VALKYRIE

PUA
Valkyrie Final Verdict

File Name: savsetupg_savsite-savsite.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 36198db866219c4b2384f4c277e5712fd47e5160
MD5: 1408f0b2710ab02ad12513b2f74005ea
First Seen Date: 2021-08-09 01:02:37 UTC
Number of Clients Seen: 3
Last Analysis Date: 2021-08-09 08:57:58 UTC
Human Expert Analysis Date: 2021-08-09 08:57:57 UTC
Human Expert Analysis Result: PUA
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2021-08-09 08:57:58 UTC	PUA	
Static Analysis Overall Verdict	2021-08-09 08:57:58 UTC	No Match	
Precise Detectors Overall Verdict	2021-08-09 08:57:58 UTC	No Match	
Human Expert Analysis Overall Verdict	2021-08-09 08:57:57 UTC	PUA	
File Certificate Validation		Not Applicable	

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2021-08-09 06:34:08 UTC
Analysis End Date: 2021-08-09 08:57:57 UTC
File Upload Date: 2021-08-09 01:01:51 UTC
Human Expert Analyst Feedback:
Verdict: PUA
Malware Family:
Malware Type: Pua

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5DA1B5ED [Sat Oct 12 11:15:57 2019 UTC]
Debug Artifacts	
Entry Point	0x4a7ed0 (.itext)
Exifinfo	[object Object]
File Size	26919960
File Type Enum	6
Imphash	eb5bc6ff6263b364dfbfb78bdb48ed59
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	Copyright \xa9 2021 Systweak Software, All rights reserved
File Version	1.0.1000.11042
Company Name	Systweak
Comments	This installation was built with Inno Setup.
Product Name	Systweak Antivirus
Product Version	1.0.1000.11042
File Description	Systweak Antivirus Setup
Original File Name	savsetupipg_.exe
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	10
Sha256	83b55eeedb8f18a848bb1c24d10122c11aeae094edb0a145196549d34fab06c4
Ssdeep	393216:u+u3xve24PCHDXiX/Bmpw7ZHjyFCR/d8FuF+dlvW+f5U1otxmgHI+xqF9:Hu3dejPCjXiX/YYHjy28Fg6+IS1oqF9
Trid	67.7,Inno Setup installer,25.6,Win32 EXE PECompact compressed (generic),2.7,Win32 Executable (generic),1.2,Win16/32 Executable Delphi generic,1.2,Generic Win/DOS Executable

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xa50e8	0xa5200	6.3692847538	f082ee6260fd65bd4406603aefa5b38a
.itext	0xa7000	0x1668	0x1800	5.95181064354	01fc0e6510748ac1fa24729bd4c8d31d
.data	0xa9000	0x37a4	0x3800	5.03516853901	34fa73ad8332bf3785e4314a4334a782
.bss	0xad000	0x6778	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xb4000	0xf1c	0x1000	4.79161091586	daddecfdccd86a491d85012d9e547c63
.didata	0xb5000	0x1a4	0x200	2.74582255367	be0581a07bd7d21a29f93f8752d3e826
.edata	0xb6000	0x9a	0x200	1.8810692045	c7a09d734ff63f677dfd4d18e3440fdf
.tls	0xb7000	0x18	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0xb8000	0x5d	0x200	1.37998812522	955f17d4899f3cf7664168fa46e1b316
.rsrc	0xb9000	0x6cc3c	0x6ce00	4.06182521966	45ba5dfc4f9d7eb8ef6f69af0ecf363f

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
- 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]