VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: None
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 43ee5c9c3970b48f2fe82c3ab3c6dcf1b1de1b07
MD5: 20127c15e4a153322c63a734aebf7513
First Seen Date: 2019-08-04 05:19:17 UTC
Number of Clients Seen: 26
Last Analysis Date: 2024-10-13 00:02:42 UTC
Human Expert Analysis Date: 2019-08-04 11:48:44 UTC
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2024-10-13 00:02:42 UTC	Clean	
Static Analysis Overall Verdict	2024-10-13 00:02:42 UTC	No Threat Found	
Precise Detectors Overall Verdict	2024-10-13 00:02:42 UTC	No Match	
Human Expert Analysis Overall Verdict	2019-08-04 11:48:44 UTC	Clean	
File Certificate Validation		Vendor not found in Trusted List	

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	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	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	2024-10-13 00:02:39 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2024-10-13 00:02:39 UTC	No Match		NotDetected
Static Precise NI Detector 3	2024-10-13 00:02:39 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2024-10-13 00:02:39 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2024-10-13 00:02:39 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2024-10-13 00:02:39 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2024-10-13 00:02:39 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2024-10-13 00:02:39 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2024-10-13 00:02:39 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2024-10-13 00:02:39 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2024-10-13 00:02:39 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2024-10-13 00:02:39 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2019-08-04 09:00:37 UTC
Analysis End Date: 2019-08-04 11:48:44 UTC
File Upload Date: 2019-08-04 04:58:24 UTC
Human Expert Analyst Feedback: None
Verdict: Clean

Additional File Information

Vendor Validation - Not Verified ✖

[+] Restoro Ltd.

Status	Not Valid ✖

Certificate Validation - Success ✔

[+] Thawte Timestamping CA

Status	NoError ✔
Start Date	1997-01-01 02:00:00
End Date	2021-01-01 01:59:59
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Name	Thawte Timestamping CA
Subject Key Identifier	null
Subject Organization	Thawte
Subject Locality	Durbanville
Subject State	Western Cape
Subject Country	ZA
Subject Organizational Unit	Thawte Certification
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	null
Issuer Organization	Thawte
Issuer Locality	Durbanville
Issuer State	Western Cape
Issuer Country	ZA
Issuer Organizational Unit	Thawte Certification
Crl link	null
Key Usage	null
Extended Usage	null

[+] Symantec Time Stamping Services CA - G2

Status	NoError ✔
Start Date	2012-12-21 02:00:00
End Date	2020-12-31 01:59:59
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Name	Symantec Time Stamping Services CA - G2
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db ec 4c 80 2e dd
Subject Organization	Symantec Corporation
Subject Country	US
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	null
Issuer Organization	Thawte
Issuer Locality	Durbanville
Issuer State	Western Cape
Issuer Country	ZA
Issuer Organizational Unit	Thawte Certification
Crl link	http://crl.thawte.com/ThawteTimestampingCA.crl
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	{"Time Stamping (1.3.6.1.5.5.7.3.8)"}

[+] VeriSign Class 3 Public Primary Certification Authority - G5

Status	NoError ✔
Start Date	2006-11-08 02:00:00
End Date	2036-07-17 02:59:59
Sha256	d0c133d98cabb2199501a761f5b8b9afd30d870477a534b41400a6dc57f5d64d
Serial	18DAD19E267DE8BB4A2158CDCC6B3B4A
Subject Name	VeriSign Class 3 Public Primary Certification Authority - G5
Subject Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Subject Organization	VeriSign, Inc.
Subject Country	US
Subject Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	null
Issuer Organization	VeriSign, Inc.
Issuer Country	US
Issuer Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Crl link	null
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	null

[+] Symantec Class 3 SHA256 Code Signing CA

Status	NoError ✔
Start Date	2013-12-10 02:00:00
End Date	2023-12-10 01:59:59
Sha256	0649cde463467e8e26bb6b7c23965e030248f95df21f6dcf28c51507fbb77c08
Serial	3D78D7F9764960B2617DF4F01ECA862A
Subject Name	Symantec Class 3 SHA256 Code Signing CA
Subject Key Identifier	96 3b 53 f0 79 33 97 af 7d 83 ef 2e 2b cc ca b7 86 1e 72 66
Subject Organization	Symantec Corporation
Subject Country	US
Subject Organizational Unit	Symantec Trust Network
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Issuer Organization	VeriSign, Inc.
Issuer Country	US
Issuer Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Crl link	http://s1.symcb.com/pca3-g5.crl
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	{"Client Authentication (1.3.6.1.5.5.7.3.2)"}

[+] Restoro Ltd.

Status	NoError ✔
Start Date	2019-03-05 02:00:00
End Date	2020-03-05 01:59:59
Sha256	23dc54ac0bacfbc1e1ba7cc4f27f1fab2b72a371904d778eea400c656307d8f7
Serial	0D5654882171 37EE9C7ACEA4002FD68B
Subject Name	Restoro Ltd.
Subject Key Identifier	4e a1 ca 64 dd 8a fe 45 9b 1e 92 35 5a db 72 a8 45 33 31 52
Subject Organization	Restoro Ltd.
Subject Locality	Douglas
Subject Country	IM
Subject Organizational Unit	Restoro Ltd.
Issuer Name	Symantec Class 3 SHA256 Code Signing CA
Issuer Key Identifier	96 3b 53 f0 79 33 97 af 7d 83 ef 2e 2b cc ca b7 86 1e 72 66
Issuer Organization	Symantec Corporation
Issuer Country	US
Issuer Organizational Unit	Symantec Trust Network
Crl link	http://sv.symcb.com/sv.crl
Key Usage	{"Digital Signature (80)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x4F47E2DF [Fri Feb 24 19:19:59 2012 UTC]
Debug Artifacts	
Entry Point	0x4039e3 (.text)
Exifinfo	[object Object]
File Size	935168
File Type Enum	6
Imphash	32f3282581436269b3a75b6675fe3e08
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	\xa9 Restoro 2019
Internal Name	Restoro Downloader
File Version	2.016
Company Name	Restoro
Legal Trademarks	Restoro
Product Name	Restoro
Product Version	2.016
File Description	Restoro Downloader
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	6
Sha256	951ed0a81277e09e0416174c970fcdbed93745c9993d0fc649d576872d3c75a9
Ssdeep	12288:REVLcMwpsGcDdHCfKbQTiHmHGluO0Q9zY8cEtDcZeOc2oVWX:RucLyNCClsO0Q97Xmep4
Trid	42.2,Win32 Executable MS Visual C++ (generic),37.3,Win64 Executable (generic),8.8,Win32 Dynamic Link Library (generic),6,Win32 Executable (generic),2.7,Generic Win/DOS Executable

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x6f10	0x7000	6.49788465186	f569e353af0ed51bf4c216faa9bed4e7
.rdata	0x8000	0x2a92	0x2c00	4.39389365097	91eee43954e068e650f7b73a8b0e6915
.data	0xb000	0x67ebc	0x200	1.472782261	db9f7acbf1c3ddfe255077b699955dfa
.ndata	0x73000	0x339000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x3ac000	0x4bfe9	0x4c000	4.92448718034	6d955beda33ddd993629bba1ad41c7b4
.reloc	0x3f8000	0xf8a	0x1000	3.23379612354	f4ad22215006a677ade6a73cdeab789f