VALKYRIE

PUA
Valkyrie Final Verdict

File Name: 6f7d35310e801dc9548d27283409c3b87224bd07pc-repair-kit-setup.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 6f7d35310e801dc9548d27283409c3b87224bd07
MD5: 030eb3443b07522fcb283002f21a15f7
First Seen Date: 2019-11-28 12:42:43 UTC
Number of Clients Seen: 6
Last Analysis Date: 2019-11-28 15:18:01 UTC
Human Expert Analysis Date: 2019-11-28 15:17:40 UTC
Human Expert Analysis Result: PUA
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2019-11-28 15:18:01 UTC	Malware
Static Analysis Overall Verdict	2019-11-28 15:18:01 UTC	No Match
Precise Detectors Overall Verdict	2019-11-28 15:18:01 UTC	No Match
Human Expert Analysis Overall Verdict	2019-11-28 15:17:40 UTC	PUA
File Certificate Validation		Vendor not found in Trusted List

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT

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	Suspicious
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

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS

No suspicious activity found

Behavioral Information

QueryFilePath

C:\Users\win7\AppData\Local\Temp\is-8DAM9.tmp\6f7d35310e801dc9548d27283409c3b87224bd07pc-repair-kit-setup.tmp
C:\Windows\system32\odbc32.dll
C:\Windows\system32\crtdll.dll
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll
C:\Users\win7\AppData\Local\Tem
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\rtl160.bpl
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\AxComponentsRTL.bpl
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\vcl160.bpl

LowerChar

f7d35310e801dc9548d27283409c3b87224bd07pc-repair-kit-setup

CreateMutex

Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000

OpenMutex

Local\MSCTF.Asm.MutexDefault1

WriteFile

C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\CFAHelper.dll
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\deu.lng
C:\6f7d35310e801dc9548d27283409c3b87224bd07pc-repair-kit-setup.exe
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\vclimg160.bpl
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\main.ini
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\sqlite3.dll
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\WizardHelper.dll
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\ita.lng
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\CommonForms.Site.dll
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\fra.lng
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\esp.lng
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\ptb.lng
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\AxBrowsers.dll
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\Localizer.dll
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\enu.lng
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\vcl160.bpl
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\PCRepairKit.exe
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\rtl160.bpl
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\AxComponentsVCL.bpl
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\AxComponentsRTL.bpl

ReadFile

C:\6f7d35310e801dc9548d27283409c3b87224bd07pc-repair-kit-setup.exe

LoadLibrary

C:\Users\win7\AppData\Local\Temp\is-8DAM9.tmp\6f7d35310e801dc9548d27283409c3b87224bd07pc-repair-kit-setup.ENU
C:\Users\win7\AppData\Local\Temp\is-8DAM9.tmp\6f7d35310e801dc9548d27283409c3b87224bd07pc-repair-kit-setup.EN
imm32.dll
C:\Windows\system32\uxtheme.dll
C:\Windows\system32\shell32.dll
C:\Windows\system32\ole32.dll
ADVAPI32.dll
ole32.dll
comctl32.dll
C:\Windows\system32\shfolder.dll
C:\Windows\system32\Rstrtmgr.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
kernel32.dll
C:\Users\win7\AppData\Local\Temp\is-6I2CO.tmp\WizardHelper.dll
OLEACCRC.DLL
C:\Windows\system32\odbcint.dll
C:\Windows\system32\crtdll.dll
C:\Windows\system32\kernel32.dll

OpenRegistryKey

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Win
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion
\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes

CreateRegistryKey

\REGISTRY\US

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2019-11-28 13:04:20 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2019-11-28 13:04:20 UTC	No Match		NotDetected
Static Precise NI Detector 3	2019-11-28 13:04:20 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2019-11-28 13:04:20 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2019-11-28 13:04:20 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2019-11-28 13:04:20 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2019-11-28 13:04:20 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2019-11-28 13:04:20 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2019-11-28 13:04:20 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2019-11-28 13:04:20 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2019-11-28 13:04:21 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2019-11-28 13:04:21 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2019-11-28 14:04:35 UTC
Analysis End Date: 2019-11-28 15:17:40 UTC
File Upload Date: 2019-11-28 12:41:47 UTC
Human Expert Analyst Feedback:
Verdict: PUA
Malware Family:
Malware Type: 0

Additional File Information

Vendor Validation - Not Verified ✖

[+] Tweakbit Pty Ltd

Status	Not Valid ✖

Certificate Validation - Success ✔

[+] DigiCert High Assurance EV Root CA

Status	NoError ✔
Start Date	2006-11-10 02:00:00
End Date	2031-11-10 02:00:00
Sha256	ed960860d0e06c89fa3ff7723437b6812c6d7e1ad370c7885b1251d2e1c2a938
Serial	02AC5C266A0B409B8F0B79F2AE462577
Subject Name	DigiCert High Assurance EV Root CA
Subject Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Subject Organization	DigiCert Inc
Subject Country	US
Subject Organizational Unit	www.digicert.com
Issuer Name	DigiCert High Assurance EV Root CA
Issuer Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Issuer Organization	DigiCert Inc
Issuer Country	US
Issuer Organizational Unit	www.digicert.com
Crl link	null
Key Usage	{"Digital Signature","Certificate Signing","Off-line CRL Signing","CRL Signing (86)"}
Extended Usage	null

[+] DigiCert High Assurance EV Root CA

Status	NoError ✔
Start Date	2006-11-10 02:00:00
End Date	2031-11-10 02:00:00
Sha256	ed960860d0e06c89fa3ff7723437b6812c6d7e1ad370c7885b1251d2e1c2a938
Serial	02AC5C266A0B409B8F0B79F2AE462577
Subject Name	DigiCert High Assurance EV Root CA
Subject Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Subject Organization	DigiCert Inc
Subject Country	US
Subject Organizational Unit	www.digicert.com
Issuer Name	DigiCert High Assurance EV Root CA
Issuer Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Issuer Organization	DigiCert Inc
Issuer Country	US
Issuer Organizational Unit	www.digicert.com
Crl link	null
Key Usage	{"Digital Signature","Certificate Signing","Off-line CRL Signing","CRL Signing (86)"}
Extended Usage	null

[+] DigiCert EV Code Signing CA (SHA2)

Status	NoError ✔
Start Date	2012-04-18 15:00:00
End Date	2027-04-18 15:00:00
Sha256	a692c7403bfd72f70438cf1a7fb928c92820e4c0c1cfd457497aa0b69b67a5ed
Serial	03F1B4E15F3A82F1149678B3D7D8475C
Subject Name	DigiCert EV Code Signing CA (SHA2)
Subject Key Identifier	8f e8 7e f0 6d 32 6a 00 05 23 c7 70 97 6a 3a 90 ff 6b ea d4
Subject Organization	DigiCert Inc
Subject Country	US
Subject Organizational Unit	www.digicert.com
Issuer Name	DigiCert High Assurance EV Root CA
Issuer Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Issuer Organization	DigiCert Inc
Issuer Country	US
Issuer Organizational Unit	www.digicert.com
Crl link	http://crl3.digicert.com/DigiCertHighAssuranceEVRootCA.crl,http://crl4.digicert.com/DigiCertHighAssuranceEVRootCA.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)"}

[+] Tweakbit Pty Ltd

Status	NoError ✔
Start Date	2018-12-05 02:00:00
End Date	2020-01-31 14:00:00
Sha256	eea084ac7b0ae70fa7d878fa725dccd6980ebdac54d86b4d2d1ae8657157e78e
Serial	073AED077070858E6FF267A838694278
Subject Name	Tweakbit Pty Ltd
Subject Key Identifier	13 8c 0b 50 52 a6 30 b9 12 e7 9a f2 38 1a c7 46 cf 23 c0 f8
Subject Organization	Tweakbit Pty Ltd
Subject Locality	Sydney
Subject State	New South Wales
Subject Country	AU
Issuer Name	DigiCert EV Code Signing CA (SHA2)
Issuer Key Identifier	8f e8 7e f0 6d 32 6a 00 05 23 c7 70 97 6a 3a 90 ff 6b ea d4
Issuer Organization	DigiCert Inc
Issuer Country	US
Issuer Organizational Unit	www.digicert.com
Crl link	http://crl3.digicert.com/EVCodeSigningSHA2-g1.crl,http://crl4.digicert.com/EVCodeSigningSHA2-g1.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	0x57051F88 [Wed Apr 6 14:39:04 2016 UTC]
Debug Artifacts	
Entry Point	0x4117dc (.itext)
Exifinfo	[object Object]
File Size	16721064
File Type Enum	6
Imphash	20dd26497880c05caed9305b3c8b9109
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	Copyright \xa9 2013-2019 TweakBit Pty Ltd
Internal Name	
File Version	1.x
Company Name	TweakBit
Comments	This installation was built with Inno Setup.
Product Name	TweakBit PCRepairKit
Product Version	1.8.4.19
File Description	TweakBit PCRepairKit Installation File
Original Filename	
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	b12141373e47afa567d24263d668c8fdd8d04eeed899ce8384436e10b959d626
Ssdeep	393216:+y4dzMIPDr/mxjwLzkfHJWbqVtzoJydTEprEfYQigAc/hl:H4BMmXPHkfpqqLQ7prTFgASl
Trid	57.2,Win32 Executable Delphi generic,18.2,Win32 Executable (generic),8.3,Win16/32 Executable Delphi generic,8,Generic Win/DOS Executable,8,DOS Executable Generic

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xf244	0xf400	6.37521350405	a33e9ff7181115027d121cd377c28c8f
.itext	0x11000	0xf64	0x1000	5.73220066616	caec456c18277b579a94c9508daf36ec
.data	0x12000	0xc88	0xe00	2.29672090879	746954890499546d73dce0e994642192
.bss	0x13000	0x56bc	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0x19000	0xe04	0x1000	4.59781255771	e9b9c0328fd9628ad4d6ab8283dcb20e
.tls	0x1a000	0x8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x1b000	0x18	0x200	0.20448815744	3dffc444ccc131c9dcee18db49ee6403
.rsrc	0x1c000	0x529f4	0x52a00	3.20896052335	1743c6204f1a73b5064f7c6776d5cf54