoInitializeEx
    - CLSIDFromProgIDEx
    - CoTaskMemAlloc
    - CoRevokeClassObject
    - CoResumeClassObjects
    - CoAddRefServerProcess
    - CoReleaseServerProcess
    - StringFromGUID2
    - CoCreateGuid
    - CoTaskMemFree
    - ProgIDFromCLSID
    - CoRegisterClassObject
    - CoTaskMemRealloc
- OLEAUT32.dll
    - RegisterTypeLib
    - UnRegisterTypeLib
    - VarBstrCmp
    - GetActiveObject
    - CreateErrorInfo
    - SetErrorInfo
    - LoadRegTypeLib
    - LoadTypeLib
    - VarBstrCat
    - VarUI4FromStr
    - VariantChangeType
    - VariantClear
    - VariantInit
    - SysAllocStringByteLen
    - SysStringByteLen
    - SysStringLen
    - SysFreeString
    - SysAllocStringLen
    - SysAllocString
    - GetErrorInfo
- SHLWAPI.dll
    - PathAppendA

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 579536, u'sha256': u'f80db74809a0dcbbd09bd01a02bc20800d0317a5e28185fbbc6f4881d8b3fb8c', u'type': u'ASCII text, with CRLF line terminators', u'size': 123}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 579664, u'sha256': u'4ad526a67e1ad9d0e5d010f95759767ce0bad6981687dfd21067a7b846557483', u'type': u'ASCII text, with CRLF line terminators', u'size': 615}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 580280, u'sha256': u'faa716ce9b0abeb30d5a587739df7eb5f1f464a115c5d58dba8c1ef8455d4f3f', u'type': u'ASCII text, with CRLF line terminators', u'size': 598}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 580880, u'sha256': u'f36701b13700a16264162b4733bb76e243814a7abd71acb220427c376399be17', u'type': u'ASCII text, with CRLF line terminators', u'size': 632}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 581512, u'sha256': u'1c01d2951acc045691ca8e8d533076e6f26b103890e855663b04ee23b53e33c7', u'type': u'ASCII text, with CRLF line terminators', u'size': 632}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 582144, u'sha256': u'026e09bf5b463d3c505cf36f7df0c838973075866ae279ab7f2367d9a7276ab1', u'type': u'ASCII text, with CRLF line terminators', u'size': 592}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 582736, u'sha256': u'5089856ded59d39333b2878c7bda882bf1f88fad4b49c4cddb63e3bb676ca17d', u'type': u'ASCII text, with CRLF line terminators', u'size': 656}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 583392, u'sha256': u'9c125ddc0b1604760d9bf5b26cb21c75aa87a34a9fe8224d6369eea771794206', u'type': u'ASCII text, with CRLF line terminators', u'size': 612}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 587216, u'sha256': u'41cc5fd9ab1e9e75788dc35a22847e5e5835ba6856a51b7503302f582f643aa6', u'type': u'ASCII text, with CRLF line terminators', u'size': 648}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 584008, u'sha256': u'5b05955ff279b478bd7329efd491e70f687d1d74e0de56e84b741d0ec8b1656b', u'type': u'ASCII text, with CRLF line terminators', u'size': 640}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 584648, u'sha256': u'fa02e212b2f12d292e7dee4ecc7a0e345f9d17af580d3b82d963fd9dde054034', u'type': u'ASCII text, with CRLF line terminators', u'size': 606}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 585256, u'sha256': u'b3c3e9560bf806c95d01e1462d8d147edffc527a398f1286660f3d96b705cc0a', u'type': u'ASCII text, with CRLF line terminators', u'size': 655}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 585912, u'sha256': u'69a9be07549d968701efed3d785c3090854ebe7d41de73a237fa14cd7c2c139b', u'type': u'ASCII text, with CRLF line terminators', u'size': 592}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 586504, u'sha256': u'c6dc71e119350257879002e12ae2a33de36ec3df9f26c71d9acdb217a29401bf', u'type': u'ASCII text, with CRLF line terminators', u'size': 712}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 587864, u'sha256': u'8ad7120d894c40af4be6533e3bdf2e3b5eb7509226a918461fc6b5812a38bf05', u'type': u'ASCII text, with CRLF line terminators', u'size': 648}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 588512, u'sha256': u'2624d0e88cbf8a2710c209eebd36a13eefd279283f488f9a28e7a99493cb2d06', u'type': u'ASCII text, with CRLF line terminators', u'size': 640}

{u'lang': u'LANG_ENGLISH', u'name': u'REGISTRY', u'offset': 589152, u'sha256': u'503c4f959fb11b7fdcd343667495b247658ff9cfd2508b2b883288f9bc1c711e', u'type': u'ASCII text, with CRLF line terminators', u'size': 649}

{u'lang': u'LANG_ENGLISH', u'name': u'TYPELIB', u'offset': 589808, u'sha256': u'79afc3f69bf3ed3715ae6b69e2eb4dc74c60bb67be55cfaf29129e894c8847ee', u'type': u'data', u'size': 44032}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 633840, u'sha256': u'07119c4d5090d44dc9317155b80cb5e59116a276d8b0f5a2ed271d6b634e2ac5', u'type': u'data', u'size': 50}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 578720, u'sha256': u'0258c8a8f1ce5ad2bc8c838da0654a3fd798167cb295988ebe27e3ad9963cab7', u'type': u'data', u'size': 812}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 633896, u'sha256': u'4bb79dcea0a901f7d9eac5aa05728ae92acb42e0cb22e5dd14134f4421a3d8df', u'type': u'XML 1.0 document text', u'size': 381}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS