VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: AutoItObfuscator.bin
File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1: 1e3cdd96256751266bcea6aa44c227717bcc167d
MD5: 08e41d1adef4d5ec6caa8cb2c02b3246
First Seen Date: 2022-01-10 18:33:29 UTC
Number of Clients Seen: 4
Last Analysis Date: 2022-01-10 18:33:29 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	2022-01-10 19:24:41 UTC	Malware
Static Analysis Overall Verdict	2022-01-10 18:33:29 UTC	No Threat Found
Precise Detectors Overall Verdict	2022-01-10 18:33:29 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	Suspicious
Illegal size of optional Header	Clean
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	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	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	2022-01-10 18:33:23 UTC	No Match	NotDetected
Static Precise PUA Detector 4	2022-01-10 18:33:23 UTC	No Match	NotDetected
Static Precise NI Detector 3	2022-01-10 18:33:23 UTC	No Match	NotDetected
Static Precise PUA Detector 5	2022-01-10 18:33:23 UTC	No Match	NotDetected
Static Precise Trojan Detector 1	2022-01-10 18:33:23 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2022-01-10 18:33:23 UTC	No Match	NotDetected
Static Precise PUA Detector 6	2022-01-10 18:33:23 UTC	No Match	NotDetected
Static Precise Trojan Detector 12	2022-01-10 18:33:24 UTC	No Match	NotDetected
Static Precise Virus Detector 1	2022-01-10 18:33:24 UTC	No Match	NotDetected
Static Precise Virus Detector 2	2022-01-10 18:33:24 UTC	No Match	NotDetected
Static Precise Trojan Detector 13	2022-01-10 18:33:24 UTC	No Match	NotDetected
Static Precise PUA Detector 2	2022-01-10 18:33:24 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	0x5CCAE30D [Thu May 2 12:31:09 2019 UTC]
Debug Artifacts	
Entry Point	0x63000a ()
Exifinfo	[object Object]
File Size	2281488
File Type Enum	6
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Translation	0x0000 0x04b0
Legal Copyright	Copyright \xa9 PELock LLC 2019
Assembly Version	1.4.0.0
Internal Name	AutoItObfuscator.exe
File Version	1.4.0.0
Company Name	PELock LLC
Legal Trademarks	
Comments	AutoIt Script Source Code Obfuscator
Product Name	AutoItObfuscator
Product Version	1.4.0.0
File Description	AutoIt Obfuscator
Original Filename	AutoItObfuscator.exe
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	1a3e4540c7866fec573e3602a3dcfc3919eccf9c3665ea764ea9896b4b96dd53
Ssdeep	49152:OWyGPyVO2/9wiuZ29ziGy+Icmj6fiCoAjeNAMWM:2VO2CZZ29Nyvcmj6BoaeNz
Trid	64.5,Win32 Executable MS Visual C++ (generic),13.6,Win32 Dynamic Link Library (generic),9.3,Win32 Executable (generic),4.2,Win16/32 Executable Delphi generic,4.1,Generic Win/DOS Executable

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
7x<]	0x2000	0x5b8c	0x5c00	7.99295996007	4a2e92f12d9afb35c557bb4fb1dad400
.text	0x8000	0x20dcb0	0x20de00	7.82505639958	f52fbb0d570a32b643e4ce92144276db
?f{4tiJ	0x216000	0x18d28	0x18e00	3.65719521658	2b0236e13f08eb704d28d0930d7b2d8e
	0x230000	0x10	0x200	0.101910425663	4e639fd7e16d317733bc02bf2a1ad7be
.reloc	0x232000	0xc	0x200	0.0776331623432	70ae9e8741e9a18e39dad858850b57c6