VALKYRIE

!

MALWARE
Valkyrie Final Verdict

File Name: 20
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 44c32dfae9ac971c3651adbd82c821971a5400dc
MD5: 2a9d0d06d292a4cbbe4a95da4650ed54
First Seen Date: 2015-08-28 12:37:14 UTC
Number of Clients Seen: 13
Last Analysis Date: 2020-04-27 19:04:49 UTC
Human Expert Analysis Date: 2020-04-27 19:00:43 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2020-04-27 19:04:49 UTC	Malware	!
Human Expert Analysis Overall Verdict	2020-04-27 19:00:43 UTC	Malware	!
File Certificate Validation		Not Applicable	?

Static Analysis

No Static Analysis Result Received

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	Clean	✓
TLS callback functions array detected	Clean	✓

Packer detection on signature database

- Armadillo v1.71
- Microsoft Visual C++ v5.0/v6.0 (MFC)
- Microsoft Visual C++

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2020-04-27 15:43:35 UTC

Analysis End Date: 2020-04-27 19:00:43 UTC

File Upload Date: 2020-04-27 14:30:47 UTC

Human Expert Analyst Feedback:

Verdict: Malware

Malware Family:

Malware Type: 0

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x4D88C1EA [Tue Mar 22 15:36:10 2011 UTC]
Entry Point	0x4015a2 (.data)
File Size	72704
File Type Enum	6
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	? 2010 Sogou.com Inc. All rights reserved.
Internal Name	SogouPY Config
File Version	5.0.0.3787
Company Name	Sogou.com Inc.
Private Build	
Legal Trademarks	
Comments	
Product Name	\u641c\u72d7\u62fc\u97f3\u8f93\u5165\u6cd5
Special Build	
Product Version	5.0.0.3787
File Description	\u641c\u72d7\u62fc\u97f3\u8f93\u5165\u6cd5 \u8bbe\u7f6e\u7a0b\u5e8f
Original Filename	Config.exe
Translation	0x0804 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	2
Sha256	09a1c17ac55cde962b4f3bcd61140d752d86362296ee74736000a6a647c73d8c

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.data	0x1000	0xbcc	0xc00	5.82042706093	2a6a06117a251a3d3aef8f00b73876a2
.rsrc	0x2000	0x11000	0x10c00	6.1287843575	74a468373ff0f87c6a068b0bfbcb969b