VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: 6f7fa9f44407a8723af6989a45b68dbaddc444bcvirussign.com_bf3acdce6a37029297b2467af6d459d8.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 6f7fa9f44407a8723af6989a45b68dbaddc444bc
MD5: bf3acdce6a37029297b2467af6d459d8
First Seen Date: 2024-11-12 16:13:49 UTC
Number of Clients Seen: 3
Last Analysis Date: 2024-11-12 20:49:48 UTC
Human Expert Analysis Date: 2024-11-12 20:49:21 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2024-11-12 18:51:31 UTC	Malware	
Static Analysis Overall Verdict	2024-11-12 20:49:48 UTC	Highly Suspicious	
Dynamic Analysis Overall Verdict	2024-11-12 20:49:48 UTC	No Threat Found	
Precise Detectors Overall Verdict	2024-11-12 20:49:48 UTC	No Match	
Human Expert Analysis Overall Verdict	2024-11-12 20:49:21 UTC	Malware	
File Certificate Validation		Not Applicable	

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	

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	

Packer detection on signature database

Microsoft Visual Basic v5.0/v6.0

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Creates a child process	
Writes to address space of another process	
Reads memory of another process	

Behavioral Information

LoadLibrary

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

CreateMutex

<NULL>

ReadFile

C:\Unicorn-28084.exe
C:\Unicorn-19510.exe
C:\Unicorn-32312.exe
C:\Unicorn-28146.exe
C:\Unicorn-11237.exe
C:\Unicorn-28364.exe
C:\Unicorn-62219.exe
C:\6f7fa9f44407a8723af6989a45b68dbaddc444bcvirussign.com_bf3acdce6a37029297b2467af6d459d8.exe

WriteFile

C:\Unicorn-11237.exe
C:\Unicorn-32312.exe
C:\Unicorn-28146.exe
C:\Unicorn-26099.exe
C:\Unicorn-19510.exe
C:\Unicorn-8498.exe
C:\Unicorn-62219.exe
C:\6f7fa9f44407a8723af6989a45b68dbaddc444bcvirussign.com_bf3acdce6a37029297b2467af6d459d8.exe
C:\Unicorn-28084.exe
C:\Unicorn-28364.exe

CreateProcess

C:\\Unicorn-32312.exe
C:\\Unicorn-62219.exe
C:\\Unicorn-8498.exe
C:\\Unicorn-26099.exe

QueryFilePath

C:\Unicorn-28228.exe
C:\Windows\system32\MSVBVM60.DLL
C:\Unicorn-28084.exe
C:\Unicorn-19510.exe
C:\Unicorn-28146.exe
C:\Unicorn-28364.exe
C:\6f7fa9f44407a8723af6989a45b68dbaddc444bcvirussign.com_bf3acdce6a37029297b2467af6d459d8.exe
C:\Unicorn-17368.exe

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2024-11-12 16:13:14 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2024-11-12 16:13:14 UTC	No Match		NotDetected
Static Precise NI Detector 3	2024-11-12 16:13:14 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2024-11-12 16:13:14 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2024-11-12 16:13:14 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2024-11-12 16:13:14 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2024-11-12 16:13:14 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2024-11-12 16:13:14 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2024-11-12 16:13:14 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2024-11-12 16:13:14 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2024-11-12 16:13:14 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2024-11-12 16:13:14 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2024-11-12 17:43:05 UTC
Analysis End Date: 2024-11-12 20:49:21 UTC
File Upload Date: 2024-11-12 15:59:47 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	0x5C43C180 [Sun Jan 20 00:32:00 2019 UTC]
Debug Artifacts	
Entry Point	0x4013d4 (.text)
Exifinfo	[object Object]
File Size	479233
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	ce0fb473bfcdecd8bcba2d5c0c8e9018771cb3bdba53f520262807aedb771de6
Ssdeep	3072:4begogxaIK57tbYZPzcfmbfD/n2DnsIH9QmyeQVqAfiKkHi3uxgIU:4btoCO7tCP4fmbfra7wfiDC3ux
Trid	90.6,Win32 Executable Microsoft Visual Basic 6,4.9,Win32 Executable (generic),2.2,Generic Win/DOS Executable,2.2,DOS Executable Generic

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x2a5c4	0x2b000	7.57117139146	06e36c9bcde09a1fd5fab4945e8bdcef
.data	0x2c000	0xa20	0x1000	0.0164084645156	fe6def1cdf5f82a8268acf3a0a468ca5
.rsrc	0x2d000	0x479f8	0x48000	2.45845977691	b1013b1705efa98008a92989502e51f1