VALKYRIE

PUA
Valkyrie Final Verdict

File Name: 7USP3.exe
File Type: PE32+ executable (GUI) x86-64, for MS Windows
SHA1: f05f137ee24090f0cd45801b1d4aca5a7d804b91
MD5: e003cb91be593f2e20f6da8da55106ce
First Seen Date: 2025-05-23 23:49:17 UTC
Number of Clients Seen: 2
Last Analysis Date: 2025-05-24 19:02:10 UTC
Human Expert Analysis Date: 2025-05-24 19:02:05 UTC
Human Expert Analysis Result: PUA
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2025-05-24 19:02:10 UTC	PUA
Static Analysis Overall Verdict	2025-05-24 19:02:10 UTC	No Threat Found
Precise Detectors Overall Verdict	2025-05-24 19:02:10 UTC	No Match
Human Expert Analysis Overall Verdict	2025-05-24 19:02:05 UTC	PUA
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	Suspicious
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

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2025-05-23 23:48:57 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2025-05-23 23:48:57 UTC	No Match		NotDetected
Static Precise NI Detector 3	2025-05-23 23:48:57 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2025-05-23 23:48:57 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2025-05-23 23:48:57 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2025-05-23 23:48:57 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2025-05-23 23:48:57 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2025-05-23 23:48:57 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2025-05-23 23:48:58 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2025-05-23 23:48:58 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2025-05-23 23:48:58 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2025-05-23 23:48:58 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2025-05-24 14:46:58 UTC
Analysis End Date: 2025-05-24 19:02:05 UTC
File Upload Date: 2025-05-23 23:48:24 UTC
Human Expert Analyst Feedback: Application
Verdict: PUA
Malware Family: Application
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	0x50E0DEB7 [Mon Dec 31 00:39:19 2012 UTC]
Debug Artifacts	
Entry Point	0x14001f8d0 (.text)
Exifinfo	[object Object]
File Size	84013345
File Type Enum	7
Imphash	08fd62a9d05cc8111782017958ea975d
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
Magic Literal Enum	4
Legal Copyright	Copyright \xa9 2024 Tech Stuff (@teknixstuff)
Internal Name	VistaUpdateMegafix
File Version	1.0.0.0
Company Name	Tech Stuff (@teknixstuff)
Private Build	v1 (12th Aug 2024)
Product Name	Unofficial WIndows Vista Service Pack 3
Product Version	1.0.0.0
File Description	Unofficial Windows Vista Service Pack 3
Original Filename	VistaUSP3.exe
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	33c9e8d8541cd9509637df966c94d1cb6ba0c524fdcb7358a820768c65dfe522
Ssdeep	1572864:MkJA0pSEA/vBzWmXx26LiXH/96Rc13gvIiTvFeiYZ6TKST+cfODIoDAg:xJ/pSF/v4mXH8fIRc1sVvKw+4noD
Trid	50,Generic Win/DOS Executable,49.9,DOS Executable Generic

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1efae	0x1f000	6.35563921643	6afaf2492621789cd6fb21ade3845d96
.rdata	0x20000	0x5b1c	0x5c00	5.18604756129	cf5a47e92a71d40addce827c8954ed5e
.data	0x26000	0x5268	0xe00	3.58541033666	2893ed32149e4a1ba6ea25e4100062ed
.pdata	0x2c000	0x1a94	0x1c00	5.05741179711	d97bb8a82df9a86a40dc5ee58d4f426a
.rsrc	0x2e000	0x1464d	0x14800	7.43474825054	8af4f8ee1bb94bb4121729b09528326b