xcitium

MALWARE
Xcitium Final Verdict

File Name: Luxuria.exe
File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1: 997a45a3707dd6ac76765664503576d3f6a37cb3
MD5: 0ffb5f463f6c63d11a48d2b4ef3be8dd
First Seen Date: 2024-05-05 13:52:00 UTC
Number of Clients Seen: 3
Last Analysis Date: 2024-05-06 16:19:58 UTC
Human Expert Analysis Date: 2024-05-06 16:19:27 UTC
Human Expert Analysis Result: Malware
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2024-05-06 16:19:58 UTC	Malware
Static Analysis Overall Verdict	2024-05-06 16:19:58 UTC	No Threat Found
Precise Detectors Overall Verdict	2024-05-06 16:19:58 UTC	No Match
Human Expert Analysis Overall Verdict	2024-05-06 16:19:27 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	Suspicious
Illegal size of optional Header	Clean
Packer detection on signature database	Unknown
Based on the sections entropy check! file is possibly packed	Suspicious
Timestamp value suspicious	Suspicious
Header Checksum is zero!	Suspicious
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	Clean
TLS callback functions array detected	Clean

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Has no visible windows	

Behavioral Information

LoadLibrary

ADVAPI32.dll
SHLWAPI.dll

OpenRegistryKey

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NE
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFra
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\M
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Micro

QueryFilePath

C:\Windows\SYSTEM32\MSCOREE.DLL
C:\Luxuria.exe

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2024-05-05 13:54:26 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2024-05-05 13:54:26 UTC	No Match		NotDetected
Static Precise NI Detector 3	2024-05-05 13:54:26 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2024-05-05 13:54:26 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2024-05-05 13:54:26 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2024-05-05 13:54:26 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2024-05-05 13:54:26 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2024-05-05 13:54:26 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2024-05-05 13:54:26 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2024-05-05 13:54:26 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2024-05-05 13:54:26 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2024-05-05 13:54:26 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2024-05-06 13:58:24 UTC
Analysis End Date: 2024-05-06 16:19:27 UTC
File Upload Date: 2024-05-05 13:51:22 UTC
Human Expert Analyst Feedback: Trojware
Verdict: Malware

Malware Family: Generic
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	0xAE8C39C6 [Wed Oct 18 19:30:14 2062 UTC] [SUSPICIOUS]
Debug Artifacts	
Entry Point	0x5fc00a ()
Exifinfo	[object Object]
File Size	2059280
File Type Enum	6
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Translation	0x0000 0x04b0
Legal Copyright	Copyright \xa9 2024
Assembly Version	1.0.0.0
Internal Name	AutoLauncher.exe
File Version	1.0.0.0
Company Name	
Legal Trademarks	
Comments	
Product Name	Luxuria
Product Version	1.0.0.0
File Description	Luxuria
Original Filename	AutoLauncher.exe
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	ae3da52225038e4f4ad470079fa2c2c08a3481456e1734e3953e539bdedc1ea3
Ssdeep	49152:ZWFxPJFPcZYQKes8mugsPngHr79/Hx8vkXhWF+DDxaUKY:ZoxPyw8mRPmvRF4DQ4
Trid	61.9,Win32 Executable MS Visual C++ (generic),13,Win32 Dynamic Link Library (generic),8.9,Win32 Executable (generic),4.1,Win16/32 Executable Delphi generic,4,OS/2 Executable (generic)

File Paths

FILE PATH ON CLIENT	SEEN COUNT
997a45a3707dd6ac76765664503576d3f6a37cb3	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
"`j+"t\	0x2000	0x74	0x200	7.66655983521	1195df2a2080004d970ea835d65f7626
.text	0x4000	0x1f0fbc	0x1f1000	7.98582700111	a9fc25c6e0288f6f4f04449b296d78ac
.UN]M6	0x1f6000	0x5172	0x5200	7.82232696925	faf8fc9418aae050a8b6f79e8e2a4d96
	0x1fc000	0x10	0x200	0.118369631259	d1fe83af3b534a501051bc91a03c10cd
.reloc	0x1fe000	0xc	0x200	0.0980041756627	a4fe72978ba527f1ceb38d4fe8ad726f