VALKYRIE

NO THREAT FOUND

File Name: ogZWC9ed.zk
File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
SHA1: 08da52a59efa983c08df72d05b24e6e11f812979
MD5: 3d2673c65c832a9eec1686ef8780c138
First Seen Date: 2016-12-28 09:30:37 UTC
Number of Clients Seen: 2
Last Analysis Date: 2016-12-28 09:30:37 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Valkyrie Automatic Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2016-12-28 09:30:37 UTC	No Match
Static Analysis Overall Verdict	2016-12-28 09:30:37 UTC	No Threat Found
Dynamic Analysis Overall Verdict	2016-12-28 09:30:37 UTC	No Threat Found
File Certificate Validation		Certificate and Vendor name are Not Valid

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	Clean
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	Clean
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
No Threat Found	

SUSPICIOUS BEHAVIORS	
Has no visible windows	❗

Behavioral Information

QueryFilePath

C:\DLL_Loader.exe

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Not Verified ✖

[+] null

Status	Not Valid ✖

Certificate Validation - FileNotSigned ✖

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5853A7FF [Fri Dec 16 08:38:23 2016 UTC]
Entry Point	0x1015f37 (.text)
File Size	172123
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	Brian Harper, \xa9 1997-2005 Stardock.net, Inc
Internal Name	IconPackager
File Version	3.10.00
Company Name	Stardock.net, Inc
Private Build	
Legal Trademarks	
Comments	December 12, 2005
Product Name	IconPackager for ObjectDesktop
O L E Self Register	
Special Build	
Product Version	3.10.00
File Description	IconPackager Repair Module
Original Filename	iprepair.dll
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	6
Sha256	1e2db9b036dc85109e0bfadac229bfdd7a94d9cc75c91d7cf084b3e06c01ae1c

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1b0fc	0x1b200	7.167726[SUSPICIOUS]	-
.rdata	0x1d000	0x2536	0x2600	6.782987	-
.data	0x20000	0xa2f4	0x400	1.769186	-
.zodec	0x2b000	0x4640	0x4800	7.255388[SUSPICIOUS]	-
.rsrc	0x30000	0x3758	0x3800	4.175801	-
.reloc	0x34000	0x474	0x600	2.837833	-

PE Imports

- KERNEL32.dll
  - GetProcAddress
  - WriteFile
  - WriteConsoleW
  - VirtualQuery
  - GetCurrentThreadId
  - GetOEMCP
  - GetModuleHandleW
  - GetProcessHeap
  - GetStartupInfoW
  - FreeEnvironmentStringsW

- LocalFree
- HeapSize
- SetStdHandle
- GetStdHandle
- TlsFree
- TerminateProcess
- LeaveCriticalSection
- GetCommandLineA
- FlushFileBuffers
- HeapReAlloc
- IsDebuggerPresent
- OutputDebugStringW
- GetACP
- RtlUnwind
- lstrlenA
- IsProcessorFeaturePresent
- TlsAlloc
- CreateFileW
- DeleteFileW
- LoadLibraryExW
- InitializeCriticalSectionAndSpinCount
- HeapFree
- FreeLibrary
- LCMapStringW
- Sleep
- GetCurrentProcessId
- GetLastError
- SetUnhandledExceptionFilter
- GetSystemTimeAsFileTime
- GetFileType
- SetFilePointerEx
- SetLastError
- TlsSetValue
- EnterCriticalSection
- UnhandledExceptionFilter
- RaiseException
- HeapDestroy

- GetModuleFileNameA
- GetLocalTime
- GetModuleFileNameW
- GetEnvironmentStringsW
- DeleteCriticalSection
- TlsGetValue
- HeapAlloc
- InterlockedIncrement
- IsValidCodePage
- GetStringTypeW
- GetCurrentProcess
- GetFileAttributesA
- LoadLibraryW
- GetCommandLineW
- InterlockedDecrement
- ExitProcess

USER32.dll

- wsprintfW
- wvsprintfW
- SendMessageA
- CharLowerA

GDI32.dll

- AddFontMemResourceEx
- CancelDC
- AnimatePalette
- BeginPath

ole32.dll

- CoCreateInstance
- CoSetProxyBlanket
- CoInitializeSecurity
- CoUninitialize
- CoInitialize

msvcrt.dll

- __set_app_type
- exit

msi.dll

null

null

PE Exports

_RegisterService@0

_WinMain2@16

PE Resources

RT_BITMAP
RT_VERSION