xcitium

CLEAN
Xcitium Final Verdict

File Name: 3D_thing.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 5b592b519d9fcdd2f1836b9409e46f2d31e4a1bc
MD5: 9c50976541bf42d1416bab718c345c8b
First Seen Date: 2023-07-17 13:00:04 UTC
Number of Clients Seen: 6
Last Analysis Date: 2023-07-17 16:43:22 UTC
Human Expert Analysis Date: 2023-07-17 16:33:37 UTC
Human Expert Analysis Result: Clean
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2023-07-17 16:43:22 UTC	Clean
Static Analysis Overall Verdict	2023-07-17 16:43:22 UTC	No Threat Found
Precise Detectors Overall Verdict	2023-07-17 16:43:22 UTC	No Match
Human Expert Analysis Overall Verdict	2023-07-17 16:33:37 UTC	Clean
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	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

BobSoft Mini Delphi -> BoB / BobSoft

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Opens a file in a system directory	

Behavioral Information

OpenMutex

Local\MSCTF.Asm.MutexDefault1

LoadLibrary

C:\3D_thing.ENU
C:\3D_thing.EN
uxtheme.dll
comctl32.dll
UxTheme.dll
ADVAPI32.dll
IMM32.dll
C:\Windows\system32\ole32.dll

ReadFile

C:\Windows\Fonts\staticcache.dat

QueryFilePath

C:\3D_thing.exe
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll

OpenRegistryKey

\REGISTRY\MACHINE\SOFTWARE\M

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise PUA Detector 1	2023-07-17 13:00:00 UTC	No Match	NotDetected
Static Precise PUA Detector 4	2023-07-17 13:00:00 UTC	No Match	NotDetected
Static Precise NI Detector 3	2023-07-17 13:00:00 UTC	No Match	NotDetected
Static Precise PUA Detector 5	2023-07-17 13:00:00 UTC	No Match	NotDetected
Static Precise Trojan Detector 1	2023-07-17 13:00:00 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2023-07-17 13:00:00 UTC	No Match	NotDetected
Static Precise PUA Detector 6	2023-07-17 13:00:00 UTC	No Match	NotDetected
Static Precise Trojan Detector 12	2023-07-17 13:00:00 UTC	No Match	NotDetected
Static Precise Virus Detector 1	2023-07-17 13:00:00 UTC	No Match	NotDetected
Static Precise Virus Detector 2	2023-07-17 13:00:00 UTC	No Match	NotDetected
Static Precise Trojan Detector 13	2023-07-17 13:00:00 UTC	No Match	NotDetected
Static Precise PUA Detector 2	2023-07-17 13:00:00 UTC	No Match	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2023-07-17 14:21:50 UTC
Analysis End Date: 2023-07-17 16:33:37 UTC
File Upload Date: 2023-07-17 12:59:55 UTC
Human Expert Analyst Feedback: None
Verdict: Clean

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	0x463008 (CODE)
Exifinfo	[object Object]
File Size	495104
File Type Enum	6
Imphash	8656a4885837fe2dfa3320c60e2d90fc
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	New Art Illusion
Internal Name	
File Version	2.1.0.0
Company Name	New Art Illusion
Legal Trademarks	
Comments	
Product Name	
Product Version	2.1.0.0
File Description	3D-Easy FUN3D
Original Filename	
Translation	0x0407 0x04e4
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	85a46e5b3e5f93a456439d5b37fd3fd3e1717db2a7b5162c008a94e4ca796245
Ssdeep	6144:KRzn53atGGtiPgj9PqZlroaeKx+8un2r6ASRnyfWKtNUrp/2AW48+qUqmMkIHW2/:kzn53atnRPHhXKtNgZ8PcCRU4H
Trid	46.7,Win32 Executable Borland Delphi 7,31.7,Win32 Executable Borland Delphi 5,18.4,Win32 Executable Borland Delphi 6,0.9,Win32 Executable Delphi generic,0.9,Windows screen saver

File Paths

FILE PATH ON CLIENT	SEEN COUNT
C:\Users\JITech\OneDrive\Desktop\Malware for valkyrie\85a46e5b3e5f93a456439d5b37fd3fd3e1717db2a7b5162c008a94e4ca796245.exe	4
3D_thing.exe	4
D:\Malware for valkyrie\85a46e5b3e5f93a456439d5b37fd3fd3e1717db2a7b5162c008a94e4ca796245.exe	4
D:\Personal OneDrive\OneDrive\Desktop\Malware for valkyrie\85a46e5b3e5f93a456439d5b37fd3fd3e1717db2a7b5162c008a94e4ca796245.exe	4

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x62090	0x62200	6.52614888554	04f451f230a10265cec3dc09e41c6153
DATA	0x64000	0x12a8	0x1400	3.9421617547	df63400172356b12e6ac974024b84499
BSS	0x66000	0x3b35	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0x6a000	0x2208	0x2400	4.88551804383	38353952405ede7a1311f4b86e56674b
.tls	0x6d000	0x10	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x6e000	0x18	0x200	0.20058190744	9bca93a5f348fdd721c8b63d983d3a6a
.reloc	0x6f000	0x74f0	0x7600	6.65319722635	3436ca5666e286f8843fddcda2bb593d
.rsrc	0x77000	0xb800	0xb800	4.01156674695	4a39c7203e86bccf8d8df936d0b7be08