VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: CCleaner64.exe
File Type: PE32+ executable (GUI) x86-64, for MS Windows
SHA1: 92fcff26e8c5f8238c2b7f1c025289c20168c9c2
MD5: e6f5ad3fd6d0f64ec88357fc481a71ab
First Seen Date: 2017-09-20 16:09:28 UTC
Number of Clients Seen: 152
Last Analysis Date: 2018-05-22 09:27:11 UTC
Human Expert Analysis Date: 2017-09-20 18:31:05 UTC
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2018-05-22 09:27:11 UTC	Clean	✓
Static Analysis Overall Verdict	2018-05-22 09:27:11 UTC	No Threat Found	?
Precise Detectors Overall Verdict	2018-05-22 09:27:11 UTC	No Match	?
Human Expert Analysis Overall Verdict	2017-09-20 18:31:05 UTC	Clean	✓
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	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	Suspicious	!
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean	✓
TLS callback functions array detected	Clean	✓

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS
No suspicious activity found

Behavioral Information

QueryFilePath

C:\Windows\SysWOW64\rundll32.exe

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2018-05-22 09:27:01 UTC	No Match		NotDetected
Static Precise Trojan Detector 5	2018-05-22 09:27:01 UTC	No Match		NotDetected
Static Precise Trojan Detector 7	2018-05-22 09:27:01 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2018-05-22 09:27:01 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2018-05-22 09:27:01 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2018-05-22 09:27:01 UTC	No Match		NotDetected
Static Precise Trojan Detector 2	2018-05-22 09:27:01 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2018-05-22 09:27:01 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2018-05-22 09:27:01 UTC	No Match		NotDetected
Static Precise Trojan Detector 10	2018-05-22 09:27:01 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2018-05-22 09:27:01 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2018-05-22 09:27:01 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2017-09-20 18:23:11 UTC
Analysis End Date: 2017-09-20 18:31:05 UTC
File Upload Date: 2017-09-20 16:07:34 UTC
Human Expert Analyst Feedback:
Verdict: Clean

Additional File Information

Vendor Validation - Verified

[+] Piriform Ltd

Status	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)"}

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

Status	NoError ✔
Start Date	2006-11-08 00:00:00
End Date	2036-07-16 23:59:59
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 00:00:00
End Date	2023-12-09 23:59:59
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)"}

[+] Piriform Ltd

Status	NoError ✔
Start Date	2017-09-20 00:00:00
End Date	2018-10-11 23:59:59
Sha256	74f78ffc55e0a6d206f80635bb11b000c0a63d60b0f4f0f091edab081c080b31
Serial	52B6A81474E8048920F1909E454D7FC0
Subject Name	Piriform Ltd
Subject Key Identifier	0b ff 86 e7 b2 4b 9a 29 e2 f3 d4 04 84 db fa e0 74 d2 97 71
Subject Organization	Piriform Ltd
Subject Locality	London
Subject Country	GB
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	0x59B179BA [Thu Sep 7 16:54:18 2017 UTC]
Debug Artifacts	[object Object]
Entry Point	0x140135658 (.text)
Exifinfo	[object Object]
File Size	9856176
File Type Enum	7
Imphash	3d8d8cb7da976dfd16394d71a00597df
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
Magic Literal Enum	4
Legal Copyright	Copyright \xa9 2005-2017 Piriform Ltd
Internal Name	ccleaner
File Version	5, 35, 0, 6210
Company Name	Piriform Ltd
Comments	CCleaner
Product Name	CCleaner
Product Version	5, 35, 0, 6210
File Description	CCleaner
Original Filename	ccleaner.exe
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	06b27f68366f8d25a599c3ad8b1d23f18158f4edddee3174a22d3698089a8bc3
Ssdeep	98304:oyP0IJH7MZu9z8oKD8pqS59yA7PwB6zcSoPGct/htjKjfB:N0IJH7QYAoKggW97Pw0E9/KF
Trid	69.9,Windows ActiveX control,24.9,Win32 EXE PECompact compressed (generic),2.7,Win32 Executable (generic),1.2,Generic Win/DOS Executable,1.2,DOS Executable Generic

File Paths

FILE PATH ON CLIENT	SEEN COUNT
C:\Program Files\CCleaner\CCleaner64.exe	8
C: \Program Files\CCleaner\CCleaner64.exe	8
C:\VTRoot\HarddiskVolume3\Program Files\CCleaner\CCleaner64.exe	8
C:\clanto\ccleaner\CCleaner64.exe	8
C:\Program Files (x86)\CCleaner\CCleaner64.exe	8
C:\Users\szasz\Desktop\narzedzia\ccsetup535\CCleaner64.exe	8
C:\VTRoot\HarddiskVolume4\Program Files\CCleaner\CCleaner64.exe	8
C:\VTRoot\HarddiskVolume2\Program Files\CCleaner\CCleaner64.exe	8

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x4735e6	0x473600	6.40759378602	8748de62cc907747a6168c5c1b926209
.rdata	0x475000	0x1c1a0a	0x1c1c00	4.60519706926	4ddb503e6e9886a031bc5b66ed867652
.data	0x637000	0x26549c	0x5ea00	3.55285773254	d753aee745c68530be5af0caa4616867
.pdata	0x89d000	0x37284	0x37400	6.48104455688	808c9a8d120f615cfc7ded855d3b33c4
.gfids	0x8d5000	0x1178	0x1200	4.05665988053	59d95ba535aaafa453cec3243f785685
.tls	0x8d7000	0x9	0x200	0.0203931352361	1f354d76203061bfdd5a53dae48d5435
.rsrc	0x8d8000	0x287f80	0x288000	6.80023094884	11144d7b1b6c569820d0c451267515dd
.reloc	0xb60000	0xe5d0	0xe600	5.45847940217	40cdf87abe0e9ea7ebaa3bdf0f60fdd3