



MALWARE
Valkyrie Final Verdict

File Name: Realtek-FORCED-7x64-1.3.893-drp.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 2929f28146763c63ac14f1cc7cae7d6b43e63f92
MD5: 1421e33d77a71bf2cf373c2e85b35381
First Seen Date: 2017-06-12 23:42:56 UTC
Number of Clients Seen: 4
Last Analysis Date: 2017-06-12 23:42:56 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	2017-06-12 23:42:56 UTC	Malware	!
Static Analysis Overall Verdict	2017-06-12 23:42:56 UTC	No Threat Found	?
Precise Detectors Overall Verdict	2017-06-12 23:42:56 UTC	No Match	?
File Certificate Validation		Certificate and Vendor name are Valid	✓

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	✓
Entry 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	✓

▼ Packer detection on signature database

- Armadillo v1.71
- Microsoft Visual C++ v5.0/v6.0 (MFC)
- Microsoft Visual C++

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Uninstaller FP Detector	2017-06-12 23:42:39 UTC	No Match	?	No match.
Yara Rule Static Malware Detector	2017-06-12 23:42:39 UTC	No Match	?	No match.
Static Precise PUA Detector 1	2017-06-12 23:42:39 UTC	No Match	?	NotDetected
Static Precise Virus Detector	2017-06-12 23:42:39 UTC	No Match	?	NotDetected
Static Precise Trojan Detector	2017-06-12 23:42:39 UTC	No Match	?	NotDetected
Malicious Url Detector	2017-06-12 23:42:56 UTC	No Match	?	No match.

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Verified ✓

[+] Kuzyakov Artur Vyacheslavovich IP

Status

Valid ✓

Certificate Validation - Success ✓

[+] Kuzyakov Artur Vyacheslavovich IP

Status	NoError 
Start Date	2016-09-22 00:00:00+00:00
End Date	2017-09-22 23:59:59+00:00
Sha256	5911d9e094880408bb079e29af11f983d1ed8541e2b5e76672b5548b27492c0d
Serial	7994EBFBBB0DCCE61C0A286CFEA1A439
Subject Name	Kuzyakov Artur Vyacheslavovich IP
Subject Key Identifier	56 46 03 18 6c 48 c9 12 fc e6 53 e0 8d 81 83 fe 96 f7 0a 96
Subject Organization	Kuzyakov Artur Vyacheslavovich IP
Subject Locality	Moscow
Subject State	Moscow
Subject Country	RU
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)

[+] COMODO RSA Code Signing CA

Status	NoError 
Start Date	2013-05-09 00:00:00+00:00
End Date	2028-05-08 23:59:59+00:00
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)

[+] COMODO RSA Certification Authority

Status	NoError 
Start Date	2010-01-19 00:00:00+00:00
End Date	2038-01-18 23:59:59+00:00
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	undefined
Issuer Organization	COMODO CA Limited
Issuer Locality	Salford
Issuer State	Greater Manchester
Issuer Country	GB
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

[+] Symantec Time Stamping Services CA - G2

Status	NoError 
Start Date	2012-12-21 00:00:00+00:00
End Date	2020-12-30 23:59:59+00:00
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	undefined
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)

[+] Thawte Timestamping CA

Status	NoError 
Start Date	1997-01-01 00:00:00+00:00
End Date	2020-12-31 23:59:59+00:00
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Name	Thawte Timestamping CA
Subject Key Identifier	undefined
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	undefined
Issuer Organization	Thawte
Issuer Locality	Durbanville
Issuer State	Western Cape
Issuer Country	ZA
Issuer Organizational Unit	Thawte Certification
Crl link	undefined
Key Usage	undefined
Extended Usage	undefined

 PE Headers		▼
PROPERTY	VALUE	
Compilation Time Stamp	0x5700444A [Sat Apr 2 22:14:34 2016 UTC]	
Entry Point	0x41c35f (.text)	
File Size	2338176	
Machine Type	Intel 386 or later - 32Bit	
Legal Copyright	Copyright \xa9 Kuzyakov Artur	
Internal Name	DriverPack	
File Version	1.0	
Company Name	DriverPack	
Private Build	2016	
Product Name	DriverPack	
Product Version	1.0	
File Description	DriverPack	
Original Filename	DriverPack.exe	
Translation	0x0000 0x04b0	
Mime Type	application/x-dosexec	
Number Of Sections	4	
Sha256	af90873d6e59034ff7bfa6f7099999abaf8b90929e48174ab9f8c7be4c0ece7e	

 PE Sections		▼

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1bd4a	0x1be00	6.71052533174	c820c58aedd8916d0cfdfacf6518a796
.rdata	0x1d000	0x41a8	0x4200	5.74601891947	61e5f1569be02d293c2f1941c8014c11
.data	0x22000	0x4c90	0x800	3.69661077531	df838379d053bbc0adb49e5333be876c
.rsrc	0x27000	0x6b0d	0x6c00	5.00686276495	0cb7e88d18950e1d06a7c50e4e98b81d