VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: crypt_b.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 74339b2f522ed9b1b47ba4249b9a6234694c1ce4
MD5: 6f0640320d81a92aafb6835b4b8366fc
First Seen Date: 2018-05-08 13:48:47 UTC
Number of Clients Seen: 5
Last Analysis Date: 2018-05-09 02:30:37 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	2018-05-09 02:30:37 UTC	Malware
Static Analysis Overall Verdict	2018-05-09 02:30:37 UTC	No Threat Found
Precise Detectors Overall Verdict	2018-05-09 02:30:37 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	Suspicious
Header Checksum is zero!	Suspicious
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	Clean
TLS callback functions array detected	Clean

Packer detection on signature database

BobSoft Mini Delphi -> BoB / BobSoft

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2018-05-08 13:48:18 UTC	No Match		NotDetected
Static Precise Trojan Detector 5	2018-05-08 13:48:18 UTC	No Match		NotDetected
Static Precise Trojan Detector 7	2018-05-08 13:48:18 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2018-05-08 13:48:18 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2018-05-08 13:48:18 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2018-05-08 13:48:18 UTC	No Match		NotDetected
Static Precise Trojan Detector 2	2018-05-08 13:48:18 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2018-05-08 13:48:18 UTC	No Match		NotDetected
Static Precise Trojan Detector 10	2018-05-08 13:48:18 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2018-05-08 13:48:18 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2018-05-08 13:48:18 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2018-05-08 13:48:18 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	0x297B4218 [Mon Jan 20 21:41:44 1992 UTC] [SUSPICIOUS]
Debug Artifacts	
Entry Point	0x465378 (CODE)
Exifinfo	
File Size	614912
File Type Enum	6
Imphash	
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	35a76eaf06b8b734159c02c2446dc9d8669cdefe99533b51b6251ed86d55b9fd
Ssdeep	
Trid	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x643c0	0x64400	6.58720480411	b5a7e97fbb8bdc097619507c43ba13be
DATA	0x66000	0x1264	0x1400	3.86340707666	fef08dd4a0f21098221630a78638228e
BSS	0x68000	0xc0d	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0x69000	0x21e0	0x2200	5.03710654782	34fe1493467a2474b12286dfe3f71cdc
.tls	0x6c000	0x10	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x6d000	0x18	0x200	0.20058190744	8b32af3e8d3851e5964e7328753a5f50
.reloc	0x6e000	0x7304	0x7400	6.63292347594	987b8244cc23e0715725ab49f8078d62
.rsrc	0x76000	0x26c40	0x26e00	6.90159016577	6a679d140e745776226de9bff0e171f2