VALKYRIE COMODO

Summary

File Name: DSTClientes.exe

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

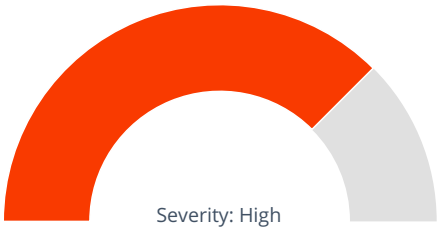
SHA1: 682433e268fccc4f51b99c44b6ecb574f18064f0

MD5: e833cbdf82a567b459f6374e74502a63

MALWARE

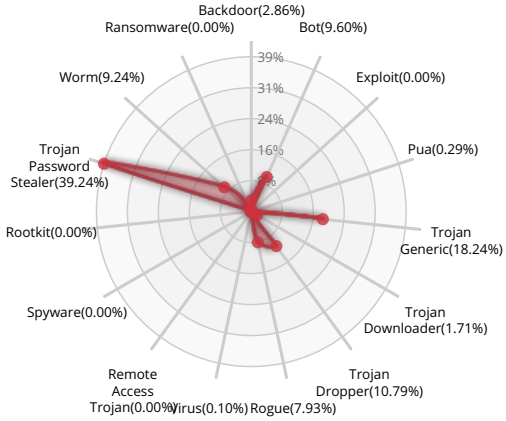
Valkyrie Final Verdict

DETECTION SECTION

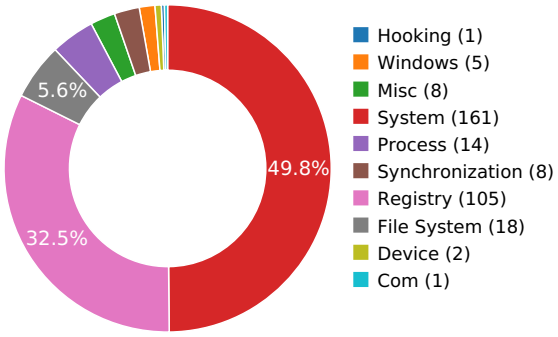


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

VALKYRIE COMODO

Behavior Graph

21:33:29 **21:33:29** **21:33:29**

PID 2940

21:33:29	Create Process	The malicious file created a child process as 682433e268fccc4f51b99c44b6ecb574f18064f0.exe **(PPID 1640)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\682433e268fccc4f51b99c44b6ecb574f18064f0.exe.cfg
C:\Windows\sysnative\C_932.NLS
C:\Windows\sysnative\C_949.NLS
C:\Windows\sysnative\C_950.NLS
C:\Windows\sysnative\C_936.NLS
C:\Users\user\AppData\Local\Temp\DeltaDST.INI
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Users\user\AppData\Local\Temp\netmsg.dll
C:\Windows\System32\netmsg.dll
C:\Windows\Fonts\staticcache.dat
C:\Windows\WINHELP.INI
C:\Windows\System32\.HLP
C:\Windows\Help\.HLP

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\HTML Help\.HLP
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Help\.HLP
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

RESOLVED APIS

cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
oleaut32.dll.OleLoadPictureEx
oleaut32.dll.DispCallFunc
oleaut32.dll.LoadTypeLibEx
oleaut32.dll.UnRegisterTypeLib
oleaut32.dll.CreateTypeLib2
oleaut32.dll.VarDateFromUdate
oleaut32.dll.VarUdateFromDate
oleaut32.dll.GetAltMonthNames
oleaut32.dll.VarNumFromParseNum
oleaut32.dll.VarParseNumFromStr
oleaut32.dll.VarDecFromR4
oleaut32.dll.VarDecFromR8
oleaut32.dll.VarDecFromDate
oleaut32.dll.VarDecFromI4
oleaut32.dll.VarDecFromCy
oleaut32.dll.VarR4FromDec
oleaut32.dll.GetRecordInfoFromTypeInfo
oleaut32.dll.GetRecordInfoFromGuids

oleaut32.dll.SafeArrayGetRecordInfo
oleaut32.dll.SafeArraySetRecordInfo
oleaut32.dll.SafeArrayGetIID
oleaut32.dll.SafeArraySetIID
oleaut32.dll.SafeArrayCopyData
oleaut32.dll.SafeArrayAllocDescriptorEx
oleaut32.dll.SafeArrayCreateEx
oleaut32.dll.VarFormat
oleaut32.dll.VarFormatDateTime
oleaut32.dll.VarFormatNumber
oleaut32.dll.VarFormatPercent
oleaut32.dll.VarFormatCurrency
oleaut32.dll.VarWeekdayName
oleaut32.dll.VarMonthName
oleaut32.dll.VarAdd
oleaut32.dll.VarAnd
oleaut32.dll.VarCat
oleaut32.dll.VarDiv
oleaut32.dll.VarEqv
oleaut32.dll.VarIdiv
oleaut32.dll.VarImp
oleaut32.dll.VarMod
oleaut32.dll.VarMul
oleaut32.dll.VarOr
oleaut32.dll.VarPow
oleaut32.dll.VarSub
oleaut32.dll.VarXor
oleaut32.dll.VarAbs
oleaut32.dll.VarFix
oleaut32.dll.VarInt
oleaut32.dll.VarNeg
oleaut32.dll.VarNot
oleaut32.dll.VarRound
oleaut32.dll.VarCmp
oleaut32.dll.VarDecAdd

oleaut32.dll.VarDecCmp
oleaut32.dll.VarBstrCat
oleaut32.dll.VarCyMull4
oleaut32.dll.VarBstrCmp
ole32.dll.CoCreateInstanceEx
ole32.dll.CLSIDFromProgIDEx
sxs.dll.SxsOleAut32MapIIDOrCLSIDToTypeLibrary
user32.dll.GetSystemMetrics
user32.dll.MonitorFromWindow
user32.dll.MonitorFromRect
user32.dll.MonitorFromPoint
user32.dll.EnumDisplayMonitors
user32.dll.GetMonitorInfoA
kernel32.dll.GetPrivateProfileStringA
user32.dll.GetAncestor
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW

REGISTRY KEYS

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\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Codepage
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VBA\Monitors
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\682433e268fccc4f51b99c44b6ecb574f18064f0.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\HTML Help
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\HTML Help\.HLP
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Help
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Help\.HLP
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

READ FILES

\Device\KsecDD

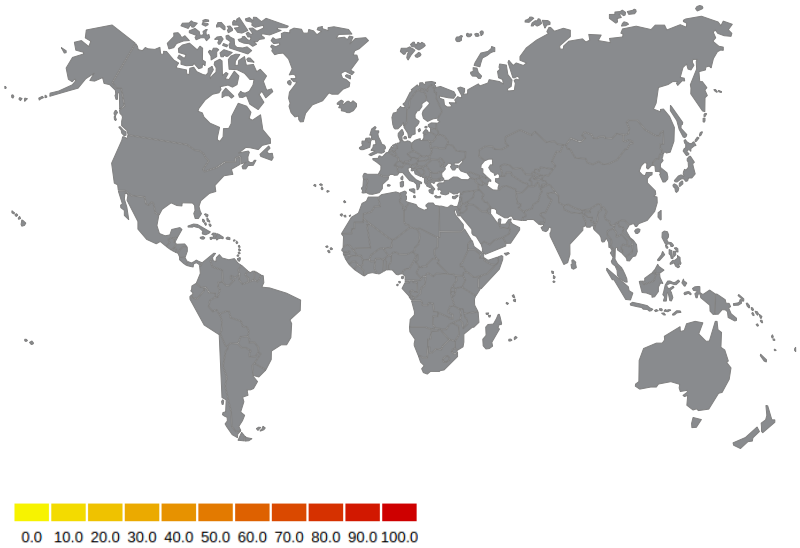
C:\Users\user\AppData\Local\Temp\DeltaDST.INI
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\System32\netmsg.dll
C:\Windows\Fonts\staticcache.dat
C:\Windows\WINHELP.INI

MUTEXES

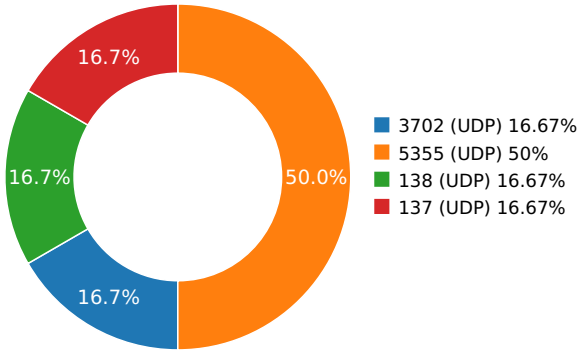
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.06580090523	Sandbox	224.0.0.252	5355
3.087018013	Sandbox	224.0.0.252	5355
3.09252691269	Sandbox	239.255.255.250	3702
3.1239130497	Sandbox	192.168.56.255	137
5.64208102226	Sandbox	224.0.0.252	5355
6.13182282448	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	DSTClientes.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	682433e268fccc4f51b99c44b6ecb574f18064f0
MD5:	e833cbdf82a567b459f6374e74502a63
First Seen Date:	2018-03-14 15:53:19.238889 (12 months ago)
Number Of Clients Seen:	2
Last Analysis Date:	2018-03-14 15:53:19.238889 (12 months ago)
Human Expert Analysis Date:	2018-03-14 17:54:11.609284 (12 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	[]
Number Of Sections	3
Trid	[[84.4, u'Win32 Executable Microsoft Visual Basic 6'], [6.7, u'Win32 Dynamic Link Library (generic)'], [4.6, u'Win32 Executab (generic)'], [2.0, u'Generic Win/DOS Executable'], [2.0, u'DOS Executable Generic']]
Compilation Time Stamp	0x57E121AD [Tue Sep 20 11:46:53 2016 UTC]
Translation	0x0409 0x04b0
InternalName	DSTClientes
FileVersion	1.00.0096
CompanyName	DELTACON
ProductName	DSTClientes
ProductVersion	1.00.0096
OriginalFilename	DSTClientes.exe
Entry Point	0x410420 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	4747264
Ssdeep	98304:B+HH3p6rMzkuSUK1Hd38/V0VGKaNGyz1iGLydlVAfB9VQRHVCMnelOg1j534YO0Q:B+HH3p6rMzkuSUK1Hd38/V0VG
Sha256	6f7ea0d90852904a8538c0cf5a34ea30cfdb63348d3501a9489ad289b54fcf8d
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/6/8/2/4/682433e268fccc4f51b99c44b6ecb574f18064f0', u'EXE:OriginalFileNa u'DSTClientes.exe', u'EXE:ProductName': u'DSTClientes', u'EXE:InternalName': u'DSTClientes', u'File:MIMEType': u'applicati stream', u'File:FileAccessDate': u'2018:03:14 15:52:46+00:00', u'EXE:InitializedDataSize': 204800, u'File:FileModifyDate': u'2(15:52:45+00:00', u'EXE:FileVersionNumber': u'1.0.0.96', u'EXE:FileVersion': u'1.00.0096', u'File:FileSize': u'4.5 MB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'1.00.0096', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'DELTACON', u'File:FileName': u'682433e268fccc4f51b99c44b6ecb574f18064f0', u'EXE:ImageVersi u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2016:09:20 11:46:53+0 u'EXE:FileFlagsMask': u'0x0000', u'EXE:LinkerVersion': 6.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/6/8/2/4', u'EXE:EntryPoint': u'0x10420', u'EXE:SubsystemVer u'EXE:CodeSize': 4734976, u'File:FileInodeChangeDate': u'2018:03:14 15:52:46+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.0.0.96'}]
Mime Type	application/x-dosexec
Imphash	1004a024c75c5b181df0dd8dc608718f

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x48365c	0x484000	5.80211689175	482d5fa6c3d09ca573c6f84d2bc52356
.data	0x485000	0x30a08	0x1000	0.0	620f0b67a91f7f74151bc5be745b7110
.rsrc	0x4b6000	0x786	0x1000	1.64069124978	8e1226720ac172ca78027038f0cb41c2

PE Imports

- MSVBVM60.DLL
  - __vbaVarSub
  - __vbaVarTstGt
  - __vbaStrI2
  - _CIcos
  - _adj_fptan
  - __vbaVarMove
  - __vbaStrI4
  - __vbaVarVargNofree
  - __vbaFreeVar
  - __vbaLenBstr
  - __vbaStrVarMove
  - __vbaLineInputStr
  - __vbaLateIdCall
  - __vbaEnd
  - __vbaFreeVarList
  - _adj_fdiv_m64
  - __vbaFpCDblR8
  - __vbaFreeObjList
  - None
  - __vbaStrErrVarCopy
  - _adj_fprem1
  - None
  - None
  - __vbaResume
  - __vbaVarCmpNe
  - __vbaStrCat
  - None
  - __vbaLsetFixstr
  - None
  - __vbaBoolErrVar
  - None
  - __vbaSetSystemError
  - __vbaStrDate
  - None
  - __vbaHresultCheckObj
  - None
  - __vbaLenVar
  - _adj_fdiv_m32
  - __vbaVarTstLe
  - __vbaAryVar
  - __vbaVarCmpGe
  - __vbaAryDestruct
  - __vbaLateMemSt
  - __vbaBoolStr
  - __vbaVarForInit
  - __vbaExitProc
  - __vbaForEachCollObj
  - None
  - None
  - __vbaOnError
  - __vbaObjSet
  - None
  - None
  - _adj_fdiv_m16i
  - None
  - None
  - __vbaObjSetAddref
  - _adj_fdivr_m16i
  - __vbaVarIndexLoad
  - None
  - None
  - None

- None
- None
- None
- __vbaBoolVar
- None
- None
- None
- __vbaRefVarAry
- __vbaFpR8
- __vbaVarTstLt
- __vbaBoolVarNull
- __vbaVargVar
- _CIsin
- __vbaErase
- None
- None
- None
- __vbaVarCmpGt
- None
- __vbaLateMemStAd
- None
- __vbaNextEachCollObj
- __vbaChkstk
- None
- __vbaFileClose
- EVENT_SINK_AddRef
- __vbaGenerateBoundsError
- None
- __vbaExitEachColl
- None
- __vbaStrCmp
- __vbaAryConstruct2
- __vbaVarTstEq
- __vbaR4Str
- __vbaDateR8
- __vbaPrintObj
- None
- __vbaI2I4
- __vbaObjVar
- DllFunctionCall
- __vbaVarLateMemSt
- __vbaVarOr
- None
- __vbaCastObjVar
- __vbaRedimPreserve
- _adj_fpatan
- __vbaR4Var
- __vbaFixstrConstruct
- __vbaLateIdCallLd
- __vbaRedim
- __vbaStrR8
- EVENT_SINK_Release
- __vbaNew
- None
- None
- _CIsqrt
- __vbaLateIdCallSt
- __vbaObjIs
- __vbaVarAnd
- None
- EVENT_SINK_QueryInterface
- __vbaVarMul
- __vbaExceptHandler
- None
- None
- __vbaStrToUnicode
- __vbaPrintFile
- None
- __vbaDateStr
- _adj_fprem
- _adj_fdivr_m64
- __vbaVarDiv
- None
- __vbaR8ErrVar
- __vbaI2Str

- None
- __vbaFPException
- __vbaInStrVar
- __vbaUbound
- __vbaStrVarVal
- __vbaVarCat
- __vbaDateVar
- __vbaI2Var
- None
- None
- _CIlog
- __vbaErrorOverflow
- __vbaFileOpen
- __vbaInStr
- __vbaVarLateMemCallLdRf
- __vbaR8Str
- __vbaNew2
- __vbaVarInt
- None
- _adj_fdiv_m32i
- _adj_fdivr_m32i
- __vbaStrCopy
- None
- __vbaI4Str
- __vbaVarNot
- __vbaVarCmpLt
- __vbaFreeStrList
- _adj_fdivr_m32
- __vbaR8Var
- _adj_fdiv_r
- None
- None
- __vbaVarTstNe
- __vbaI4Var
- __vbaVarLateMemStAd
- __vbaVarCmpEq
- None
- __vbaAryLock
- __vbaVarAdd
- __vbaLateMemCall
- __vbaStrToAnsi
- None
- __vbaVarDup
- None
- __vbaFpI2
- None
- __vbaVarTstGe
- __vbaUnkVar
- __vbaFpI4
- __vbaVarCopy
- __vbaVarLateMemCallLd
- __vbaVarSetObjAddref
- None
- __vbaLateMemCallLd
- _CIatan
- __vbaI2ErrVar
- __vbaAryCopy
- __vbaStrMove
- __vbaCastObj
- __vbaStrVarCopy
- None
- None
- None
- _allmul
- None
- None
- __vbaLateIdSt
- None
- _CItan
- None
- None
- __vbaFPInt
- __vbaAryUnlock
- __vbaVarForNext
- _CIexp

- __vbaFreeObj
- __vbaFreeStr
- __vbaI4ErrVar
- None

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 4940958, u'sha256': u'12fe321b0621c80aa6f6c93b4242a06c1ffe58a6a3ef2e39d36512671b56a7b7', u'type': u'data', u'size': 744}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 4940662, u'sha256': u'1d79c577d33c037f4a6df3192f5f84a4e70e42573cdf9cecb7654e692af26755', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 4940628, u'sha256': u'f5e735ae527bb0eba5289d4218d6a900acb806a504b9ecf973ede85a11438b57', u'type': u'MS Windows icon resource - 2 icons, 32x32, 16 colors', u'size': 34}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 4940064, u'sha256': u'01bd1170ff82458275277b51fb26d89e3fc0761d04305bcd38eea8c5622afc32', u'type': u'data', u'size': 564}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS