xcitium

!

MALWARE
Xcitium Final Verdict

File Name: LixoDestructive.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 2add11e25d07dc9e154ae1be916c869804047146
MD5: 7d538a430eb4e0bfd7671b921a8b76a1
First Seen Date: 2023-05-02 13:15:25 UTC
Number of Clients Seen: 4
Last Analysis Date: 2023-05-03 18:55:31 UTC
Human Expert Analysis Date: 2023-05-03 18:54:37 UTC
Human Expert Analysis Result: Malware
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2023-05-03 18:55:31 UTC	Malware	!
Static Analysis Overall Verdict	2023-05-03 18:55:31 UTC	No Threat Found	?
Precise Detectors Overall Verdict	2023-05-03 18:55:31 UTC	No Match	?
Human Expert Analysis Overall Verdict	2023-05-03 18:54:37 UTC	Malware	!
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	✓

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	2023-05-03 18:55:27 UTC	No Match	?	NotDetected
Static Precise PUA Detector 4	2023-05-03 18:55:27 UTC	No Match	?	NotDetected
Static Precise NI Detector 3	2023-05-03 18:55:27 UTC	No Match	?	NotDetected
Static Precise PUA Detector 5	2023-05-03 18:55:27 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 1	2023-05-03 18:55:27 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 3	2023-05-03 18:55:27 UTC	No Match	?	NotDetected
Static Precise PUA Detector 6	2023-05-03 18:55:27 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 12	2023-05-03 18:55:27 UTC	No Match	?	NotDetected
Static Precise Virus Detector 1	2023-05-03 18:55:27 UTC	No Match	?	NotDetected
Static Precise Virus Detector 2	2023-05-03 18:55:27 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 13	2023-05-03 18:55:27 UTC	No Match	?	NotDetected
Static Precise PUA Detector 2	2023-05-03 18:55:27 UTC	No Match	?	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2023-05-02 14:36:26 UTC
Analysis End Date: 2023-05-03 18:54:37 UTC
File Upload Date: 2023-05-02 13:14:41 UTC
Human Expert Analyst Feedback: -
Verdict: Malware
Malware Family:
Malware Type: Trojan Generic

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x64223EF1 [Tue Mar 28 01:12:17 2023 UTC]
Debug Artifacts	
Entry Point	0x407f6d (.text)
Exifinfo	
File Size	484352
File Type Enum	6
Imphash	
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Mime Type	application/x-dosexec
Number Of Sections	6
Sha256	3a4ea5e72e50bcba550efa034818f35785076adb37af4c1cee9374fe9e013ec1
Ssdeep	
Trid	

File Paths

FILE PATH ON CLIENT	SEEN COUNT
LixoDestructive.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x489d0	0x48a00	6.63352370442	dd7150650ce709ab2dc703342af33dc7
.rdata	0x4a000	0xf69c	0xf800	5.75183497883	7c186d4c6b5714ed3bf4f4f081dd4755
.data	0x5a000	0x1cf0	0xa00	2.46526476329	0fe90a099face26e50573e8f8f491640
.msvcjmc	0x5c000	0x16	0x200	0.255742020076	85bb7567c9540c02a36ab2534359c3af
.rsrc	0x5d000	0x1a4b8	0x1a600	5.95991151638	a4944c494e0465bf8a3bac0c21fd686c
.reloc	0x78000	0x2b60	0x2c00	6.69701565351	e0240d393546e7014d03aa140aacd7ef