VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: LibreWolf-WinUpdater_1.exe
File Type: PE32+ executable (GUI) x86-64, for MS Windows
SHA1: 311f0938c3a0a5327b6a28491c7c560d1220a670
MD5: 2abb3b02e7da9fa55e9d3e49ea3d58fd
First Seen Date: 2022-01-29 18:19:21 UTC
Number of Clients Seen: 2
Last Analysis Date: 2022-01-29 18:19:21 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 02:02:03 UTC	Clean
Static Analysis Overall Verdict	2022-01-29 18:19:21 UTC	No Threat Found
Precise Detectors Overall Verdict	2022-01-29 18:19:21 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	Suspicious
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

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise PUA Detector 1	2022-01-29 18:19:13 UTC	No Match	NotDetected
Static Precise PUA Detector 4	2022-01-29 18:19:13 UTC	No Match	NotDetected
Static Precise NI Detector 3	2022-01-29 18:19:13 UTC	No Match	NotDetected
Static Precise PUA Detector 5	2022-01-29 18:19:13 UTC	No Match	NotDetected
Static Precise Trojan Detector 1	2022-01-29 18:19:13 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2022-01-29 18:19:13 UTC	No Match	NotDetected
Static Precise PUA Detector 6	2022-01-29 18:19:13 UTC	No Match	NotDetected
Static Precise Trojan Detector 12	2022-01-29 18:19:13 UTC	No Match	NotDetected
Static Precise Virus Detector 1	2022-01-29 18:19:13 UTC	No Match	NotDetected
Static Precise Virus Detector 2	2022-01-29 18:19:13 UTC	No Match	NotDetected
Static Precise Trojan Detector 13	2022-01-29 18:19:13 UTC	No Match	NotDetected
Static Precise PUA Detector 2	2022-01-29 18:19:13 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	0x612ACE11 [Sun Aug 29 00:00:17 2021 UTC]
Debug Artifacts	
Entry Point	0x1400cc550 (.text)
Exifinfo	[object Object]
File Size	1236480
File Type Enum	7
Imphash	2004a5f6f543f8c26e144c1ceb66f943
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
Magic Literal Enum	4
Legal Copyright	
Internal Name	
File Version	1.1.0
Product Name	
Product Version	1.1.33.10
File Description	LibreWolf WinUpdater
Original Filename	
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	7
Sha256	113221a890b027bc8df9b79691ee7c66d5e1ad05ba13b2312f66f1f1760c892e
Ssdeep	24576:QjdvkUZ0pDZe+Bczu3+ZO0IRR3wTkgr9BNpiUU11Wsp1Igj20wq2Vd:QjdvkY0pDZe+Bczu3+ZO0IRR3eFr9B/i
Trid	87.3,Win64 Executable (generic),6.3,Generic Win/DOS Executable,6.3,DOS Executable Generic

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xdcc06	0xdce00	6.54242716511	a717d880a5590abfb7764852fd4d19eb
.rdata	0xde000	0x30e86	0x31000	4.98365760232	5781b7664a5d2b5105f5749ccc4e6fe4
.data	0x10f000	0xc3c8	0x5000	3.33355081441	233c9071e6709b885cb8b57f11f22958
.pdata	0x11c000	0x78b4	0x7a00	5.99412607849	6ec777258442d33c04809fda2f06a8b8
text	0x124000	0x258d	0x2600	5.77638092432	648bb61ffda80e1d555e32a70474e814
data	0x127000	0x6ec0	0x7000	6.45735927966	8f4275b626558a8640120f611553e570
.rsrc	0x12e000	0x9ab8	0x9c00	3.82551788146	02bac8906e104028ce432f8138cc4d33