VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: StopAd_Installer.exe
File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1: af9b8e0ba0c61c949c9479f15ad2b48e286d3da1
MD5: 6f858290adad6f917a6b7542729ae4b4
First Seen Date: 2018-01-02 19:41:23 UTC
Number of Clients Seen: 4
Last Analysis Date: 2018-01-02 19:41:23 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2018-01-02 19:41:23 UTC	Clean	
Static Analysis Overall Verdict	2018-01-02 19:41:23 UTC	No Threat Found	
Precise Detectors Overall Verdict	2018-01-02 19:41:23 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	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 C# / Basic .NET
- .NET executable

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	2018-01-02 19:40:49 UTC	No Match	NotDetected
Static Precise Virus Detector	2018-01-02 19:40:49 UTC	No Match	NotDetected
Static Precise Trojan Detector	2018-01-02 19:40:49 UTC	No Match	NotDetected
Static Precise Adware InstallCore Detector 1	2018-01-02 19:40:49 UTC	No Match	NotDetected
Static Precise Trojan Detector 2	2018-01-02 19:40:49 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2018-01-02 19:40:49 UTC	No Match	NotDetected
Static Precise Trojan Generic Cryptor Detector 1	2018-01-02 19:40:49 UTC	No Match	NotDetected
Static Precise Virus Detector 2	2018-01-02 19:40:49 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	0x5A391B92 [Tue Dec 19 14:00:50 2017 UTC]
Debug Artifacts	[object Object]
Entry Point	0x53aeee (.text)
Exifinfo	[object Object]
File Size	1336944
File Type Enum	6
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Translation	0x0000 0x04b0
Legal Copyright	\ufffd 2017 NOVNIFY LIMITED. All rights reserved.
Assembly Version	1.0.280.1
Internal Name	installer.exe
File Version	1.0.280.1
Company Name	Novnify
Legal Trademarks	
Comments	StopAd Installer
Product Name	StopAd Installer
Product Version	1.0.280.1
File Description	StopAd Installer
Original Filename	installer.exe
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	a933666ddd3e14d73fd322bfe36f114548b1a309b32d32ca12dad369aa03a9b6
Ssdeep	24576:GrYsbfNopsZxbqJTbwz2FwXaMwxwb4Tp2XCg3kaE5NKwWmdwlYvNb9EeUgaZ:GFopsaJfE2FMCxwb4T8XxATWmClY1b9w
Trid	49.4,Win64 Executable (generic),23.4,Windows screen saver,11.7,Win32 Dynamic Link Library (generic),8,Win32 Executable (generic),3.5,Generic Win/DOS Executable

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0x138ef4	0x139000	7.91622682739	982220207fe8b6714471ce245586089f
.rsrc	0x13c000	0x9a00	0x9a00	4.00813111049	2860ee513c0e0a842b555d01931863c6
.reloc	0x146000	0xc	0x200	0.101910425663	df6160779094dd04e93033ac8c37fdbe