VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: 1064817724.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 5d6572665560b7352b3eb45d26e837cc1ab1691c
MD5: 8d01c393b5663644f7c787ca03662cd7
First Seen Date: 2017-04-24 10:18:20 UTC
Number of Clients Seen: 16
Last Analysis Date: 2017-05-02 08:55:33 UTC
Human Expert Analysis Date: 2017-06-08 08:18:20 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2017-05-02 08:55:33 UTC	Malware
Static Analysis Overall Verdict	2017-05-02 08:55:33 UTC	No Threat Found
Precise Detectors Overall Verdict	2017-05-02 08:55:33 UTC	No Match
Human Expert Analysis Overall Verdict	2017-06-08 08:18:20 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	Suspicious
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	Clean
TLS callback functions array detected	Clean

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Uninstaller FP Detector	2017-05-02 08:55:33 UTC	No Match		No match.
Yara Rule Static Malware Detector	2017-05-02 08:55:33 UTC	No Match		No match.
Static Precise PUA Detector 1	2017-05-02 08:55:33 UTC	No Match		NotDetected
Static Precise Virus Detector	2017-05-02 08:55:33 UTC	No Match		NotDetected
Static Precise Trojan Detector	2017-05-02 08:55:33 UTC	No Match		NotDetected
Malicious Url Detector	2017-05-02 08:55:43 UTC	No Match		No match.

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2017-04-24 11:53:18 UTC
Analysis End Date: 2017-06-08 08:18:20 UTC
File Upload Date: 2017-05-27 08:05:59 UTC
Human Expert Analyst Feedback: Malware
Verdict: Malware
Malware Family: Trojware.Win32.Agent
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	0x58FD6E9C [Mon Apr 24 03:18:52 2017 UTC]
Entry Point	0x801262 (.text)
File Size	218112
Machine Type	Intel 386 or later - 32Bit
Mime Type	application/x-dosexec
Number Of Sections	4
Sha256	190d5c8de27115b98484d653dff246fc05ce02ac69fedd009e469d7535f3faeb

File Paths

FILE PATH ON CLIENT	SEEN COUNT
C:\VTRoot\HarddiskVolume3\Users\Shop\AppData\Local\Temp\1064817724.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x6dfc	0x6e00	6.501365	-
.rdata	0x8000	0x24e0	0x2600	4.787947	-
.data	0xb000	0x3cac	0xe00	2.251052	-
.rsrc	0xf000	0x2ad24	0x2ae00	7.618512[SUSPICIOUS]	-