VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: ShareX_NativeMessagingHost.exe
File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1: a837a13d3970418932158fbcc6b3e1626a50b53c
MD5: deb3c9b791986a397d8c57a93c658169
First Seen Date: 2017-04-17 14:13:53 UTC
Number of Clients Seen: 2
Last Analysis Date: 2017-04-17 14:13:53 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	2017-04-17 14:13:53 UTC	Clean
Static Analysis Overall Verdict	2017-04-17 14:13:53 UTC	No Threat Found
Dynamic Analysis Overall Verdict	2017-04-17 14:13:53 UTC	No Threat Found
Precise Detectors Overall Verdict	2017-04-17 14:13:53 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	Clean
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	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
Operation successfully finished.

Behavioral Information

QueryFilePath

C:\Windows\SysWOW64\rundll32.exe

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise PUA Detector 1	2017-04-17 14:13:12 UTC	No Match	NotDetected
Static Precise Virus Detector	2017-04-17 14:13:12 UTC	No Match	NotDetected
Static Precise Trojan Detector	2017-04-17 14:13:12 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	0x58EFF610 [Thu Apr 13 22:05:04 2017 UTC]
Entry Point	0x402df2 (.text)
File Size	6656
Machine Type	Intel 386 or later - 32Bit
Translation	0x0000 0x04b0
Legal Copyright	Copyright (c) 2007-2017 ShareX Team
Assembly Version	1.0.0.0
Internal Name	ShareX_NativeMessagingHost.exe
File Version	1.0.0.0
Company Name	ShareX Team
Legal Trademarks	
Comments	
Product Name	ShareX
Product Version	1.0.0.0
File Description	ShareX NativeMessagingHost
Original Filename	ShareX_NativeMessagingHost.exe
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	8d1bbce4b602aaacbf7e2153c83793ed67a2bf121e5eea2e57bb783b9b023dc7

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0xdf8	0xe00	5.334402	-
.rsrc	0x4000	0x64c	0x800	3.525980	-
.reloc	0x6000	0xc	0x200	0.081539[SUSPICIOUS]	-