VALKYRIE

?

NO THREAT FOUND

File Name: word.exe
File Type: PE32+ executable (GUI) x86-64, for MS Windows
SHA1: df4888f00a7c86a838385729737d2849f5207504
MD5: 944836d5bb621f20fbfb699955dd2266
First Seen Date: 2024-09-03 15:17:02 UTC
Number of Clients Seen: 5
Last Analysis Date: 2024-09-08 16:52:34 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Valkyrie Automatic Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2024-09-08 16:52:34 UTC	No Match	?
Static Analysis Overall Verdict	2024-09-08 16:52:34 UTC	No Threat Found	?
Dynamic Analysis Overall Verdict	2024-09-08 16:52:34 UTC	No Threat Found	?
Precise Detectors Overall Verdict	2024-09-08 16:52:34 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	Suspicious	!
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!	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	Suspicious	!
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:\Windows\SysWOW64\rundll32.exe

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2024-09-08 16:52:23 UTC	No Match	?	NotDetected
Static Precise PUA Detector 4	2024-09-08 16:52:23 UTC	No Match	?	NotDetected
Static Precise NI Detector 3	2024-09-08 16:52:23 UTC	No Match	?	NotDetected
Static Precise PUA Detector 5	2024-09-08 16:52:23 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 1	2024-09-08 16:52:23 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 3	2024-09-08 16:52:23 UTC	No Match	?	NotDetected
Static Precise PUA Detector 6	2024-09-08 16:52:23 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 12	2024-09-08 16:52:23 UTC	No Match	?	NotDetected
Static Precise Virus Detector 1	2024-09-08 16:52:23 UTC	No Match	?	NotDetected
Static Precise Virus Detector 2	2024-09-08 16:52:23 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 13	2024-09-08 16:52:23 UTC	No Match	?	NotDetected
Static Precise PUA Detector 2	2024-09-08 16:52:23 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	0x66D6BED5 [Tue Sep 3 07:46:29 2024 UTC]
Debug Artifacts	
Entry Point	0x14001b7a8 (.text)
Exifinfo	
File Size	655360
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	6
Sha256	6f145c1ed78deec4ef725b9eb8696f0e706ce9652337f65ca0a3d72a3e74af5d
Ssdeep	
Trid	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1c65f	0x1c800	6.43580880261	9f11d109fe73763c0de5bb93e598e381
.rdata	0x1e000	0x5162e	0x51800	7.57579796332	3d8dbdd16af54306d81316c1f56d6940
.data	0x70000	0x10b8	0x1000	6.65438744917	fa5bc61e85d47e03c0b2fc6d6e6d55db
.pdata	0x72000	0x1488	0x1600	4.90877500599	cea7340ead28339803a913f7c7e245ec
.rsrc	0x74000	0x2eda0	0x2ee00	3.02874210011	4f792683cc7b8658f0a29fd3e7eea4fb
.reloc	0xa3000	0x6d0	0x800	5.1025879477	c17cb55d6d4dd32cda0a936bad15aa31