VALKYRIE

PUA
Valkyrie Final Verdict

File Name: FunCloud_c9002_s.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 0499a3d96d757d3a6f50e708ecb7b77fbc2b00da
MD5: ff2085822c90a881003319c6a9093eb2
First Seen Date: 2016-01-20 10:20:57 UTC
Number of Clients Seen: 11
Last Analysis Date: 2017-01-09 11:20:46 UTC
Human Expert Analysis Date: 2016-02-01 13:45:10 UTC
Human Expert Analysis Result: PUA
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2017-01-09 11:20:46 UTC	Malware
Static Analysis Overall Verdict	2017-01-09 11:20:46 UTC	No Threat Found
Dynamic Analysis Overall Verdict	2017-01-09 11:20:46 UTC	Highly Suspicious
Human Expert Analysis Overall Verdict	2016-02-01 13:45:10 UTC	PUA
File Certificate Validation		Vendor not found in Trusted List

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

DETECTOR	RESULT
Optional Header LoaderFlags field is valued illegal	Clean
Non-ascii or empty section names detected	Clean
Illegal size of optional Header	Clean
Packer detection on signature database	Unknown
Based on the sections entropy check! file is possibly packed	Suspicious
Timestamp value suspicious	Clean
Header Checksum is zero!	Clean
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean
Anti-vm present	Suspicious
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean
TLS callback functions array detected	Clean

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	

SUSPICIOUS BEHAVIORS	
Creates a child process	
Reads memory of another process	
Writes to address space of another process	
Uses a function clandestinely	
Downloads data from internet	
Modifies Windows policies	
Opens a file in a system directory	

Behavioral Information

QueryFilePath

C:\Windows\SysWOW64\rundll32.exe
C:\Windows\SysWOW64\rundll32.ex
C:\Users\win7\AppData\Local\Temp\FunCloudIns.dll
C:\Windows\syswow64\CRYPT32.dll
C:\Windows\SysWOW64\cryptnet.dll
C:\Windows\system32\cryptnet.dll
C:\FunCloud_c9002_s.exe

InternetDownload

cc000c

LoadLibrary

C:\Users\win7\AppData\Local\Temp\FunCloudIns.dll
KERNEL32.DLL
ADVAPI32.dll
CRYPT32.dll
imagehlp.dll
IPHLPAPI.DLL
ole32.dll
OLEAUT32.dll
SHELL32.dll
SHLWAPI.dll
urlmon.dll
USER32.dll
VERSION.dll
WININET.dll
WINTRUST.dll
WSOCK32.dll
SspiCli.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
C:\Windows\system32\kernel32.dll
C:\Users\win7\AppData\Local\Temp\gma.dll
C:\Users\win7\AppData\Local\Temp\FunWorks64.dll
Secur32.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
WS2_32.dll
winhttp.dll
api-ms-win-downlevel-shlwapi-l2-1-0.dll
DNSAPI.dll
Comctl32.dll
imm32.dll
C:\Windows\system32\ws2_32

CRYPTBASE.dll
dhcpcsvc.DLL
C:\Users\win7\AppData\Local\Temp\Firemanii.dll
CRYPTSP.dll
WINTRUST.DLL
C:\Windows\syswow64\CRYPT32.dll
ncrypt.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
bcrypt.dll
USERENV.dll
API-MS-Win-Security-SDDL-L1-1-0.dll
cryptnet.dll
C:\Windows\SysWOW64\cryptnet.dll
profapi.dll
SensApi.dll
API-MS-WIN-Service-Management-L1-1-0.dll
API-MS-WIN-Service-winsvc-L1-1-0.dll
RPCRT4.dll
ADVAPI32.DLL
comctl32.dll
C:\Windows\system32\cryptnet.dll
ntdll.dll
setupapi.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
Cabinet.dll
DEVRTL.dll

LowerChar

http

ReadRegisteryKey

EnableLUA
aptdir
sioiname
mac
aptid
guid
SyncMode5
FEATURE_CLIENTAUTHCERTFILTER
FromCacheTimeout
SecureProtocols
DisableKeepAlive
IdnEnabled
PreConnectLimit
PreResolveLimit
SqmHttpStreamRandomUploadPoolSize
CacheMode
EnableHttp1_1
ProxyHttp1.1
EnableNegotiate
DisableBasicOverClearChannel
ClientAuthBuiltInUI
DisableReadRange
SocketSendBufferLength
SocketReceiveBufferLength
KeepAliveTimeout
MaxHttpRedirects
MaxConnectionsPerServer
MaxConnectionsPer1_0Server
MaxConnectionsPerProxy
ServerInfoTimeout
ConnectTimeOut
ConnectRetries
SendTimeOut
ReceiveTimeOut
DisableNTLMPreAuth
ScavengeCacheLowerBound
CertCacheNoValidate
ScavengeCacheFileLifeTime
ScavengeCacheFileLimit

HttpDefaultExpiryTimeSecs
FtpDefaultExpiryTimeSecs
LeashLegacyCookies
SendExtraCRLF
WpadSearchAllDomains
DontUseDNSLoadBalancing
ShareCredsWithWinHttp
DnsCacheEnabled
DnsCacheEntries
DnsCacheTimeout
WarnOnPost
WarnAlwaysOnPost
WarnOnZoneCrossing
WarnOnBadCertRecving
WarnOnPostRedirect
AlwaysDrainOnRedirect
WarnOnHTTPSToHTTPRedirect
TcpAutotuning
BadProxyExpiresTime
FrameTabWindow
FrameMerging
SessionMerging
AdminTabProcs
TabProcGrowth
AutoProxyDetectType
WpadOverride
DisableBranchCache
UseFirstAvailable
CombineFalseStartData
DisableFalseStartBlocklist
EnforceP3PValidity
DuoProtocols
EnableSpdyDebugAsserts
SystemSetupInProgress
ProxyEnable
ProxyServer
ProxyOverride
AutoConfigURL
AutoDetect
SavedLegacySettings
DefaultConnectionSettings
<NULL>
Compatible
Version
Platform
DisableSecuritySettingsCheck
CreateUriCacheSize
EnablePunycode
WpadDecision
WpadDecisionTime
WpadExpirationDays
WpadDecisionReason
WpadDhcp
WpadDns
WpadDetectedUrl
cid
appversion

CreateRegisteryKey

S-1-5-21-3979321414-2393373014-2172761192-1000\Software\SystemSres
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Software\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
52-54-00-12-35-02
{69DC4768-446B-4F82-A6B0-63966A243064}

CreateFile

C:\Users\win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat
\\.\Nsi
C:\Windows\system32\rsaenh.dll

C:\Users\win7\AppData\Local\Temp\FiremaniiTmp.dll
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\378B079587A9184B2E2AB859CB263F40_524AD1B9B08D3C6450727265AE77B7D2
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\378B079587A9184B2E2AB859CB263F40_524AD1B9B08D3C6450727265AE77B7D2
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8EB35376744F392396307460D546222D_1EDE0C64F54544A8723268C97FF33DBA
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\8EB35376744F392396307460D546222D_1EDE0C64F54544A8723268C97FF33DBA
C:\Users\win7\AppData\Local\Temp\senvclear.zip
C:\Users\win7\AppData\Local\Temp/senvclear.daw
C:\Users\win7\AppData\Local\Temp\senvclear.daw
C:\Users\win7\AppData\Local\Temp\ssenvclear.daw
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\win7\AppData\Local\Temp\Cab3CD3.tmp
C:\Users\win7\AppData\Local\Temp\Tar3CD4.tmp
C:\Users\win7\AppData\Local\Temp\FunCloudIns.dll

OpenRegisteryKey

SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\SystemSres
Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
Software\Microsoft\Internet Explorer\Main\FeatureControl
FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
RETRY_HEADERONLYPOST_ONCONNECTIONRESET
FEATURE_MIME_HANDLING
FEATURE_BYPASS_CACHE_FOR_CREDPOLICY_KB936611
FEATURE_IGNORE_MAPPINGS_FOR_CREDPOLICY
FEATURE_INCLUDE_PORT_IN_SPN_KB908209
FEATURE_BUFFERBREAKING_818408
FEATURE_SKIP_POST_RETRY_ON_INTERNETWRITEFILE_KB895954
FEATURE_FIX_CHUNKED_PROXY_SCRIPT_DOWNLOAD_KB843289
FEATURE_USE_CNAME_FOR_SPN_KB911149
FEATURE_PERMIT_CACHE_FOR_AUTHENTICATED_FTP_KB910274
FEATURE_DISABLE_UNICODE_HANDLE_CLOSING_CALLBACK
FEATURE_DISALLOW_NULL_IN_RESPONSE_HEADERS
FEATURE_DIGEST_NO_EXTRAS_IN_URI
FEATURE_ENABLE_PASSPORT_SESSION_STORE_KB948608
FEATURE_EXCLUDE_INVALID_CLIENT_CERT_KB929477
FEATURE_USE_UTF8_FOR_BASIC_AUTH_KB967545
FEATURE_RETURN_FAILED_CONNECT_CONTENT_KB942615
FEATURE_PRESERVE_SPACES_IN_FILENAMES_KB952730
FEATURE_ENABLE_PROXY_CACHE_REFRESH_KB2983228
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Policies
Software
Software\Policies\Microsoft\Internet Explorer
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
FEATURE_DISABLE_NOTIFY_UNVERIFIED_SPN_KB2385266
FEATURE_COMPAT_USE_CONNECTION_BASED_NEGOTIATE_AUTH_KB2151543
FEATURE_SCH_SEND_AUX_RECORD_KB_2618444
Software\Microsoft\Internet Explorer\Main
Software\Policies\Microsoft\Internet Explorer\Main
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
System\Setup
Software\Policies\Microsoft\PeerDist\Service
Software\Microsoft\Windows NT\CurrentVersion\PeerDist\Service
FEATURE_BROWSER_EMULATION
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent
Microsoft\Windows\CurrentVersion\Internet Settings\User Agent
Pre Platform
Post Platform
FEATURE_IGNORE_POLICIES_ZONEMAP_IF_ESC_ENABLED_KB918915
FEATURE_ZONES_CHECK_ZONEMAP_POLICY_KB941001
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Microsoft\Internet Explorer\Security
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
FEATURE_LOCALMACHINE_LOCKDOWN
FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB932562
Content
Cookies
History
{69DC4768-446B-4F82-A6B0-63966A243064}

Software\Microsoft\Cryptography\Wintrust\Config
System\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}

CreateMutex

<NULL>
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex

CreateProcess

rundll32.exe "C:\Users\win7\AppData\Local\Temp\FunCloudIns.dll" startup

DeleteFile

C:\Users\win7\AppData\Local\Temp\Firemanii_192.dll
C:\Users\win7\AppData\Local\Temp\senvclear.zip
C:\Users\win7\AppData\Local\Temp\senvclear.daw
C:\Users\win7\AppData\Local\Temp\Cab3CD3.tmp
C:\Users\win7\AppData\Local\Temp\Tar3CD4.tmp

QueryProcessAddress

CreateProcessW
InternetReadFile
ShellExecuteW
IsDebuggerPresent

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2016-01-20 12:10:59 UTC
Analysis End Date: 2016-02-01 13:45:10 UTC
File Upload Date: 2016-01-20 10:21:27 UTC
Human Expert Analyst Feedback: PUA
Verdict: PUA

Additional File Information

Vendor Validation - Not Verified ✖

[+] Beijing Funshion Online Technologies Ltd.

Status	Not Valid ✖

Certificate Validation - Success ✔

[+] Beijing Funshion Online Technologies Ltd.

Status	NotTimeValid (no effect on chain status)
Start Date	2014-07-04 00:00:00+00:00
End Date	2016-08-01 23:59:59+00:00
Sha256	1ce18bb0b9481f4e93844e8fa556da912b2757a1a31261c2b2ac263099fa8c84
Serial	33A6A2626F7248245F3A615A8CE7DADE
Subject Name	Beijing Funshion Online Technologies Ltd.
Subject Key Identifier	96 69 5e d0 59 9d 4a 98 2f 0a af 57 3b d6 ca c7 50 fc 11 20
Subject Organization	Beijing Funshion Online Technologies Ltd.
Subject Locality	Beijing
Subject State	Beijing
Subject Country	CN
Subject Organizational Unit	SECURE APPLICATION DEVELOPMENT
Issuer Name	Thawte Code Signing CA - G2
Issuer Key Identifier	d4 0d 65 3f 7a bd 34 c6 fe 47 e7 4c 0d c0 bd f2 de 15 ab 71
Issuer Organization	Thawte, Inc.
Issuer Country	US
Crl link	http://th.symcb.com/th.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] Thawte Code Signing CA - G2

Status	NoError
Start Date	2010-02-08 00:00:00+00:00
End Date	2020-02-07 23:59:59+00:00
Sha256	a44fef327fa3436f37535d337f7cd8c480a5fe23ae5369476877c3341873ed20
Serial	47974D7873A5BCAB0D2FB370192FCE5E
Subject Name	Thawte Code Signing CA - G2
Subject Key Identifier	d4 0d 65 3f 7a bd 34 c6 fe 47 e7 4c 0d c0 bd f2 de 15 ab 71
Subject Organization	Thawte, Inc.
Subject Country	US
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Issuer Organization	thawte, Inc.
Issuer Country	US
Issuer Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Crl link	http://crl.thawte.com/ThawtePCA.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Client Authentication (1.3.6.1.5.5.7.3.2)

[+] thawte Primary Root CA

Status	NoError ✔
Start Date	2006-11-17 00:00:00+00:00
End Date	2036-07-16 23:59:59+00:00
Sha256	d6a37f73bd37d7adacb96997064639215d4806b63a4ccee5416e3da8d68a3b1f
Serial	344ED55720D5EDEC49F42FCE37DB2B6D
Subject Name	thawte Primary Root CA
Subject Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Subject Organization	thawte, Inc.
Subject Country	US
Subject Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	undefined
Issuer Organization	thawte, Inc.
Issuer Country	US
Issuer Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

[+] Thawte Code Signing CA - G2

Status	NoError ✔
Start Date	2010-02-08 00:00:00+00:00
End Date	2020-02-07 23:59:59+00:00
Sha256	a44fef327fa3436f37535d337f7cd8c480a5fe23ae5369476877c3341873ed20
Serial	47974D7873A5BCAB0D2FB370192FCE5E
Subject Name	Thawte Code Signing CA - G2
Subject Key Identifier	d4 0d 65 3f 7a bd 34 c6 fe 47 e7 4c 0d c0 bd f2 de 15 ab 71
Subject Organization	Thawte, Inc.
Subject Country	US
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Issuer Organization	thawte, Inc.
Issuer Country	US
Issuer Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Crl link	http://crl.thawte.com/ThawtePCA.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Client Authentication (1.3.6.1.5.5.7.3.2)

[+] thawte Primary Root CA

Status	NoError ✔
Start Date	2006-11-17 00:00:00+00:00
End Date	2036-07-16 23:59:59+00:00
Sha256	d6a37f73bd37d7adacb96997064639215d4806b63a4ccee5416e3da8d68a3b1f
Serial	344ED55720D5EDEC49F42FCE37DB2B6D
Subject Name	thawte Primary Root CA
Subject Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Subject Organization	thawte, Inc.
Subject Country	US
Subject Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	undefined
Issuer Organization	thawte, Inc.
Issuer Country	US
Issuer Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x568382DD [Wed Dec 30 07:08:13 2015 UTC]
Entry Point	0x45bb15 (.text)
File Size	1845240
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	Copyright (C) 2015- All Rights Reserved.
Internal Name	tkinstall.exe
File Version	1.0.2.1
Company Name	\x5317\x4eac\x98ce\x884c\x5728\x7ebf\x6280\x672f\x6709\x9650\x516c\x53f8
Product Name	\x98ce\x884c\x89c6\x9891\x52a0\x901f\x5668
Product Version	1.0.2.1
File Description	\x98ce\x884c\x89c6\x9891\x52a0\x901f\x5668\x5b89\x88c5\x7a0b\x5e8f
Original Filename	tkinstall.exe
Translation	0x0804 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	6
Sha256	6ae4f5294e91fc84d3a9971e0e87fcb2c6940a22e03b076b4a349eedc354eeee

File Paths

FILE PATH ON CLIENT	SEEN COUNT
0499a3d96d757d3a6f50e708ecb7b77fbc2b00da	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x83fa2	0x84000	6.542148	-
.rdata	0x85000	0x1db90	0x1dc00	4.580450	-
.data	0xa3000	0xc900	0x7c00	4.984827	-
.tls	0xb0000	0x2	0x200	0.000000	-
.rsrc	0xb1000	0x10587c	0x105a00	7.570574[SUSPICIOUS]	-
.reloc	0x1b7000	0x11b60	0x11c00	4.271468	-

PE Imports

gdiplus.dll

- GdipGetPathWorldBounds
- GdipGetFontStyle
- GdipGetFontSize
- GdipAddPathString
- GdipDeleteStringFormat
- GdipCreateStringFormat
- GdipDeletePath
- GdipCreatePath
- GdipGetFamilyName
- GdipGetFamily
- GdipCreateFontFamilyFromName
- GdipDeleteFontFamily
- GdipGetGenericFontFamilySansSerif
- GdipCreateFont
- GdipCloneBrush
- GdipDeleteBrush
- GdipCreateSolidFill
- GdipDrawString
- GdipDrawImageRectRect
- GdipSetImageAttributesColorMatrix
- GdipCreateImageAttributes
- GdipGetImageHeight
- GdipGetImageWidth
- GdipDrawLine
- GdipDeletePen
- GdipCreatePen1
- GdipSetTextRenderingHint
- GdipResetClip
- GdipEndContainer

- GdipRotateWorldTransform
- GdipScaleWorldTransform
- GdipTranslateWorldTransform
- GdipBeginContainer2
- GdipSetClipRect
- GdipLoadImageFromFileICM
- GdipDisposeImage
- GdipCloneImage
- GdipAlloc
- GdipFree
- GdipCreateBitmapFromStream
- GdiplusShutdown
- GdipCreateFromHDC
- GdipDeleteGraphics
- GdipReleaseDC
- GdipDeleteFont
- GdipDisposeImageAttributes
- GdipGetFontHeightGivenDPI
- GdiplusStartup

- WS2_32.dll
  - null
  - null
  - null

- VERSION.dll
  - GetFileVersionInfoSizeW
  - GetFileVersionInfoW
  - VerQueryValueW

- KERNEL32.dll
  - TlsAlloc
  - TlsFree
  - GetModuleHandleExA
  - WaitForSingleObject
  - ResetEvent
  - CreateEventW
  - GetModuleFileNameW
  - LoadLibraryW

- GetProcAddress
- Sleep
- CreateToolhelp32Snapshot
- Process32FirstW
- OpenProcess
- Process32NextW
- TerminateProcess
- FreeLibrary
- lstrcmpW
- GetNativeSystemInfo
- GetVersionExW
- GetSystemInfo
- WideCharToMultiByte
- CreateFileW
- WriteFile
- GetModuleHandleW
- GlobalAlloc
- GlobalLock
- GlobalUnlock
- GetCurrentProcess
- GetPrivateProfileStringW
- WritePrivateProfileStringW
- CreateProcessW
- GetTickCount
- GetTempPathW
- GetFileAttributesW
- FindFirstFileW
- SetFileAttributesW
- FindNextFileW
- FindClose
- CopyFileW
- DeleteFileW
- CreateMutexW
- GetLastError
- GetProcessHeap
- HeapFree
- ReleaseSemaphore

- CreateSemaphoreA
- GetSystemTimeAsFileTime
- ResumeThread
- WaitForMultipleObjects
- HeapAlloc
- GetCommandLineW
- lstrlenW
- GetSystemDefaultLangID
- LockResource
- SetLastError
- TlsSetValue
- lstrcpyW
- LocalAlloc
- LocalFree
- lstrcmpA
- lstrcpynW
- ReadFile
- InterlockedPopEntrySList
- InterlockedIncrement
- InterlockedDecrement
- EncodePointer
- DecodePointer
- OpenEventA
- SystemTimeToFileTime
- SetWaitableTimer
- CreateWaitableTimerA
- FormatMessageA
- QueryPerformanceCounter
- HeapSetInformation
- GetStartupInfoW
- ExitThread
- CreateThread
- RtlUnwind
- LCMapStringW
- GetCPInfo
- UnhandledExceptionFilter
- SetUnhandledExceptionFilter

- IsDebuggerPresent
- ExitProcess
- GetStdHandle
- GetLocaleInfoW
- FreeEnvironmentStringsW
- GetEnvironmentStringsW
- SetHandleCount
- GetFileType
- HeapCreate
- SizeofResource
- GetACP
- GetOEMCP
- IsValidCodePage
- GetStringTypeW
- GetConsoleCP
- GetConsoleMode
- SetFilePointer
- FlushFileBuffers
- GetUserDefaultLCID
- GetLocaleInfoA
- CloseHandle
- SetEvent
- CreateEventA
- TlsGetValue
- InterlockedExchange
- DeleteCriticalSection
- EnterCriticalSection
- LeaveCriticalSection
- InitializeCriticalSection
- GetCurrentProcessId
- GetCurrentThreadId
- MultiByteToWideChar
- FindResourceExW
- FindResourceW
- VirtualAlloc
- VirtualFree
- IsProcessorFeaturePresent

- InterlockedPushEntrySList
- InterlockedCompareExchange
- HeapSize
- RaiseException
- LoadResource
- InitializeCriticalSectionAndSpinCount
- EnumSystemLocalesA
- HeapDestroy
- IsValidLocale
- WriteConsoleW
- SetStdHandle
- SetEndOfFile
- FlushInstructionCache
- GetPrivateProfileIntW
- MoveFileW
- CreateDirectoryW
- HeapReAlloc

- USER32.dll
  - GetCursorPos
  - GetDesktopWindow
  - ReleaseDC
  - UpdateLayeredWindow
  - GetWindowDC
  - GetWindowRect
  - ReleaseCapture
  - GetCapture
  - SetCapture
  - GetWindowLongW
  - SetWindowLongW
  - ShowWindow
  - IsWindow
  - RegisterClassW
  - LoadIconW
  - SendMessageW
  - PtInRect
  - LoadCursorW
  - SystemParametersInfoW

- GetDC
- MessageBoxExW
- MessageBoxW
- DestroyWindow
- SetTimer
- PostQuitMessage
- UnregisterClassW
- PostMessageW
- KillTimer
- WaitMessage
- GetQueueStatus
- TranslateMessage
- RegisterClassExW
- CallMsgFilterW
- MsgWaitForMultipleObjectsEx
- CreateWindowExW
- DefWindowProcW
- DispatchMessageW
- PeekMessageW
- GetClassInfoExW
- IsWindowVisible
- SetWindowTextW
- GetWindowTextW
- GetWindowTextLengthW
- GetClientRect
- SetFocus
- CallWindowProcW
- SetCursor
- UnregisterClassA
- SetWindowPos

GDI32.dll

- DeleteDC
- SetTextColor
- CreateFontIndirectW
- GetStockObject
- GetObjectW
- EnumFontFamiliesW

- DeleteObject
- SelectObject
- CreateDIBSection
- CreateCompatibleDC

- ADVAPI32.dll
  - RegCreateKeyExW
  - RegCloseKey
  - RegSetValueExW
  - RegOpenKeyExW
  - RegQueryValueExW
- SHELL32.dll
  - SHCreateDirectoryExW
  - SHGetPathFromIDListW
  - SHBrowseForFolderW
  - null
  - ShellExecuteW
  - SHGetSpecialFolderPathW
- ole32.dll
  - CoUninitialize
  - CoInitialize
  - CoCreateGuid
  - CoInitializeEx
  - CoTaskMemFree
  - CoCreateInstance
  - CreateStreamOnHGlobal
- WINTRUST.dll
  - WinVerifyTrust
- imagehlp.dll
  - ImageGetCertificateHeader
  - ImageGetCertificateData
- CRYPT32.dll
  - CryptDecodeObject
  - CertCloseStore
  - CryptMsgGetParam
  - CertFreeCertificateContext
  - CryptMsgClose

- CryptVerifyMessageSignature
- CryptQueryObject

WININET.dll
- InternetOpenUrlW
- InternetCloseHandle
- HttpQueryInfoA
- HttpQueryInfoW
- InternetGetConnectedState
- InternetOpenA
- InternetSetOptionA
- InternetReadFile

SHLWAPI.dll
- PathFileExistsW
- PathFindFileNameW
- SHSetValueW
- PathRemoveFileSpecW
- PathRemoveExtensionW
- PathIsURLW
- PathIsFileSpecW
- PathAppendW
- SHGetValueW

urlmon.dll
- UrlMkGetSessionOption

PE Exports

- ??_B?1??get_instance@?$singleton@VCFpInstallPath@@@serialization@boost@@CAAAVCFpInstallPath@@XZ@51
- ??_B?1??get_instance@?$singleton@VCFpSysLanguage@@@serialization@boost@@CAAAVCFpSysLanguage@@XZ@51
- ?get_instance@?$singleton@VCFpInstallPath@@@serialization@boost@@CAAAVCFpInstallPath@@XZ
- ?get_instance@?$singleton@VCFpSysLanguage@@@serialization@boost@@CAAAVCFpSysLanguage@@XZ
- ?get_mutable_instance@?$singleton@VCFpInstallPath@@@serialization@boost@@SAAAVCFpInstallPath@@XZ
- ?get_mutable_instance@?$singleton@VCFpSysLanguage@@@serialization@boost@@SAAAVCFpSysLanguage@@XZ
- ?instance@?$singleton@VCFpInstallPath@@@serialization@boost@@0AAVCFpInstallPath@@A
- ?instance@?$singleton@VCFpSysLanguage@@@serialization@boost@@0AAVCFpSysLanguage@@A
- ?t@?1??get_instance@?$singleton@VCFpInstallPath@@@serialization@boost@@CAAAVCFpInstallPath@@XZ@4V?$singleton_wrapper@VCFpInstallPath@@@detail@34@A
- ?t@?1??get_instance@?$singleton@VCFpSysLanguage@@@serialization@boost@@CAAAVCFpSysLanguage@@XZ@4V?$singleton_wrapper@VCFpSysLanguage@@@detail@34@A

PE Resources

RT_ICON
RT_GROUP_ICON
RT_VERSION
RT_MANIFEST