xcitium

MALWARE
Xcitium Final Verdict

File Name: 63ebbfac1ae03d7db04bf55523f07f3f4aa2b534
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 63ebbfac1ae03d7db04bf55523f07f3f4aa2b534
MD5: f734d3c885625d361b085cfc8af1fc25
First Seen Date: 2024-10-17 06:25:08 UTC
Number of Clients Seen: 2
Last Analysis Date: 2024-10-17 10:40:07 UTC
Human Expert Analysis Date: 2024-10-17 10:40:05 UTC
Human Expert Analysis Result: Malware
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2024-10-17 10:40:07 UTC	Malware
Static Analysis Overall Verdict	2024-10-17 10:40:07 UTC	No Threat Found
Dynamic Analysis Overall Verdict	2024-10-17 10:40:07 UTC	No Threat Found
Precise Detectors Overall Verdict	2024-10-17 10:40:07 UTC	No Match
Human Expert Analysis Overall Verdict	2024-10-17 10:40:05 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	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	Suspicious
TLS callback functions array detected	Clean

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Creates a child process	
Reads memory of another process	
Writes to address space of another process	
Uses a function clandestinely	
Downloads data from internet	
Opens a file in a system directory	
Has no visible windows	

Behavioral Information

LoadLibrary

ADVAPI32.dll
kernel32.dll
Msctf.dll
imm32.dll
wtsapi32.dll
USER32.dll
WINSTA.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
RPCRT4.dll
uxtheme.dll
C:\Windows\system32\uxtheme.dll
C:\Windows\system32\shell32.dll
C:\Windows\system32\shfolder.dll
C:\Windows\system32\Rstrtmgr.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
C:\Users\win7\AppData\Local\Temp\is-UMOEU.tmp\idp.dll
Secur32.dll
SHELL32.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
WS2_32.dll
winhttp.dll
IPHLPAPI.DLL
CRYPTBASE.dll
CRYPT32.dll
USERENV.dll
api-ms-win-downlevel-shlwapi-l2-1-0.dll
RASAPI32.dll
shlwapi.dll
DNSAPI.dll
ole32.dll
OLEAUT32.dll
dhcpcsvc.DLL
urlmon.dll
Comctl32.dll
C:\Windows\system32\ws2_32
secur32.dll
ncrypt.dll
WINTRUST.dll
CRYPTSP.dll
cryptnet.dll
C:\Windows\system32\cryptnet.dll
SensApi.dll
SHLWAPI.dll
WINHTTP.dll
SspiCli.dll
ntdll.dll
NSI.dll
CFGMGR32.dll
API-MS-Win-Security-SDDL-L1-1-0.dll
profapi.dll

API-MS-WIN-Service-Management-L1-1-0.dll
API-MS-WIN-Service-winsvc-L1-1-0.dll
setupapi.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
advapi32.dll
Cabinet.dll
DEVRTL.dll
C:\Windows\syswow64\CRYPT32.dll

LowerChar

3ebbfac1ae03d7db04bf55523f07f3f4aa2b534
http

CreateProcess

"C:\Windows\system32\cmd.exe" /C ""C:\Users\win7\AppData\Local\Temp\is-UMOEU.tmp\my.bat""

InternetDownload

cc000c

ReadFile

C:\Users\win7\AppData\Local\Temp\is-UMOEU.tmp\my.bat
C:\63ebbfac1ae03d7db04bf55523f07f3f4aa2b534
C:\Users\win7\AppData\Local\Temp\CabF29.tmp
C:\Users\win7\AppData\Local\Temp\TarF2A.tmp

DeleteFile

C:\Users\win7\AppData\Local\Temp\is-E4RC8.tmp\63ebbfac1ae03d7db04bf55523f07f3f4aa2b534.tmp
C:\Users\win7\AppData\Local\Temp\CabF29.tmp
C:\Users\win7\AppData\Local\Temp\TarF2A.tmp
C:\Users\win7\AppData\Local\Temp\is-UMOEU.tmp\idp.dll
C:\Users\win7\AppData\Local\Temp\is-UMOEU.tmp\my.bat
C:\Users\win7\AppData\Local\Temp\is-UMOEU.tmp_isetup_setup64.tmp

WriteFile

C:\Users\win7\AppData\Local\Temp\TarF2A.tmp
C:\63ebbfac1ae03d7db04bf55523f07f3f4aa2b534
C:\Users\win7\AppData\Local\Temp\is-UMOEU.tmp\idp.dll
C:\Users\win7\AppData\Local\Temp\CabF29.tmp
C:\Users\win7\AppData\Local\Temp\is-UMOEU.tmp_isetup_setup64.tmp

CreateMutex

Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000
RasPbFile
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
<NULL>

QueryFilePath

C:\Users\win7\AppData\Local\Temp\is-E4RC8.tmp\63ebbfac1ae03d7db04bf55523f07f3f4aa2b534.tmp

C:\Windows\SysWOW64\cmd.exe
C:\Windows\SysWOW64\schannel.dll
C:\Windows\system32\cryptnet.dll
C:\Windows\syswow64\CRYPT32.dll

OpenRegistryKey

\REGISTRY\USER\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_DISABLE_UNICODE_HANDLE_CLOSING_CALLBACK
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Win
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\PeerDist\Service
\REGISTRY\USER\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_MIME_HANDLING

QueryProcessAddress

IsDebuggerPresent

CreateRegistryKey

\REGISTRY\USER\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
\REGISTRY\USER\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
\REGISTRY\USER\.DEFAULT\SOFTWARE\Microsoft\RestartManager\Session0000
\REGISTRY\USER\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-12-35-02
\REGISTRY\USER\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{69DC4768-446B-4F82-A6B0-63966A243064}\52-54-00-12-35-02

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2024-10-17 06:24:35 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2024-10-17 06:24:35 UTC	No Match		NotDetected
Static Precise NI Detector 3	2024-10-17 06:24:35 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2024-10-17 06:24:35 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2024-10-17 06:24:35 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2024-10-17 06:24:35 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2024-10-17 06:24:35 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2024-10-17 06:24:35 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2024-10-17 06:24:35 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2024-10-17 06:24:35 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2024-10-17 06:24:35 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2024-10-17 06:24:35 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2024-10-17 08:42:55 UTC
Analysis End Date: 2024-10-17 10:40:05 UTC
File Upload Date: 2024-10-17 07:02:05 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	0x63ECF218 [Wed Feb 15 14:54:16 2023 UTC]
Debug Artifacts	
Entry Point	0x4b5eec (.itext)
Exifinfo	[object Object]
File Size	1764456
File Type Enum	6
Imphash	e569e6f445d32ba23766ad67d1e3787f
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	
File Version	
Company Name	
Comments	This installation was built with Inno Setup.
Product Name	OneInstaller
Product Version	1.0
File Description	OneInstaller Setup
Original File Name	
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	10
Sha256	1fc070d52f6c24eb6e83d5e9474d63868d47509a8aea3687782ebf61ebe97cfd
Ssdeep	24576:s7FUDowAyrTVE3U5F/3GqKXKic6QL3E2vVsjECUAQT45deRV9Rp:sBuZrEUqBKly029s4C1eH9L
Trid	53.5,Inno Setup installer,21,InstallShield setup,20.2,Win32 EXE PECompact compressed (generic),2.1,Win32 Executable (generic),1,Win16/32 Executable Delphi generic

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	0xb39e4	0xb3a00	6.35763504999	43af0a9476ca224d8e8461f1e22c94da
.itext	0xb5000	0x1688	0x1800	5.97142542844	185e04b9a1f554e31f7f848515dc890c
.data	0xb7000	0x37a4	0x3800	5.04864859437	cab2107c933b696aa5cf0cc6c3fd3980
.bss	0xbb000	0x6de8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xc2000	0xfdc	0x1000	5.0290874811	e7d1635e2624b124cfdce6c360ac21cd
.didata	0xc3000	0x1a4	0x200	2.7509822286	8ced971d8a7705c98b173e255d8c9aa7
.edata	0xc4000	0x9a	0x200	1.8771629545	8d4e1e508031afe235bf121c80fd7d5f
.tls	0xc5000	0x18	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0xc6000	0x5d	0x200	1.38389437522	8f2f090acd9622c88a6a852e72f94e96
.rsrc	0xc7000	0x11000	0x11000	3.69262675545	c07ae3ae61166fbc7f4de436aa4603c4

PE Imports

- kernel32.dll
  - GetACP
  - GetExitCodeProcess
  - LocalFree
  - CloseHandle
  - SizeofResource
  - VirtualProtect
  - VirtualFree
  - GetFullPathNameW
  - ExitProcess
  - HeapAlloc
  - GetCPInfoExW
  - RtlUnwind
  - GetCPInfo
  - GetStdHandle
  - GetModuleHandleW
  - FreeLibrary
  - HeapDestroy
  - ReadFile
  - CreateProcessW
  - GetLastError
  - GetModuleFileNameW
  - SetLastError
  - FindResourceW

- CreateThread
- CompareStringW
- LoadLibraryA
- ResetEvent
- GetVersion
- RaiseException
- FormatMessageW
- SwitchToThread
- GetExitCodeThread
- GetCurrentThread
- LoadLibraryExW
- LockResource
- GetCurrentThreadId
- UnhandledExceptionFilter
- VirtualQuery
- VirtualQueryEx
- Sleep
- EnterCriticalSection
- SetFilePointer
- LoadResource
- SuspendThread
- GetTickCount
- GetFileSize
- GetStartupInfoW
- GetFileAttributesW
- InitializeCriticalSection
- GetSystemWindowsDirectoryW
- GetThreadPriority
- SetThreadPriority
- GetCurrentProcess
- VirtualAlloc
- GetSystemInfo
- GetCommandLineW
- LeaveCriticalSection
- GetProcAddress
- ResumeThread
- GetVersionExW

- VerifyVersionInfoW
- HeapCreate
- GetWindowsDirectoryW
- VerSetConditionMask
- GetDiskFreeSpaceW
- FindFirstFileW
- GetUserDefaultUILanguage
- lstrlenW
- QueryPerformanceCounter
- SetEndOfFile
- HeapFree
- WideCharToMultiByte
- FindClose
- MultiByteToWideChar
- LoadLibraryW
- SetEvent
- CreateFileW
- GetLocaleInfoW
- GetSystemDirectoryW
- DeleteFileW
- GetLocalTime
- GetEnvironmentVariableW
- WaitForSingleObject
- WriteFile
- ExitThread
- DeleteCriticalSection
- TlsGetValue
- GetDateFormatW
- SetErrorMode
- IsValidLocale
- TlsSetValue
- CreateDirectoryW
- GetSystemDefaultUILanguage
- EnumCalendarInfoW
- LocalAlloc
- GetUserDefaultLangID
- RemoveDirectoryW
- CreateEventW

- SetThreadLocale
- GetThreadLocale

- comctl32.dll
  - InitCommonControls

- version.dll
  - GetFileVersionInfoSizeW
  - VerQueryValueW
  - GetFileVersionInfoW

- user32.dll
  - CreateWindowExW
  - TranslateMessage
  - CharLowerBuffW
  - CallWindowProcW
  - CharUpperW
  - PeekMessageW
  - GetSystemMetrics
  - SetWindowLongW
  - MessageBoxW
  - DestroyWindow
  - CharUpperBuffW
  - CharNextW
  - MsgWaitForMultipleObjects
  - LoadStringW
  - ExitWindowsEx
  - DispatchMessageW

- oleaut32.dll
  - SysAllocStringLen
  - SafeArrayPtrOfIndex
  - VariantCopy
  - SafeArrayGetLBound
  - SafeArrayGetUBound
  - VariantInit
  - VariantClear
  - SysFreeString
  - SysReAllocStringLen
  - VariantChangeType
  - SafeArrayCreate

netapi32.dll

- NetWkstaGetInfo
- NetApiBufferFree

advapi32.dll

- ConvertStringSecurityDescriptorToSecurityDescriptorW
- RegQueryValueExW
- AdjustTokenPrivileges
- GetTokenInformation
- ConvertSidToStringSidW
- LookupPrivilegeValueW
- RegCloseKey
- OpenProcessToken
- RegOpenKeyExW

PE Exports

- TMethodImplementationIntercept
- __dbk_fcall_wrapper
- dbkFCallWrapperAddr

PE Resources

[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]
[object Object]