VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: qw787_2102v2.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 263610b09096511eb54892a82b7d631ac6ec4995
MD5: 979f958d3a5f08efc058fe85f58bac6e
First Seen Date: 2021-03-05 07:12:04 UTC
Number of Clients Seen: 2
Last Analysis Date: 2021-03-05 07:12:04 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	2021-03-05 10:48:22 UTC	Malware	
Static Analysis Overall Verdict	2021-03-05 07:12:04 UTC	No Match	
Precise Detectors Overall Verdict	2021-03-05 07:12:04 UTC	No Match	
File Certificate Validation		Not Applicable	

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

No Detector Result Received

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	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
Debug Artifacts	
Entry Point	0x49ab80 (CODE)
Exifinfo	[object Object]
File Size	11873792
File Type Enum	6
Imphash	332f7ce65ead0adfb3d35147033aabe9
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	
Internal Name	
File Version	1.0.0.4
Company Name	Synaptics
Legal Trademarks	
Comments	
Product Name	Synaptics Pointing Device Driver
Product Version	1.0.0.0
File Description	Synaptics Pointing Device Driver
Original Filename	
Translation	0x041f 0x04e6
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	5cf16b5f456f7a7142b719af75bcbbde7249e596e89b8fe7ccabb4ef7782fce9
Ssdeep	196608:hLOr+f5WK3giPQSFbredGAZpbw79NRbOqQnKoG/Pn3Sw70OZb:h5kCgXS5rlGxRbOfKo8n3R7FZb
Trid	79,Win32 Executable Borland Delphi 7,13,Inno Setup installer,4.9,Win32 EXE PECompact compressed (generic),1.6,Win32 Executable Delphi generic,0.5,Win32 Executable (generic)

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x99bec	0x99c00	6.57295787036	33fbe30e8a64654287edd1bf05ae7c8c
DATA	0x9b000	0x2e54	0x3000	4.85462079781	1f5e19e7d20c1d128443d738ac7bc610
BSS	0x9e000	0x11e5	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xa0000	0x2a42	0x2c00	4.91933321603	21ff53180b390dc06e3a1adf0e57a073
.tls	0xa3000	0x10	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0xa4000	0x39	0x200	0.784620157709	a92cf494c617731a527994013429ad97
.reloc	0xa5000	0xa980	0xaa00	6.67412498558	dcd1b1c3f3d28d444920211170d1e8e6
.rsrc	0xb0000	0xaa8418	0xaa8600	7.97060735553	431de89dd63dc3eab0290a5f61adedf8