VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: virussign.com_0294f103cf2a4bf978983b54ee882ee6.exe
File Type: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
SHA1: 019c6ae7809e3c860a8d93eea365de57d128b6b9
MD5: 0294f103cf2a4bf978983b54ee882ee6
First Seen Date: 2025-01-04 21:16:41 UTC
Number of Clients Seen: 2
Last Analysis Date: 2025-01-05 12:09:57 UTC
Human Expert Analysis Date: 2025-01-05 12:09:47 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2025-01-04 22:39:13 UTC	Malware
Static Analysis Overall Verdict	2025-01-05 12:09:57 UTC	Highly Suspicious
Dynamic Analysis Overall Verdict	2025-01-05 12:09:57 UTC	No Threat Found
Precise Detectors Overall Verdict	2025-01-05 12:09:57 UTC	No Match
Human Expert Analysis Overall Verdict	2025-01-05 12:09:47 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	Suspicious
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	Suspicious
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	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

MingWin32 v?.? (h)

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS
Creates a child process
Creates file in a system directory
Writes to address space of another process
Uses a function clandestinely
Copies itself to startup
Reads memory of another process
Opens a file in a system directory

Behavioral Information

CopyFile

{"lpNewFileName": "C:\\Windows\\system32\\smnss.exe", "lpExistingFileName": "C:\\Windows\\system32\\grcopy.dll"}

QueryFilePath

C:\Windows\SysWOW64\smnss.exe

CreateProcess

C:\Windows\system32\smnss.exe

CreateMutex

VULnaShvolna
x_socks5aan
RasPbFile

WriteFile

C:\Windows\system32\zipfi.dll
C:\Windows\system32\zipfiaq.dll

ReadFile

C:\Windows\system32\grcopy.dll
C:\Windows\system32\zipfi.dll
C:\Windows\system32\zipfiaq.dll
C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\FrameworkList.xml
C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\WinFXList.xml
C:\ProgramData\Microsoft\Windows\Power Efficiency Diagnostics\energy-report-2015-06-11.xml
C:\ProgramData\Microsoft\Windows\Power Efficiency Diagnostics\energy-report-2015-07-27.xml
C:\ProgramData\Microsoft\Windows\Power Efficiency Diagnostics\energy-report-2023-10-13.xml
C:\ProgramData\Microsoft\Windows\Power Efficiency Diagnostics\energy-report-2023-12-05.xml

C:\ProgramData\Microsoft\Windows\Power Efficiency Diagnostics\energy-report-latest.xml
C:\ProgramData\Microsoft\Windows\Power Efficiency Diagnostics\energy-report.html
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_VBoxService.exe_91a333d46311590cce87f7069321f373d62a236_cab_089744f2\WER4262.tm
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_VBoxService.exe_91a333d46311590cce87f7069321f373d62a236_cab_089744f2\WER42F0.tm
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_0_ff109b8e6ff4d05d9a6d51ed29594fae5ed875d_cab_077bf59b\client_manifest.txt
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_x64_d473a376adfb18a7b165c5e3c26de43cd8bccb_cab_07087674\DMI7607.tmp.log.xml

LoadLibrary

Secur32.dll
SHELL32.dll
ADVAPI32.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
C:\Windows\system32\shervans.dll
KERNEL32.DLL
api-ms-win-downlevel-ole32-l1-1-0.dll
ADVAPI32.DLL
msvcrt.dll
USER32.dll
WSOCK32.DLL
API-MS-Win-Security-SDDL-L1-1-0.dll
WS2_32.dll
winhttp.dll
IPHLPAPI.DLL
api-ms-win-downlevel-shlwapi-l2-1-0.dll
RASAPI32.dll
shlwapi.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
CRYPTBASE.dll

OpenRegistryKey

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_DISABLE_UNICODE_HANDLE_CLOSING_CALLBACK
\REGISTRY\USER\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
\REGISTRY\MA
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN
\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InprocServer32
\REGISTRY\MACHINE\SO

QueryProcessAddress

CreateProcessA

CreateRegistryKey

\REGISTRY\USER\.DEFAULT\SOFTWARE\Mic

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2025-01-04 21:16:38 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2025-01-04 21:16:38 UTC	No Match		NotDetected
Static Precise NI Detector 3	2025-01-04 21:16:38 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2025-01-04 21:16:38 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2025-01-04 21:16:38 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2025-01-04 21:16:38 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2025-01-04 21:16:38 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2025-01-04 21:16:38 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2025-01-04 21:16:38 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2025-01-04 21:16:38 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2025-01-04 21:16:38 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2025-01-04 21:16:38 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2025-01-05 09:56:52 UTC
Analysis End Date: 2025-01-05 12:09:47 UTC
File Upload Date: 2025-01-04 21:16:32 UTC
Human Expert Analyst Feedback: Trojware
Verdict: Malware
Malware Family: Generic
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	0x0 [Thu Jan 1 00:00:00 1970 UTC] [SUSPICIOUS]
Debug Artifacts	
Entry Point	0x4012a0 (45e3fsky)
Exifinfo	
File Size	199777
File Type Enum	6
Imphash	
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Mime Type	application/x-dosexec
Number Of Sections	14
Sha256	812bdf773194fa8e24833e37e3b82551217dc78b8ad82da3f0bb9140af4a5ace
Ssdeep	
Trid	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
45e3fsky	0x1000	0x13000	0x12600	6.55135485658	c2fae80e933ac914ad3fe864de788c40
475cokak	0x14000	0xa000	0x9c00	2.11910609727	cacd7b4fbb47f8496127ff00e5f9a37c
48f1pfcg	0x1e000	0x1000	0xa00	3.20058942264	0d8e7a6d2d4cc43befe05f8496d6761a
	0x1f000	0x1000	0xc00	5.25278825498	7b7aa1accf9d6eb83487f33fd6f402be
dMrQUrpm	0x20000	0x47c	0x600	0.763890224148	428da4f6efd2ff37eaddaed1b12452a1
wTdzgxdL	0x21000	0x4533	0x4600	5.51376677406	23e1f42df7ce9d2729e90672eb544637
EBcQahwr	0x26000	0x37	0x200	0.179432541656	7d6b92079386875cf1bfa94196ab3519
FQXfMeYO	0x27000	0xe84	0x1000	4.52363169147	a318aa7719b6cd568ca0a1e66d8297e1
hKmyjwiO	0x28000	0x11b	0x200	1.66827897619	05b2efd7846e4ba33da9846f8a833f51
PXGYXprF	0x29000	0x34b	0x400	3.74602564844	1eabda6dfce2b76cda0e1d3861dc06fb
hNfGxQeL	0x2a000	0xb9b8	0xba00	6.01031132381	4a8742251e4c3080f8d4a1a3897424bc
nSMexQnR	0x36000	0x3f0	0x400	1.29710313331	29fb822d2da95245075b7224aa5da5dc
VGiRpyFT	0x37000	0x900	0xa00	3.50196698966	b62320e01081de3a325edfb31670caed
HHmipRio	0x38000	0x2d2	0x400	3.10815148029	f3dffbccf192f6ea29ac32fc8d0333fa