xcitium

MALWARE
Xcitium Final Verdict

File Name: 6c7a2124b7076383f577eb0042f9ea917b2b4066
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 6c7a2124b7076383f577eb0042f9ea917b2b4066
MD5: 8432070440b9827f88a75bef7e65dd60
First Seen Date: 2024-10-09 06:33:18 UTC
Number of Clients Seen: 3
Last Analysis Date: 2024-10-09 14:40:15 UTC
Human Expert Analysis Date: 2024-10-09 14:39:52 UTC
Human Expert Analysis Result: Malware
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2024-10-09 14:40:15 UTC	Malware
Static Analysis Overall Verdict	2024-10-09 14:40:15 UTC	No Match
Dynamic Analysis Overall Verdict	2024-10-09 14:40:15 UTC	Highly Suspicious
Precise Detectors Overall Verdict	2024-10-09 14:40:15 UTC	No Match
Human Expert Analysis Overall Verdict	2024-10-09 14:39:52 UTC	Malware
File Certificate Validation		Not Applicable

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT

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	Suspicious
TLS callback functions array detected	Clean

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	

SUSPICIOUS BEHAVIORS	
Creates a child process	
Writes to address space of another process	
Logs user key strokes	
Reads memory of another process	
Opens a file in a system directory	
Has no visible windows	

Behavioral Information

QueryFilePath

C:\6c7a2124b7076383f577eb0042f9ea917b2b4066
C:\Windows\system32\RichEd20.DLL
C:\Windows\SysWOW64\ieframe.dll
C:\Windows\system32\propsys.dll

LowerChar

.exe
program
file

CreateProcess

"C:\Windows\System32\cmd.exe" /c move Tall Tall.bat & Tall.bat

ReadFile

C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000010.db
C:\Users\win7\Desktop\desktop.ini
C:\6c7a2124b7076383f577eb0042f9ea917b2b4066

DeleteFile

C:\Users\win7\AppData\Local\Temp\nsnD11.tmp

WriteFile

C:\Users\win7\AppData\Local\Temp\Norwegian
C:\Users\win7\AppData\Local\Temp\Booty
C:\Users\win7\AppData\Local\Temp\Picking
C:\Users\win7\AppData\Local\Temp\Awareness
C:\Users\win7\AppData\Local\Temp\Distributor
C:\Users\win7\AppData\Local\Temp\Tours
C:\Users\win7\AppData\Local\Temp\Mysql
C:\Users\win7\AppData\Local\Temp\Tall

CreateMutex

<NULL>
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex

LoadLibrary

imm32.dll
SHFOLDER
ole32.dll
comctl32.dll
ADVAPI32.dll
SHELL32.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
propsys.dll
ntmarta.dll
RichEd20
C:\Windows\SysWOW64\ieframe.dll
kernel32.dll
Secur32.dll
API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL
OLEAUT32.dll

OpenRegistryKey

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Win
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN
\REGISTRY\MACHINE\SOFTWARE\Wow64
\REGISTRY\USER\.DEFAULT\Control Panel\Desktop

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2024-10-09 06:32:47 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2024-10-09 06:32:47 UTC	No Match		NotDetected
Static Precise NI Detector 3	2024-10-09 06:32:47 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2024-10-09 06:32:47 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2024-10-09 06:32:48 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2024-10-09 06:32:47 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2024-10-09 06:32:48 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2024-10-09 06:32:48 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2024-10-09 06:32:48 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2024-10-09 06:32:48 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2024-10-09 06:32:48 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2024-10-09 06:32:48 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2024-10-09 08:33:53 UTC
Analysis End Date: 2024-10-09 14:39:52 UTC

File Upload Date: 2024-10-09 07:31:47 UTC
Human Expert Analyst Feedback:
Verdict: Malware
Malware Family: Trojware
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	0x4F47E2DA [Fri Feb 24 19:19:54 2012 UTC]
Debug Artifacts	
Entry Point	0x403883 (.text)
Exifinfo	
File Size	874887
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	459443def8fd0c940b2da33d9703fcf5771dbcd9ce4aff2dcc670528c1d1d3c1
Ssdeep	
Trid	

File Paths

FILE PATH ON CLIENT	SEEN COUNT
file/to/path	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x6dae	0x6e00	6.50852956314	00499a6f70259150109c809d6aa0e6ed
.rdata	0x8000	0x2a62	0x2c00	4.39053502099	07990aaa54c3bc638bb87a87f3fb13e3
.data	0xb000	0x67ebc	0x200	1.43086025975	014871d9a00f0e0c8c2a7cd25606c453
.ndata	0x73000	0x81000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0xf4000	0x11c98	0x11e00	2.28583914595	b408de031817d1136bd7732c539d10c4
.reloc	0x106000	0xf32	0x1000	2.69496540588	6261b615407e8c1bebc009ac8b3f594c