xcitium

PUA
Xcitium Final Verdict

File Name: 2023-03-01_8efccd45c79b053ace1c9691a3add9da_mafia
File Type: PE32 executable (console) Intel 80386, for MS Windows
SHA1: 40f40a99ea7be53397a801921abbd77a1f9abc64
MD5: 8efccd45c79b053ace1c9691a3add9da
First Seen Date: 2023-03-15 13:27:27 UTC
Number of Clients Seen: 3
Last Analysis Date: 2023-03-15 18:42:41 UTC
Human Expert Analysis Date: 2023-03-15 18:42:34 UTC
Human Expert Analysis Result: PUA
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2023-03-15 17:18:41 UTC	Malware
Static Analysis Overall Verdict	2023-03-15 18:42:41 UTC	No Threat Found
Precise Detectors Overall Verdict	2023-03-15 18:42:41 UTC	No Match
Human Expert Analysis Overall Verdict	2023-03-15 18:42:34 UTC	PUA
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!	Clean
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean
Anti-vm present	Suspicious
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
Highly Suspicious	

SUSPICIOUS BEHAVIORS	
Installs a driver	!
Installs a kernel/file system driver	!
Modifies Windows Service Keys	!
Has no visible windows	!

Behavioral Information

CreateService

OpenService

LoadLibrary

Wtsapi32.dll

QueryFilePath

C:\2023-03-01_8efccd45c79b053ace1c9691a3add9da_mafia

OpenRegistryKey

\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\TCPIP6\P
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\GroupOrderLis
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\tdx
\REGISTRY\MACHINE\SYSTEM\ControlSet001\services

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2023-03-15 13:27:21 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2023-03-15 13:27:21 UTC	No Match		NotDetected
Static Precise NI Detector 3	2023-03-15 13:27:21 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2023-03-15 13:27:21 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2023-03-15 13:27:21 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2023-03-15 13:27:21 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2023-03-15 13:27:22 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2023-03-15 13:27:22 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2023-03-15 13:27:22 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2023-03-15 13:27:22 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2023-03-15 13:27:22 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2023-03-15 13:27:22 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2023-03-15 14:40:42 UTC
Analysis End Date: 2023-03-15 18:42:34 UTC
File Upload Date: 2023-03-15 13:26:46 UTC
Human Expert Analyst Feedback:
Verdict: PUA
Malware Family:
Malware Type: Pua

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x54796616 [Sat Nov 29 06:22:14 2014 UTC]
Debug Artifacts	
Entry Point	0x4213ae (.text)
Exifinfo	[object Object]
File Size	296224
File Type Enum	6
Imphash	5a3059a8a0dd70a76ef776580685cce4
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	1
Legal Copyright	
Internal Name	
File Version	1, 1, 1, 0
Company Name	
Product Name	
Product Version	1, 1, 1, 0
File Description	
Original Filename	
Translation	0x0419 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	c431e7f789b17dd9879f02e4559dd713bad6eb4958f8be64f0d5da822199ac9d
Ssdeep	6144:Jk0tnURexVtDLJJtYd1RSWRotvcTB5E8Gl:60tnUReNDLJJtYd1RSWRotvcTr+l
Trid	42.2,Win32 Executable MS Visual C++ (generic),37.3,Win64 Executable (generic),8.8,Win32 Dynamic Link Library (generic),6,Win32 Executable (generic),2.7,Generic Win/DOS Executable

File Paths

FILE PATH ON CLIENT	SEEN COUNT
2023-03-01_8efccd45c79b053ace1c9691a3add9da_mafia	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x348b8	0x34a00	6.63336789556	a1dcf00bbf8b14fc9022bb4cd0ec7230
.rdata	0x36000	0xc2c4	0xc400	5.62897350206	ceda9ce3257cebbc57b99900ab5bf110
.data	0x43000	0x4464	0x1c00	4.09340365582	b3cb1fc94b3468c188c7e2607ad25dc6
.rsrc	0x48000	0x440	0x600	4.58177873263	a23f62b767b4ef51cee21c493e7fe22e
.reloc	0x49000	0x379e	0x3800	5.55165767203	35181fccdf47c0ee939cf6803697ca89

PE Imports

- KERNEL32.dll
  - ReadFile
  - GetOverlappedResult
  - GetLastError
  - GetProcAddress

- ResetEvent
- DeviceIoControl
- WaitForMultipleObjects
- GetModuleHandleA
- CancelIo
- GetCurrentProcessId
- CreateEventA
- GetFileSize
- SetFilePointer
- SetEndOfFile
- CreateFileW
- GetTempFileNameW
- GetTempPathW
- CreateDirectoryW
- FreeLibrary
- LoadLibraryA
- ProcessIdToSessionId
- OpenProcess
- WriteFile
- GetTickCount
- SetEvent
- WaitForSingleObject
- DeleteCriticalSection
- EnterCriticalSection
- LeaveCriticalSection
- InitializeCriticalSection
- CloseHandle
- CreateToolhelp32Snapshot
- SetConsoleCtrlHandler
- Process32Next
- Sleep
- Process32First
- CreateFileA
- ExitProcess
- WriteConsoleW
- SetStdHandle
- LoadLibraryW
- GetStringTypeW

- IsValidLocale
- EnumSystemLocalesA
- GetLocaleInfoA
- GetUserDefaultLCID
- InterlockedIncrement
- InterlockedDecrement
- EncodePointer
- DecodePointer
- HeapFree
- DeleteFileA
- GetSystemTimeAsFileTime
- HeapAlloc
- ExitThread
- GetCurrentThreadId
- CreateThread
- HeapReAlloc
- GetCommandLineA
- HeapSetInformation
- RaiseException
- RtlUnwind
- WideCharToMultiByte
- LCMapStringW
- MultiByteToWideChar
- GetCPInfo
- TerminateProcess
- GetCurrentProcess
- UnhandledExceptionFilter
- SetUnhandledExceptionFilter
- IsDebuggerPresent
- SetHandleCount
- GetStdHandle
- InitializeCriticalSectionAndSpinCount
- GetFileType
- GetStartupInfoW
- IsProcessorFeaturePresent
- HeapCreate
- GetModuleHandleW

- GetConsoleCP
- GetConsoleMode
- FlushFileBuffers
- TlsAlloc
- TlsGetValue
- TlsSetValue
- TlsFree
- SetLastError
- GetModuleFileNameW
- GetACP
- GetOEMCP
- IsValidCodePage
- GetLocaleInfoW
- HeapSize
- GetModuleFileNameA
- FreeEnvironmentStringsW
- GetEnvironmentStringsW
- QueryPerformanceCounter
- GetProcessHeap

ADVAPI32.dll

- LookupAccountSidA
- GetTokenInformation
- RegCloseKey
- OpenSCManagerA
- RegOpenKeyExA
- StartServiceA
- CreateServiceA
- RegQueryValueExA
- RegSetValueExA
- DeleteService
- CloseServiceHandle
- OpenServiceA
- AdjustTokenPrivileges
- LookupPrivilegeValueA
- OpenProcessToken
- LookupAccountSidW

PSAPI.DLL

GetModuleFileNameExA

WS2_32.dll

WSAAddressToStringA

WSACleanup

WSAStartup

htons

PE Exports

?STObject_create@StLibs@@YAPAVSTObject@1@HH@Z

?pf_addFilter@StLibs@@YAH_KW4_ST_FilterType@1@KW4_ST_OpTarget@1@1@Z

?pf_canDisableFiltering@StLibs@@YAH_K@Z

?pf_deleteFilter@StLibs@@YAH_KW4_ST_FilterType@1@@Z

?pf_free@StLibs@@YAXXZ

?pf_getFilterCount@StLibs@@YAH_K@Z

?pf_getNFEventHandler@StLibs@@YAPAVNF_EventHandler@stapi@@XZ

?pf_getProcessOwnerA@StLibs@@YAHKPADH@Z

?pf_getProcessOwnerW@StLibs@@YAHKPA_WH@Z

?pf_init@StLibs@@YAHPAVSTEvents@1@PB_W@Z

?pf_isFilterActive@StLibs@@YAH_KW4_ST_FilterType@1@@Z

?pf_postObject@StLibs@@YAH_KPAVSTObject@1@@Z

?pf_setRootSSLCertSubject@StLibs@@YAXPBD@Z

?pf_unzipStream@StLibs@@YAHPAVSTStream@1@@Z

PE Resources

[object Object]
[object Object]