VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: ccsetup538_slim.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 38f9967c5a21f81990904141026709d508784864
MD5: d66808d43ec486a190136bd19169f277
First Seen Date: 2017-12-19 20:29:45 UTC
Number of Clients Seen: 7
Last Analysis Date: 2017-12-19 20:29:45 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	2017-12-19 20:29:45 UTC	Clean	
Static Analysis Overall Verdict	2017-12-19 20:29:45 UTC	No Threat Found	
Precise Detectors Overall Verdict	2017-12-19 20:29:45 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	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

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Opens a file in a system directory	!
Uses a function clandestinely	!

Behavioral Information

LoadLibrary

C:\Windows\system32\UXTHEME
C:\Windows\system32\USERENV
C:\Windows\system32\SETUPAPI
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
advapi32.dll
C:\Windows\system32\SHFOLDER
ole32.dll
comctl32.dll
ADVAPI32.dll
SHELL32.dll
propsys.dll
ntmarta.dll
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\System.dll
UxTheme.dll
C:\Windows\system32\ole32.dll
C:\Windows\syswow64\MSCTF.dll
OLEAUT32.DLL
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\p\pfBL
CRYPTSP.dll
CRYPTBASE.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
OLEAUT32.dll
C:\Windows\system32\RichEd20
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\ButtonEvent.dll
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\nsDialogs.dll
IMM32.dll
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\nsProcess.dll
NTDLL.DLL
C:\Program Files\CCleaner\CCleaner.exe
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\inetc.dll
Secur32.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
WS2_32.dll
winhttp.dll
wininet.dll
IPHLPAPI.DLL
api-ms-win-downlevel-shlwapi-l2-1-0.dll
DNSAPI.dll
dhcpcsvc.DLL

CreateMutex

<NULL>

DeleteFile

C:\Users\win7\AppData\Local\Temp\nsgA3DA.tmp
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp

OpenMutex

Local\MSCTF.Asm.MutexDefault1

WriteFile

C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\ButtonEvent.dll
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\p\pfBL.dll
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\nsProcess.dll
C:\Windows\Fonts\staticcache.dat
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\modern-wizard.bmp
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsbA40A.tmp
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\inetc.dll
C:\Users\win7\AppData\Local\Temp\nsgA42A.tmp\modern-header.bmp

ReadFile

C:\ccsetup538_slim.exe
C:\Users\win7\AppData\Local\Temp\nsbA40A.tmp
C:\Windows\Fonts\staticcache.dat

QueryFilePath

C:\ccsetup538_slim.exe
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\system32\RichEd20.DLL

OpenRegistryKey

HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
HKEY_CURRENT_USERSoftware\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_CURRENT_USERSOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
HKEY_CURRENT_USERSoftware\Piriform\CCleaner
HKEY_LOCAL_MACHINESoftware\Policies\Microsoft\Internet Explorer\Main
HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINESYSTEM\CurrentControlSet\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}\{CFE68B1E-656A-488B-8077-738CA67BA3A5}\Connection
HKEY_LOCAL_MACHINESoftware\Policies\Microsoft\Internet Explorer
HKEY_LOCAL_MACHINESoftware
HKEY_CURRENT_USERSoftware\Policies
HKEY_LOCAL_MACHINESOFTWARE\CCleaner
HKEY_LOCAL_MACHINESoftware\Microsoft\Internet Explorer\Main
HKEY_CURRENT_USERSoftware\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINESoftware\Policies\Microsoft\PeerDist\Service
HKEY_CURRENT_USERSOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
HKEY_CURRENT_USERSoftware\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINESOFTWARE\Piriform\CCleaner
HKEY_LOCAL_MACHINESoftware\Microsoft\Windows NT\CurrentVersion\PeerDist\Service
HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINESystem\Setup
HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_CURRENT_USERSoftware
HKEY_CURRENT_USERSoftware\Policies\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_CURRENT_USERSoftware\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
HKEY_LOCAL_MACHINESoftware\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
HKEY_LOCAL_MACHINESoftware\Policies\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_LOCAL_MACHINESoftware\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINESOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
HKEY_LOCAL_MACHINESoftware\Policies
HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINESoftware\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_CURRENT_USERSoftware\Microsoft\Internet Explorer\Main
HKEY_LOCAL_MACHINESoftware\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINESoftware\Microsoft\Windows\CurrentVersion
HKEY_CURRENT_USERSoftware\Policies\Microsoft\Internet Explorer\Main
HKEY_LOCAL_MACHINESoftware\Microsoft\WBEM\CIMOM

CreateRegistryKey

HKEY_CURRENT_USERSoftware\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
HKEY_CURRENT_USERSOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_CURRENT_USERSoftware\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_CURRENT_USERSoftware\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2017-12-19 20:28:26 UTC	No Match	?	NotDetected
Static Precise Virus Detector	2017-12-19 20:28:26 UTC	No Match	?	NotDetected
Static Precise Trojan Detector	2017-12-19 20:28:26 UTC	No Match	?	NotDetected
Static Precise Adware InstallCore Detector 1	2017-12-19 20:28:26 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 2	2017-12-19 20:28:26 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 3	2017-12-19 20:28:26 UTC	No Match	?	NotDetected
Static Precise Trojan Generic Cryptor Detector 1	2017-12-19 20:28:26 UTC	No Match	?	NotDetected
Static Precise Virus Detector 2	2017-12-19 20:28:26 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	0x5682FC79 [Tue Dec 29 21:34:49 2015 UTC]
Debug Artifacts	
Entry Point	0x403a1c (.text)
Exifinfo	[object Object]
File Size	8344776
File Type Enum	6
Imphash	377a97652fdf5740d8cc11d5ce124fed
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	Copyright \xa9 2005-2017 Piriform Ltd
Product Name	CCleaner
File Description	CCleaner Installer
File Version	5.38.99.6357
Company Name	Piriform Ltd
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	a989b426cc2f60db03826de6cf5510862e39961967e52c7b6e0481c1c81d5eba
Ssdeep	196608:mGBN5AVwa4wMPJYd1J6Ku2BxWETAilBpyu8lEGBmWJcSt3u:mGj5AVwVwB82BAqqx2wh3u
Trid	67.4,Win32 Executable MS Visual C++ (generic),14.2,Win32 Dynamic Link Library (generic),9.7,Win32 Executable (generic),4.3,Generic Win/DOS Executable,4.3,DOS Executable Generic

File Paths

FILE PATH ON CLIENT	SEEN COUNT
\\SERVER\User_Docs$\Administrator\Downloads\ccsetup538_slim.exe	3
ccsetup538_slim.exe	3
C:\CBServices\CBXexecute\ccsetup538_slim.exe	3

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x7250	0x7400	6.46491468355	2cf4cea611906abda27f6bec5b76ffbd
.rdata	0x9000	0x2b38	0x2c00	4.41938697887	5275f8cae603f81939930ac752de3d01
.data	0xc000	0x67edc	0x200	1.89688793125	3096d49b7b4c3de8338c4639cbb79a13
.ndata	0x74000	0x2fd000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x371000	0x98c4	0x9a00	4.86184280444	f4070f8f6e6f2622e8bdd32614a78672