VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: virussign.com_5b24ac26cb4207e5d2c92992ce9f80a6.vir
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 708623a6031fb5d83c30a3c5706167346d73a6a0
MD5: 5b24ac26cb4207e5d2c92992ce9f80a6
First Seen Date: 2024-07-24 16:08:49 UTC
Number of Clients Seen: 2
Last Analysis Date: 2024-07-25 06:56:14 UTC
Human Expert Analysis Date: 2024-07-25 06:56:07 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2024-07-25 06:56:14 UTC	Malware	!
Static Analysis Overall Verdict	2024-07-25 06:56:14 UTC	No Threat Found	?
Precise Detectors Overall Verdict	2024-07-25 06:56:14 UTC	No Match	?
Human Expert Analysis Overall Verdict	2024-07-25 06:56:07 UTC	Malware	!
File Certificate Validation		Not Applicable	?

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	?

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	?

SUSPICIOUS BEHAVIORS	
Creates a child process	!

Behavioral Information

LoadLibrary

OLEAUT32.DLL
SXS.DLL
C:\Windows\system32\vb6chs.dll
C:\Windows\system32\asycfilt.dll
user32
C:\Windows\system32\kernel32.dll
ntvdm64.dll

CreateMutex

<NULL>

ReadFile

C:\virussign.com_5b24ac26cb4207e5d2c92992ce9f80a6.exe
C:\Unicorn-9647.exe
C:\Unicorn-9372.exe

WriteFile

C:\virussign.com_5b24ac26cb4207e5d2c92992ce9f80a6.exe
C:\Unicorn-9647.exe
C:\Unicorn-54986.exe
C:\Unicorn-9372.exe

CreateProcess

C:\\Unicorn-9647.exe
C:\\Unicorn-9372.exe
C:\\Unicorn-54986.exe

QueryFilePath

C:\virussign.com_5b24ac26cb4207e5d2c92992ce9f80a6.vir
C:\Windows\system32\MSVBVM60.DLL

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2024-07-24 16:08:16 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2024-07-24 16:08:16 UTC	No Match		NotDetected
Static Precise NI Detector 3	2024-07-24 16:08:16 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2024-07-24 16:08:16 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2024-07-24 16:08:16 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2024-07-24 16:08:16 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2024-07-24 16:08:16 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2024-07-24 16:08:16 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2024-07-24 16:08:16 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2024-07-24 16:08:16 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2024-07-24 16:08:16 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2024-07-24 16:08:16 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2024-07-25 06:03:09 UTC
Analysis End Date: 2024-07-25 06:56:07 UTC

File Upload Date: 2024-07-24 16:08:02 UTC
Human Expert Analyst Feedback:
Verdict: Malware
Malware Family:
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	0x5C432780 [Sat Jan 19 13:34:56 2019 UTC]
Debug Artifacts	
Entry Point	0x4013d4 (.text)
Exifinfo	[object Object]
File Size	479573
File Type Enum	6
Imphash	5d6cad172c5535e4b6b6bbd246571621
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Internal Name	Kawaii-Unicorn
File Version	1.00
Company Name	UEFI
Product Name	Kawaii-Unicorn
Product Version	1.00
Original Filename	Kawaii-Unicorn.exe
Translation	0x0804 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	f28b4e7e994c4295cc56123f1aa662e5079cd7bd4745443f3bda29fcaf449b01
Ssdeep	3072:sD+qogWdjf8U2bYh8zxjffr/Gh7jvIp5mDHeBVy+lh039pk+gwld:sDbopkU2+8tjffq0RRlh6fk+g
Trid	88.6,Win32 Executable Microsoft Visual Basic 6,4.8,Win32 Executable (generic),2.1,OS/2 Executable (generic),2.1,Generic Win/DOS Executable,2.1,DOS Executable Generic

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x2a5c4	0x2b000	7.57108685339	4f34a8eb4756a97302d0de1e516452cf
.data	0x2c000	0xa20	0x1000	0.00984533685143	78b3a7243dede89de44755429cfb738f
.rsrc	0x2d000	0x479f8	0x48000	2.45666301737	c1d6046c12b614ce694f503c8aae1733