VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: SUMo.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: f2e0c529875cc119d562ef5436cb99e5e4234118
MD5: e2b451474883baf4d56da619ded26ac7
First Seen Date: 2017-09-23 15:22:41 UTC
Number of Clients Seen: 3
Last Analysis Date: 2017-09-23 17:19:59 UTC
Human Expert Analysis Date: 2017-09-23 20:25:50 UTC
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2017-09-23 17:19:59 UTC	Clean	✓
Static Analysis Overall Verdict	2017-09-23 17:19:59 UTC	No Threat Found	?
Precise Detectors Overall Verdict	2017-09-23 17:19:59 UTC	No Match	?
Human Expert Analysis Overall Verdict	2017-09-23 20:25:50 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	Suspicious	!
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 Trojan Detector 2	2017-09-23 17:19:43 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2017-09-23 17:19:43 UTC	No Match		NotDetected
Static Precise Adware InstallCore Detector 1	2017-09-23 17:19:43 UTC	No Match		NotDetected
Static Precise Trojan Generic Cryptor Detector 1	2017-09-23 17:19:43 UTC	No Match		NotDetected
Static Precise PUA Detector 1	2017-09-23 17:19:43 UTC	No Match		NotDetected
Static Precise Virus Detector	2017-09-23 17:19:43 UTC	No Match		NotDetected
Static Precise Trojan Detector	2017-09-23 17:19:43 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2017-09-23 17:19:43 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2017-09-23 17:38:40 UTC
Analysis End Date: 2017-09-23 20:25:50 UTC
File Upload Date: 2017-09-23 17:19:35 UTC
Human Expert Analyst Feedback:
Verdict: Clean

Additional File Information

Vendor Validation - Not Verified ✖

[+] KC Softwares

Status	Not Valid ✖

Certificate Validation - Success ✔

[+] Thawte Timestamping CA

Status	NoError ✔
Start Date	1997-01-01 00:00:00
End Date	2020-12-31 23:59:59
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 00:00:00
End Date	2020-12-30 23:59:59
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)"}

[+] COMODO RSA Certification Authority

Status	NoError ✔
Start Date	2010-01-19 00:00:00
End Date	2038-01-18 23:59:59
Sha256	f1bc8293a80c7d1bb2fd1d6e9b714b06e6b66686ca9b26a76d91e06e2934fa83
Serial	4CAAF9CADB636FE01FF74ED85B03869D
Subject Name	COMODO RSA Certification Authority
Subject Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Subject Organization	COMODO CA Limited
Subject Locality	Salford
Subject State	Greater Manchester
Subject Country	GB
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	null
Issuer Organization	COMODO CA Limited
Issuer Locality	Salford
Issuer State	Greater Manchester
Issuer Country	GB
Crl link	null
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	null

[+] COMODO RSA Code Signing CA

Status	NoError ✔
Start Date	2013-05-09 00:00:00
End Date	2028-05-08 23:59:59
Sha256	be4b37864cefc39611d4b6a1de110074e5f282de90016aa5d36849ab452eab2c
Serial	2E7C87CC0E934A52FE94FD1CB7CD34AF
Subject Name	COMODO RSA Code Signing CA
Subject Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Subject Organization	COMODO CA Limited
Subject Locality	Salford
Subject State	Greater Manchester
Subject Country	GB
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Issuer Organization	COMODO CA Limited
Issuer Locality	Salford
Issuer State	Greater Manchester
Issuer Country	GB
Crl link	http://crl.comodoca.com/COMODORSACertificationAuthority.crl
Key Usage	{"Digital Signature","Certificate Signing","Off-line CRL Signing","CRL Signing (86)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

[+] KC Softwares

Status	NoError ✔
Start Date	2015-05-05 00:00:00
End Date	2018-05-04 23:59:59
Sha256	c3293a10c8cfa4d259cc9846340fe433e1dc76c30e41292eb47c64bb1430df82
Serial	12A9F5D7A3247BAD09F6DCFF84BA497C
Subject Name	KC Softwares
Subject Key Identifier	e9 95 93 13 3a 1a b0 47 bb 8c ac 50 3c 59 63 23 01 1b 92 8e
Subject Organization	KC Softwares
Subject Locality	Auterive
Subject State	Outside United States
Subject Country	FR
Subject Organizational Unit	KC Softwares
Issuer Name	COMODO RSA Code Signing CA
Issuer Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Issuer Organization	COMODO CA Limited
Issuer Locality	Salford
Issuer State	Greater Manchester
Issuer Country	GB
Crl link	http://crl.comodoca.com/COMODORSACodeSigningCA.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	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
Entry Point	0x534864 (CODE)
File Size	2029240
File Type Enum	6
Machine Type	Intel 386 or later - 32Bit
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	7b4a48448d539f92d484871c6005ccbe3715929772b1f52f63c054e3d543313b

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x1339c8	0x133a00	6.54656375734	6382ddd7ca71ecabfa9b5284061c2e08
DATA	0x135000	0xf5ac	0xf600	2.6792435038	e180fb9e507ca10cb4a8f14e31e5da28
BSS	0x145000	0x3501	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0x149000	0x2efc	0x3000	5.01232006693	2d7e7957f942e0f2e8f77913d9bdf983
.tls	0x14c000	0x12	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x14d000	0x18	0x200	0.210826267787	7858ff81700bdf197371a974b611fd7c
.reloc	0x14e000	0x14698	0x14800	6.6919949569	d4b2767168dfd3b5aa034674ad840e26
.rsrc	0x163000	0x93000	0x93000	5.20079146816	3a2204a13265905842324afa0709927b