xcitium

MALWARE
Xcitium Final Verdict

File Name: crazydown.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: e953cba0da973e377aa364b9dd08e03c530c2cc3
MD5: 31e8dd7f62b0d6210b603e64c438c120
First Seen Date: 2023-06-30 09:03:44 UTC
Number of Clients Seen: 7
Last Analysis Date: 2023-07-02 19:48:31 UTC
Human Expert Analysis Date: 2023-07-02 19:48:28 UTC
Human Expert Analysis Result: Malware
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2023-07-01 08:17:46 UTC	Malware
Static Analysis Overall Verdict	2023-07-02 19:48:31 UTC	No Threat Found
Precise Detectors Overall Verdict	2023-07-02 19:48:31 UTC	No Match
Human Expert Analysis Overall Verdict	2023-07-02 19:48:28 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	Suspicious
TLS callback functions array detected	Clean

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Opens a file in a system directory	❗
Has no visible windows	❗

Behavioral Information

LoadLibrary

imm32.dll
C:\Windows\system32\UXTHEME.dll
C:\Windows\system32\USERENV.dll
C:\Windows\system32\SETUPAPI.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
advapi32.dll
C:\Windows\system32\APPHELP.dll
C:\Windows\system32\PROPSYS.dll
ADVAPI32.dll
propsys.dll
C:\Windows\system32\DWMAPI.dll
C:\Windows\system32\CRYPTBASE.dll
C:\Windows\system32\OLEACC.dll
OLEACCRC.DLL
C:\Windows\system32\CLBCATQ.dll
C:\Windows\system32\NTMARTA.dll
C:\Windows\system32\SHFOLDER.dll
ole32.dll
comctl32.dll
SHELL32.dll
ntmarta.dll
C:\Windows\system32\IconCodecService.dll
WindowsCodecs.dll
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\nsis7z.dll
api-ms-win-core-synch-l1-2-0
kernel32
api-ms-win-core-fibers-l1-1-1
api-ms-win-core-localization-l1-2-1
api-ms-win-appmodel-runtime-l1-1-2

CreateMutex

<NULL>

WriteFile

C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\v8_context_snapshot.bin
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\fil.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\te.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\ta.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\mr.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\tr.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\vk_swiftshader_icd.json
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\nsis7z.dll
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\chrome_100_percent.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\zh-CN.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\es-419.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\LICENSE.electron.txt
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy\browser.js
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\en-US.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\pt-BR.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy\fallbacks
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\et.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\ko.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\it.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\app-64.7z
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\sk.pak

C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\ca.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\sl.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\fi.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy\fallbacks\linux\xsel
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy\lib\linux.js
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\cs.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy\fallbacks\linux
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\id.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\icudtl.dat
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\bg.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\gu.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\ja.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\sw.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\en-GB.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\pl.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\de.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\am.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\fr.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\nb.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\kn.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy\package.json
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\el.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy\lib
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\th.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy\fallbacks\windows
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\vi.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy\license
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\ml.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\libGLESv2.dll
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\hu.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\es.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\zh-TW.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy\lib\termux.js
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\ur.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\ru.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy\lib\macos.js
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\bn.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\ffmpeg.dll
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\sv.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\libEGL.dll
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\uk.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\chrome_200_percent.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\ms.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\LICENSES.chromium.html
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy\lib\windows.js
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\ar.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\sr.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\ro.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\pt-PT.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\fa.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\nl.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\da.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\snapshot_blob.bin
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\lt.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy\index.js
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\resources\app.asar.unpacked\node_modules\clipboardy
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\hr.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\af.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\lv.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\he.pak
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\7z-out\locales\hi.pak

ReadFile

C:\crazydown.exe
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\app-64.7z
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp\nsis7z.dll

QueryFilePath

C:\crazydown.exe

DeleteFile

C:\Users\win7\AppData\Local\Temp\nsw7100.tmp
C:\Users\win7\AppData\Local\Temp\nsb716E.tmp

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2023-07-01 08:17:46 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2023-07-01 08:17:47 UTC	No Match		NotDetected
Static Precise NI Detector 3	2023-07-01 08:17:47 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2023-07-01 08:17:47 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2023-07-01 08:17:47 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2023-07-01 08:17:47 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2023-07-01 08:17:47 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2023-07-01 08:17:47 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2023-07-01 08:17:47 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2023-07-01 08:17:47 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2023-07-01 08:17:47 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2023-07-01 08:17:47 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2023-06-30 10:06:26 UTC
Analysis End Date: 2023-07-02 19:48:28 UTC
File Upload Date: 2023-06-30 09:02:44 UTC
Human Expert Analyst Feedback:
Verdict: Malware
Malware Family:
Malware Type: 0

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5C157F86 [Sat Dec 15 22:26:14 2018 UTC]
Debug Artifacts	
Entry Point	0x40338f (.text)
Exifinfo	[object Object]
File Size	70817952
File Type Enum	6
Imphash	b34f154ec913d2d2c435cbd644e91687
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	Copyright \xa9 2023 evil
File Version	1.0.0
Company Name	evil
Product Name	build
Product Version	1.0.0
File Description	evil
Translation	0x0409 0x04e4
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	dca13fc006a3b55756ae0534bd0d37a1b53a219b5d7de236f20b0262f3662659
Ssdeep	1572864:8KTTF204vwsTTPn8chTPO8vJ4n1vy0XTDrz3mN1LrtXubAptsDilNoR07:TXF204v9n8chHuv7TD/2Tr4bgtsMNoS7
Trid	67.4,Win32 Executable MS Visual C++ (generic),14.2,Win32 Dynamic Link Library (generic),9.7,Win32 Executable (generic),4.3,Generic Win/DOS Executable,4.3,DOS Executable Generic

File Paths

FILE PATH ON CLIENT	SEEN COUNT
crazydown.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x6627	0x6800	6.45028234851	7618d4c0cd8bb67ea9595b4266b3a91f
.rdata	0x8000	0x14a2	0x1600	5.02517892911	eecac1fed9cc6b447d50940d178404d8
.data	0xa000	0x70ff8	0x600	4.03711773145	db8f31a08a2242d80c29e1f9500c6527
.ndata	0x7b000	0x90000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x10b000	0xb360	0xb400	7.92477617063	addf49233d9c76c8c514188e9cd7a352