VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: lVeckQArv.342
File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
SHA1: 4a573351cf0dfe6f27ef3f2ad46547907974596f
MD5: c7b49ae21e22eab80c938e4a74d1bea6
First Seen Date: 2016-12-26 15:20:13 UTC
Number of Clients Seen: 4
Last Analysis Date: 2016-12-26 15:20:13 UTC
Human Expert Analysis Date: 2016-12-27 06:23:00 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2016-12-26 15:20:13 UTC	Malware	!
Static Analysis Overall Verdict	2016-12-26 15:20:13 UTC	No Threat Found	?
Dynamic Analysis Overall Verdict	2016-12-26 15:20:13 UTC	No Threat Found	?
Human Expert Analysis Overall Verdict	2016-12-27 06:23:00 UTC	Malware	!
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!	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	✓

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	?

SUSPICIOUS BEHAVIORS	
Has no visible windows	!

Behavioral Information

QueryFilePath

C:\DLL_Loader.exe

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2016-12-27 06:07:14 UTC
Analysis End Date: 2016-12-27 06:23:00 UTC
File Upload Date: 2016-12-27 05:57:54 UTC
Human Expert Analyst Feedback: Malware
Verdict: Malware
Malware Family: Trojware.Win32.Ransom.Locky
Malware Type: Trojan Generic

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x583DD40F [Tue Nov 29 19:16:31 2016 UTC]
Entry Point	0x10001fa0 (.text)
File Size	204800
Machine Type	Intel 386 or later - 32Bit
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	4580a67b6eedcf233f9c74723635d89f29ccf1cc58fe0c12ef0b8aa80e38aa73

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x6dde	0x7000	5.972678	-
.rdata	0x8000	0x13fe	0x2000	3.463543	-
.data	0xa000	0x2634c	0x26000	5.504609	-
.rsrc	0x31000	0xa0	0x1000	0.096823[SUSPICIOUS]	-
.reloc	0x32000	0xb9a	0x1000	5.075811	-

PE Imports

- msi.dll
  - null
- KERNEL32.dll
  - LoadLibraryA
  - VirtualAlloc
  - GetProcAddress
- MSVCRT.dll
  - __dllonexit
  - free
  - memcpy
  - _onexit
  - _initterm
  - malloc
  - _adjust_fdiv

PE Exports

- ?SetData@@YGXXZ

PE Resources

- RT_STRING