VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: Favorites_Setup_v5_3.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 5e1764dead2eda86365f5ed931402d34e7f333bf
MD5: 9d058520129efffa5b6e6ab240141131
First Seen Date: 2022-02-01 16:20:41 UTC
Number of Clients Seen: 2
Last Analysis Date: 2022-02-02 12:31:02 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2022-02-01 17:52:56 UTC	Clean	
Static Analysis Overall Verdict	2022-02-02 12:31:02 UTC	No Threat Found	
Precise Detectors Overall Verdict	2022-02-02 12:31:02 UTC	No Match	
File Certificate Validation		Not Applicable	

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	Suspicious	
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	Suspicious	
TLS callback functions array detected	Clean	

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2022-02-02 12:30:57 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2022-02-02 12:30:57 UTC	No Match		NotDetected
Static Precise NI Detector 3	2022-02-02 12:30:57 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2022-02-02 12:30:57 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2022-02-02 12:30:57 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2022-02-02 12:30:57 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2022-02-02 12:30:57 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2022-02-02 12:30:57 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2022-02-02 12:30:57 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2022-02-02 12:30:57 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2022-02-02 12:30:57 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2022-02-02 12:30:57 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x60B88E27 [Thu Jun 3 08:09:11 2021 UTC]
Debug Artifacts	
Entry Point	0x4b5eec (.itext)
Exifinfo	[object Object]
File Size	3521208
File Type Enum	6
Imphash	5a594319a0d69dbc452e748bcf05892e
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	
File Version	
Company Name	DATAKENT
Comments	This installation was built with Inno Setup.
Product Name	MyFavorites
Product Version	5.3
File Description	MyFavorites Setup
Original File Name	
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	10
Sha256	df035583cbd38254362986486d14a91ac69940bff2f15710e3d0936bac6f1239
Ssdeep	49152:1qe3f6nSypktMznFIMQcHBo31wRB5LrqmTvfp4Le21N2SffPMWrQ0Zk2:ESitktMr+3rO5fPvxOLnPcMN
Trid	53.5,Inno Setup installer,21,InstallShield setup,20.2,Win32 EXE PECompact compressed (generic),2.1,Win32 Executable (generic),1,Win16/32 Executable Delphi generic

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xb361c	0xb3800	6.35605820433	ad6e46e3a3acdb533eb6a077f6d065af
.itext	0xb5000	0x1688	0x1800	5.97275005522	d40fc822339d01f2abcc5493ac101c94
.data	0xb7000	0x37a4	0x3800	5.04440056201	4c195d5591f6d61265df08a3733de3a2
.bss	0xbb000	0x6de8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xc2000	0xf36	0x1000	4.89870464796	a73d686f1e8b9bb06ec767721135e397
.didata	0xc3000	0x1a4	0x200	2.75636286825	41b8ce23dd243d14beebc71771885c89
.edata	0xc4000	0x9a	0x200	1.87222286659	37c1a5c63717831863e018c0f51dabb7
.tls	0xc5000	0x18	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0xc6000	0x5d	0x200	1.38389437522	8f2f090acd9622c88a6a852e72f94e96
.rsrc	0xc7000	0x10e00	0x10e00	3.71027906881	4d3eb9b51e78d0ef50228de0de1cc7c7

PE Imports

- kernel32.dll
  - GetACP
  - GetExitCodeProcess
  - LocalFree
  - CloseHandle

- SizeofResource
- VirtualProtect
- VirtualFree
- GetFullPathNameW
- ExitProcess
- HeapAlloc
- GetCPInfoExW
- RtlUnwind
- GetCPInfo
- GetStdHandle
- GetModuleHandleW
- FreeLibrary
- HeapDestroy
- ReadFile
- CreateProcessW
- GetLastError
- GetModuleFileNameW
- SetLastError
- FindResourceW
- CreateThread
- CompareStringW
- LoadLibraryA
- ResetEvent
- GetVersion
- RaiseException
- FormatMessageW
- SwitchToThread
- GetExitCodeThread
- GetCurrentThread
- LoadLibraryExW
- LockResource
- GetCurrentThreadId
- UnhandledExceptionFilter
- VirtualQuery
- VirtualQueryEx
- Sleep
- EnterCriticalSection

- SetFilePointer
- LoadResource
- SuspendThread
- GetTickCount
- GetFileSize
- GetStartupInfoW
- GetFileAttributesW
- InitializeCriticalSection
- GetThreadPriority
- SetThreadPriority
- GetCurrentProcess
- VirtualAlloc
- GetSystemInfo
- GetCommandLineW
- LeaveCriticalSection
- GetProcAddress
- ResumeThread
- GetVersionExW
- VerifyVersionInfoW
- HeapCreate
- GetWindowsDirectoryW
- VerSetConditionMask
- GetDiskFreeSpaceW
- FindFirstFileW
- GetUserDefaultUILanguage
- lstrlenW
- QueryPerformanceCounter
- SetEndOfFile
- HeapFree
- WideCharToMultiByte
- FindClose
- MultiByteToWideChar
- LoadLibraryW
- SetEvent
- CreateFileW
- GetLocaleInfoW
- GetSystemDirectoryW

- DeleteFileW
- GetLocalTime
- GetEnvironmentVariableW
- WaitForSingleObject
- WriteFile
- ExitThread
- DeleteCriticalSection
- TlsGetValue
- GetDateFormatW
- SetErrorMode
- IsValidLocale
- TlsSetValue
- CreateDirectoryW
- GetSystemDefaultUILanguage
- EnumCalendarInfoW
- LocalAlloc
- GetUserDefaultLangID
- RemoveDirectoryW
- CreateEventW
- SetThreadLocale
- GetThreadLocale

comctl32.dll

- InitCommonControls

version.dll

- GetFileVersionInfoSizeW
- VerQueryValueW
- GetFileVersionInfoW

user32.dll

- CreateWindowExW
- TranslateMessage
- CharLowerBuffW
- CallWindowProcW
- CharUpperW
- PeekMessageW
- GetSystemMetrics
- SetWindowLongW

- MessageBoxW
- DestroyWindow
- CharUpperBuffW
- CharNextW
- MsgWaitForMultipleObjects
- LoadStringW
- ExitWindowsEx
- DispatchMessageW

oleaut32.dll

- SysAllocStringLen
- SafeArrayPtrOfIndex
- VariantCopy
- SafeArrayGetLBound
- SafeArrayGetUBound
- VariantInit
- VariantClear
- SysFreeString
- SysReAllocStringLen
- VariantChangeType
- SafeArrayCreate

netapi32.dll

- NetWkstaGetInfo
- NetApiBufferFree

advapi32.dll

- RegQueryValueExW
- AdjustTokenPrivileges
- LookupPrivilegeValueW
- RegCloseKey
- OpenProcessToken
- RegOpenKeyExW

PE Exports

- TMethodImplementationIntercept
- __dbk_fcall_wrapper
- dbkFCallWrapperAddr

PE Resources

[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]