xcitium

PUA
Xcitium Final Verdict

File Name: FMX_Automatic_Transmission_Diagnosis_Service_...exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: caaa052ae05d6032d8361e61fa22a686c6b5a392
MD5: 71eabe2172181c2e4517c30c22cb6d12
First Seen Date: 2023-01-02 23:39:04 UTC
Number of Clients Seen: 6
Last Analysis Date: 2023-06-29 10:07:27 UTC
Human Expert Analysis Date: 2023-06-29 10:07:27 UTC
Human Expert Analysis Result: PUA
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2023-06-29 10:07:27 UTC	PUA
Static Analysis Overall Verdict	2023-06-29 10:07:27 UTC	No Threat Found
Precise Detectors Overall Verdict	2023-06-29 10:07:27 UTC	No Match
Human Expert Analysis Overall Verdict	2023-06-29 10:07:27 UTC	PUA
File Certificate Validation		Vendor not found in Trusted List

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!	Clean
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Suspicious
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	Suspicious
TLS callback functions array detected	Clean

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	2023-01-02 23:39:00 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2023-01-02 23:39:00 UTC	No Match		NotDetected
Static Precise NI Detector 3	2023-01-02 23:39:00 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2023-01-02 23:39:00 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2023-01-02 23:39:00 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2023-01-02 23:39:00 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2023-01-02 23:39:00 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2023-01-02 23:39:00 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2023-01-02 23:39:00 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2023-01-02 23:39:00 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2023-01-02 23:39:00 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2023-01-02 23:39:01 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2023-01-03 10:10:59 UTC
Analysis End Date: 2023-06-29 10:07:27 UTC
File Upload Date: 2023-01-02 23:38:30 UTC
Human Expert Analyst Feedback:
Verdict: PUA
Malware Family:
Malware Type: Pua

Additional File Information

Vendor Validation - Not Verified ✖

[+] LIMESTONE DIGITAL LIMITED

Status	Not Valid ✖

Certificate Validation - Success ✔

[+] LIMESTONE DIGITAL LIMITED

Status	NoError ✔
Start Date	2022-10-12 19:50:16
End Date	2023-10-12 19:48:39
Sha256	9d8d93f10c9145b71ecac9164ac268779b0e22a51d88adb6a017c4905ea60818
Serial	4D2DC3C461FF097059BC7440DAC6207B
Subject Name	LIMESTONE DIGITAL LIMITED
Subject Key Identifier	98 67 c3 86 29 f1 7f 9c 0a 1e c7 a4 77 f0 bd 0f e6 70 eb 72
Subject Organization	LIMESTONE DIGITAL LIMITED
Subject Locality	Stoke-On-Trent
Subject Country	GB
Issuer Name	SSL.com EV Code Signing Intermediate CA RSA R3
Issuer Key Identifier	36 bd 49 ff 31 2c eb af 6a 40 fe 99 c0 16 ed ba fc 48 dd 5f
Issuer Organization	SSL Corp
Issuer Locality	Houston
Issuer State	Texas
Issuer Country	US
Crl link	http://crls.ssl.com/SSLcom-SubCA-EV-CodeSigning-RSA-4096-R3.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] SSL.com EV Code Signing Intermediate CA RSA R3

Status	NoError ✔
Start Date	2019-03-26 19:44:23
End Date	2034-03-22 19:44:23
Sha256	2c97d43d97ac766d1acf3cbd761985f121105be1aa3b2e8d39f704533915634c
Serial	424B6A53CEC766141C2A63B1A51C4104
Subject Name	SSL.com EV Code Signing Intermediate CA RSA R3
Subject Key Identifier	36 bd 49 ff 31 2c eb af 6a 40 fe 99 c0 16 ed ba fc 48 dd 5f
Subject Organization	SSL Corp
Subject Locality	Houston
Subject State	Texas
Subject Country	US
Issuer Name	SSL.com EV Root Certification Authority RSA R2
Issuer Key Identifier	f9 60 bb d4 e3 d5 34 f6 b8 f5 06 80 25 a7 73 db 46 69 a8 9e
Issuer Organization	SSL Corporation
Issuer Locality	Houston
Issuer State	Texas
Issuer Country	US
Crl link	http://crls.ssl.com/SSLcom-RootCA-EV-RSA-4096-R2.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] SSL.com EV Root Certification Authority RSA R2

Status	NoError ✔
Start Date	2017-05-31 21:14:37
End Date	2042-05-30 21:14:37
Sha256	e990def57fffd366fa099377f10e7c620e78daef67575d12d5f3655578349a6d
Serial	56B629CD34BC78F6
Subject Name	SSL.com EV Root Certification Authority RSA R2
Subject Key Identifier	f9 60 bb d4 e3 d5 34 f6 b8 f5 06 80 25 a7 73 db 46 69 a8 9e
Subject Organization	SSL Corporation
Subject Locality	Houston
Subject State	Texas
Subject Country	US
Issuer Name	SSL.com EV Root Certification Authority RSA R2
Issuer Key Identifier	f9 60 bb d4 e3 d5 34 f6 b8 f5 06 80 25 a7 73 db 46 69 a8 9e
Issuer Organization	SSL Corporation
Issuer Locality	Houston
Issuer State	Texas
Issuer Country	US
Crl link	undefined
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	undefined

[+] DigiCert Trusted Root G4

Status	NoError ✔
Start Date	2022-08-01 03:00:00
End Date	2031-11-10 01:59:59
Sha256	7db041d3e5a28c7e2100661b0a0dd9ad92b88e2736cfa807977ca7c02b3abec8
Serial	0E9B188EF9D02DE7EFDB50E20840185A
Subject Name	DigiCert Trusted Root G4
Subject Key Identifier	ec d7 e3 82 d2 71 5d 64 4c df 2e 67 3f e7 ba 98 ae 1c 0f 4f
Subject Organization	DigiCert Inc
Subject Country	US
Subject Organizational Unit	www.digicert.com
Issuer Name	DigiCert Assured ID Root CA
Issuer Key Identifier	45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f
Issuer Organization	DigiCert Inc
Issuer Country	US
Issuer Organizational Unit	www.digicert.com
Crl link	http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	undefined

[+] DigiCert Assured ID Root CA

Status	NoError ✔
Start Date	2006-11-10 02:00:00
End Date	2031-11-10 02:00:00
Sha256	69656a6548d46f112fad68a56675b12667e863fe923f84fb47014c2cc5352b40
Serial	0CE7E0E517D846FE8FE560FC1BF03039
Subject Name	DigiCert Assured ID Root CA
Subject Key Identifier	45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f
Subject Organization	DigiCert Inc
Subject Country	US
Subject Organizational Unit	www.digicert.com
Issuer Name	DigiCert Assured ID Root CA
Issuer Key Identifier	45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f
Issuer Organization	DigiCert Inc
Issuer Country	US
Issuer Organizational Unit	www.digicert.com
Crl link	undefined
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	undefined

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5F5DDFC3 [Sun Sep 13 09:00:51 2020 UTC]
Debug Artifacts	
Entry Point	0x4b5eec (.itext)
Exifinfo	
File Size	25461096
File Type Enum	6
Imphash	
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	
File Version	
Company Name	Limestone
Comments	This installation was built with Inno Setup.
Product Name	Installer
Product Version	1.0
File Description	Installer Setup
Original File Name	
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	10
Sha256	147e1b5a750fbfd8863449d523e3d6d110defceb74ad9cdb7c939ab75ffa2180
Ssdeep	
Trid	

File Paths

FILE PATH ON CLIENT	SEEN COUNT
C:\Users\CalgaryMaint\Desktop\FMX Automatic Transmission Diagnosis Service ...exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xb361c	0xb3800	6.35605820433	ad6e46e3a3acdb533eb6a077f6d065af
.itext	0xb5000	0x1688	0x1800	5.97275005522	d40fc822339d01f2abcc5493ac101c94
.data	0xb7000	0x37a4	0x3800	5.04440056201	4c195d5591f6d61265df08a3733de3a2
.bss	0xbb000	0x6de8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xc2000	0xf36	0x1000	4.89870464796	a73d686f1e8b9bb06ec767721135e397
.didata	0xc3000	0x1a4	0x200	2.75636286825	41b8ce23dd243d14beebc71771885c89
.edata	0xc4000	0x9a	0x200	1.87222286659	37c1a5c63717831863e018c0f51dabb7
.tls	0xc5000	0x18	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0xc6000	0x5d	0x200	1.38389437522	8f2f090acd9622c88a6a852e72f94e96
.rsrc	0xc7000	0x4800	0x4800	4.42031310958	6035bf047fc992a22e0bdc7eced636e6