xcitium

!

PUA
Xcitium Final Verdict

File Name: 69c72aaa506368b23c93b30347c56a00f135645deeab5046c695579586eb7fcb.ex
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 0537f9741eaeb183d6e0e96719fb8f86912615f7
MD5: cd2543a1e63bc31315f59893f4607abf
First Seen Date: 2023-07-07 11:50:41 UTC
Number of Clients Seen: 3
Last Analysis Date: 2023-07-07 23:16:41 UTC
Human Expert Analysis Date: 2023-07-07 23:16:40 UTC
Human Expert Analysis Result: PUA
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2023-07-07 14:53:14 UTC	Malware	!
Static Analysis Overall Verdict	2023-07-07 23:16:41 UTC	Highly Suspicious	!
Precise Detectors Overall Verdict	2023-07-07 23:16:41 UTC	No Match	?
Human Expert Analysis Overall Verdict	2023-07-07 23:16:40 UTC	PUA	!
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	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

- Armadillo v1.71
- Microsoft Visual C++ v5.0/v6.0 (MFC)
- Microsoft Visual C++

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2023-07-07 11:50:22 UTC	No Match	?	NotDetected
Static Precise PUA Detector 4	2023-07-07 11:50:22 UTC	No Match	?	NotDetected
Static Precise NI Detector 3	2023-07-07 11:50:22 UTC	No Match	?	NotDetected
Static Precise PUA Detector 5	2023-07-07 11:50:22 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 1	2023-07-07 11:50:22 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 3	2023-07-07 11:50:22 UTC	No Match	?	NotDetected
Static Precise PUA Detector 6	2023-07-07 11:50:22 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 12	2023-07-07 11:50:22 UTC	No Match	?	NotDetected
Static Precise Virus Detector 1	2023-07-07 11:50:22 UTC	No Match	?	NotDetected
Static Precise Virus Detector 2	2023-07-07 11:50:22 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 13	2023-07-07 11:50:22 UTC	No Match	?	NotDetected
Static Precise PUA Detector 2	2023-07-07 11:50:22 UTC	No Match	?	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2023-07-07 12:55:55 UTC
Analysis End Date: 2023-07-07 23:16:40 UTC
File Upload Date: 2023-07-07 11:49:01 UTC
Human Expert Analyst Feedback:
Verdict: PUA
Malware Family:
Malware Type: Pua

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x3CC4C509 [Tue Apr 23 02:20:57 2002 UTC]
Debug Artifacts	
Entry Point	0x41be59 (UPX0)
Exifinfo	[object Object]
File Size	273156
File Type Enum	6
Imphash	08bca23b44274b89c6980b3fd0bc0ab9
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Product Version	5.1.0.0
File Version	5.1.0.0
Original Filename	divxenc.exe
File Description	
Translation	0x0409 0x04e4
Mime Type	application/x-dosexec
Number Of Sections	4
Sha256	69c72aaa506368b23c93b30347c56a00f135645deeab5046c695579586eb7fcb
Ssdeep	6144:jh8Z5hMWNFM8LAurlEzAX7oAwfSZ4sX9zQI:VEXM5qrllX7Xw2EI
Trid	27.1,Win32 Executable MS Visual C++ (generic),23.5,UPX compressed Win32 Executable,23,Win32 EXE Yoda's Crypter,11.3,Windows screen saver,5.7,Win32 Dynamic Link Library (generic)

File Paths

FILE PATH ON CLIENT	SEEN COUNT
Z:\Prevalent_Set_2023-07-A\Pua\69c72aaa506368b23c93b30347c56a00f135645deeab5046c695579586eb7fcb.ex$	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0x22000	0x22000	6.4613655026	6e585c2a2ea059302e83376c71db43a3
UPX1	0x23000	0x16000	0x15a00	4.00855873885	c3ec8c2070c3ac813709cef23f5b1796
.rsrc	0x39000	0x1000	0x600	2.76130880003	ee69ceaa897f3c8ede10c6ddf5c6dc8c
.htext	0x3a000	0x5000	0x5000	3.52040728913	a6c697b6c8f888a1ab486401a44a789a