VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: conquer.png
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 7cae8d176784d8f271398f7504c307092d27903c
MD5: bb4ca1e6cb5fad3425fd6622414eb454
First Seen Date: 2019-03-23 11:08:17 UTC
Number of Clients Seen: 3
Last Analysis Date: 2019-03-27 06:46:50 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	2019-03-28 03:02:03 UTC	Malware
Static Analysis Overall Verdict	2019-03-27 06:46:50 UTC	No Threat Found
Precise Detectors Overall Verdict	2019-03-27 06:46:50 UTC	No Match
File Certificate Validation		Certificate and Vendor name are Not 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
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

Packer detection on signature database

- Microsoft Visual Basic v5.0
- Microsoft Visual Basic v5.0/v6.0

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS
No suspicious activity found

Behavioral Information

CreateMutex

<NULL>

LoadLibrary

OLEAUT32.DLL
SXS.DLL
kernel32

QueryFilePath

C:\conquer.png
C:\Windows\system32\MSVBVM60.DLL

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise PUA Detector 1	2019-03-27 06:46:34 UTC	No Match	NotDetected
Static Precise Trojan Detector 5	2019-03-27 06:46:34 UTC	No Match	NotDetected
Static Precise Trojan Detector 7	2019-03-27 06:46:34 UTC	No Match	NotDetected
Static Precise PUA Detector 4	2019-03-27 06:46:34 UTC	No Match	NotDetected
Static Precise PUA Detector 5	2019-03-27 06:46:34 UTC	No Match	NotDetected
Static Precise Trojan Detector 1	2019-03-27 06:46:34 UTC	No Match	NotDetected
Static Precise Trojan Detector 2	2019-03-27 06:46:34 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2019-03-27 06:46:34 UTC	No Match	NotDetected
Static Precise Trojan Detector 12	2019-03-27 06:46:34 UTC	No Match	NotDetected
Static Precise Trojan Detector 10	2019-03-27 06:46:34 UTC	No Match	NotDetected
Static Precise Virus Detector 1	2019-03-27 06:46:34 UTC	No Match	NotDetected
Static Precise Virus Detector 2	2019-03-27 06:46:34 UTC	No Match	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Not Verified ✖

[+] Rails switch france software (c) 2012

Status	Not Valid ✖

Certificate Validation - UntrustedRoot ✖

[+] Rails switch france software (c) 2012

Status	UntrustedRoot ✖
Start Date	2019-03-22 11:15:40
End Date	2022-03-21 11:15:40
Sha256	1f674e6faac2069e29c9be47fbce81234ba4139cad5b3050d7038c1408497510
Serial	01
Subject Name	Rails switch france software (c) 2012
Subject Key Identifier	null
Subject Organization	France rails corporation (c) 2012
Subject Country	FR
Issuer Name	Rails switch france software (c) 2012
Issuer Key Identifier	null
Issuer Organization	France rails corporation (c) 2012
Issuer Country	FR
Crl link	null
Key Usage	null
Extended Usage	null

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5C93AC54 [Thu Mar 21 15:23:00 2019 UTC]
Debug Artifacts	
Entry Point	0x401094 (.text)
Exifinfo	[object Object]
File Size	517448
File Type Enum	6
Imphash	e280f031ed3c7fae5e07f81bd4859f8f
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Translation	0x0409 0x04b0
Internal Name	FIGNERIA
File Version	1.07.0002
Company Name	epicarid10
Comments	Cedarpoint6
Product Name	ENGAGEMENT
Product Version	1.07.0002
Original Filename	FIGNERIA.exe
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	b97cfd740e7bb2b10b7141afcb2193064db254082d85985fd96748e687fe3238
Ssdeep	6144:mGVehYSa4zSqExmq+UIyZArBPCd/kbRADVRNl2xP4YwbRoPCnBsG6oS:mRucd5yZAo8dB
Trid	84.4,Win32 Executable Microsoft Visual Basic 6,6.7,Win32 Dynamic Link Library (generic),4.6,Win32 Executable (generic),2,Generic Win/DOS Executable,2,DOS Executable Generic

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x7ad34	0x7b000	6.36549032971	d11099bcf1cc492a05f2ff8554a9091d
.data	0x7c000	0x115c	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x7e000	0xe52	0x1000	5.50070264095	a67db54cc71e613b3c68b92fb18153ce