









PUA
Valkyrie Final Verdict













File Name: SECOH-QAD.exe
File Type: PE32+ executable (GUI) x86-64, for MS Windows
SHA1: 66c72019eafa41bbf3e708cc3824c7c4447bdab6
MD5: 38de5b216c33833af710e88f7f64fc98
First Seen Date: 2015-08-31 04:56:27 UTC
Number of Clients Seen: 588
Last Analysis Date: 2023-03-20 21:59:13 UTC
Human Expert Analysis Date: 2018-10-24 14:39:07 UTC
Human Expert Analysis Result: PUA
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary


ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2023-03-20 21:59:13 UTC	PUA 
Static Analysis Overall Verdict	2023-03-20 21:59:13 UTC	No Threat Found 
Precise Detectors Overall Verdict	2023-03-20 21:59:13 UTC	No Match 
Human Expert Analysis Overall Verdict	2018-10-24 14:39:07 UTC	PUA 
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	Suspicious 
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 
Entry 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	
File size is too small	
Has no visible windows	

Behavioral Information

QueryFilePath	
C:\Windows\SysWOW64\rundll32.exe	

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2023-03-20 21:59:10 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2023-03-20 21:59:10 UTC	No Match		NotDetected
Static Precise NI Detector 3	2023-03-20 21:59:10 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2023-03-20 21:59:10 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2023-03-20 21:59:10 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2023-03-20 21:59:10 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2023-03-20 21:59:10 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2023-03-20 21:59:10 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2023-03-20 21:59:10 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2023-03-20 21:59:10 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2023-03-20 21:59:10 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2023-03-20 21:59:10 UTC	No Match		NotDetected


Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2018-10-24 10:55:44 UTC
Analysis End Date: 2018-10-24 14:39:07 UTC
File Upload Date: 2018-10-24 09:13:34 UTC
Human Expert Analyst Feedback:
Verdict: PUA
Malware Family:
Malware Type: 0

Additional File Information

Vendor Validation	
Vendor Validation is not Applicable 	



📄 PE Headers



PROPERTY	VALUE
Compilation Time Stamp	0x52E2A76B [Fri Jan 24 17:48:27 2014 UTC]
Debug Artifacts	
Entry Point	0x140001000 (.text)
Exifinfo	
File Size	4608
File Type Enum	7
Imphash	
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
Magic Literal Enum	4
Mime Type	application/x-dosexec
Number Of Sections	4
Sha256	9896a6fcb9bb5ac1ec5297b4a65be3f647589adf7c37b45f3f7466decd6a4a7f
Ssdeep	
Trid	

📄 PE Sections



NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x3ff	0x400	5.707653344	2087ce3b7f5940a3e4cd bca11c9815df
.rdata	0x2000	0x530	0x600	3.83424840523	9fdfb5d778dd18b4fb57ebb90e9e681a
.pdata	0x3000	0x30	0x200	0.428564979938	63f90834bf508c3c466106a0fd9df225
.rsrc	0x4000	0x1e0	0x200	4.70150325825	8d096de51d16180d98ba04bad2632f19