xcitium

**CLEAN**
Xcitium Final Verdict

**File Name:** MCA_Selector.exe
**File Type:** PE32+ executable (GUI) x86-64, for MS Windows
**SHA1:** 638622c2558a52cc86eb26e919b3cd9e525d9267
**MD5:** 117f44c56d4f16938662732806030218
**First Seen Date:** 2023-06-27 21:32:37 UTC
**Number of Clients Seen:** 2
**Last Analysis Date:** 2023-06-29 15:58:17 UTC
**Human Expert Analysis Date:** 2023-06-28 08:05:54 UTC
**Human Expert Analysis Result:** Clean
**Verdict Source:** Xcitium Human Expert Analysis Overall Verdict

## Analysis Summary

| ANALYSIS TYPE | DATE | VERDICT |
|---|---|---|
| Signature Based Detection | 2023-06-29 15:58:17 UTC | Clean |
| Static Analysis Overall Verdict | 2023-06-29 15:58:17 UTC | No Threat Found |
| Precise Detectors Overall Verdict | 2023-06-29 15:58:17 UTC | No Match |
| Human Expert Analysis Overall Verdict | 2023-06-28 08:05:54 UTC | Clean |
| File Certificate Validation | | Not Applicable |

## Static Analysis

| STATIC ANALYSIS OVERALL VERDICT | RESULT |
|---|---|
| No Threat Found | |

## Dynamic Analysis

| DYNAMIC ANALYSIS OVERALL VERDICT | RESULT |
|---|---|
| No Threat Found | |

| SUSPICIOUS BEHAVIORS |
|---|
| Has no visible windows |

## Behavioral Information

**QueryFilePath**

C:\Windows\SysWOW64\rundll32.exe

## Precise Detectors Analysis Results

| DETECTOR NAME | DATE | VERDICT | REASON |
|---|---|---|---|
| Static Precise PUA Detector 1 | 2023-06-29 15:58:14 UTC | No Match | NotDetected |
| Static Precise PUA Detector 4 | 2023-06-29 15:58:14 UTC | No Match | NotDetected |
| Static Precise NI Detector 3 | 2023-06-29 15:58:14 UTC | No Match | NotDetected |
| Static Precise PUA Detector 5 | 2023-06-29 15:58:14 UTC | No Match | NotDetected |
| Static Precise Trojan Detector 1 | 2023-06-29 15:58:14 UTC | No Match | NotDetected |
| Static Precise Trojan Detector 3 | 2023-06-29 15:58:14 UTC | No Match | NotDetected |
| Static Precise PUA Detector 6 | 2023-06-29 15:58:14 UTC | No Match | NotDetected |
| Static Precise Trojan Detector 12 | 2023-06-29 15:58:14 UTC | No Match | NotDetected |
| Static Precise Virus Detector 1 | 2023-06-29 15:58:14 UTC | No Match | NotDetected |
| Static Precise Virus Detector 2 | 2023-06-29 15:58:14 UTC | No Match | NotDetected |
| Static Precise Trojan Detector 13 | 2023-06-29 15:58:15 UTC | No Match | NotDetected |
| Static Precise PUA Detector 2 | 2023-06-29 15:58:15 UTC | No Match | NotDetected |

## Advance Heuristics

### No Advanced Heuristic Analysis Result Received

## Human Expert Analysis Results

**Analysis Start Date:** 2023-06-28 06:27:51 UTC
**Analysis End Date:** 2023-06-28 08:05:54 UTC
**File Upload Date:** 2023-06-27 11:49:39 UTC
**Human Expert Analyst Feedback:** None
**Verdict:** Clean

## Additional File Information

**Vendor Validation** - Vendor Validation is not Applicable ?

**Certificate Validation** - Certificate Validation is not Applicable ?

**PE Headers**

| PROPERTY | VALUE |
|---|---|
| Compilation Time Stamp | 0x5169EEA0 [Sat Apr 13 23:47:44 2013 UTC] |
| Debug Artifacts | |
| Entry Point | 0x14000bda0 (.text) |
| Exifinfo | [object Object] |
| File Size | 167424 |
| File Type Enum | 7 |
| Imphash | 8e66a4b75ac568d26dc3f47f4cd0ffd9 |
| Machine Type | AMD64 only, not Itaniums, with 0200 - 64 bit |
| Magic Literal Enum | 4 |
| Legal Copyright | \xa9 2018-2022 Querz |
| File Version | 2.2.2.0 |
| Product Name | MCA Selector |
| Product Version | 2.2.2 |
| File Description | MCA Selector |
| Original Filename | MCA Selector.exe |
| Translation | 0x0409 0x04b0 |
| Mime Type | application/x-dosexec |
| Number Of Sections | 5 |
| Sha256 | cd2a6de8cea016a5f9d6f395751105ae7a6c6e491c8130a06a1b134cefe553c2 |
| Ssdeep | 3072:+czGLGyWl6/uRk2y+aR/pf7IGbPf+FuAEc20jZOKQKiLNmCWbLY1RiMN:+Khap2k9L+/XjZOE |
| Trid | 87.3,Win64 Executable (generic),6.3,Generic Win/DOS Executable,6.3,DOS Executable Generic |

## File Paths

| FILE PATH ON CLIENT | SEEN COUNT |
|---|---|
| MCA_Selector.exe | 1 |

## PE Sections

| NAME | VIRTUAL ADDRESS | VIRTUAL SIZE | RAW SIZE | ENTROPY | MD5 |
|---|---|---|---|---|---|
| .text | 0x1000 | 0x1c50e | 0x1c600 | 6.37108261599 | 098ab83789b8d05e4bbd6abefa3618af |
| .rdata | 0x1e000 | 0x7273 | 0x7400 | 5.5322668395 | a0f213e8c30727b44013c6e208ed3008 |
| .data | 0x26000 | 0x66a0 | 0x2e00 | 4.45346993221 | 3fdcf4cc36267f67dceffea2492282a2 |
| .pdata | 0x2d000 | 0x165c | 0x1800 | 5.05809035379 | 8346bdf871d974d63c7c54d8ce33b036 |
| .rsrc | 0x2f000 | 0x99a | 0xa00 | 3.17548608205 | 52edd953b668b9d31baec00704664a31 |

## PE Imports

- PSAPI.DLL
  - GetModuleFileNameExA
- KERNEL32.dll
  - GetModuleHandleA
  - GetVersionExA
  - SetStdHandle
  - GetStdHandle
  - LoadLibraryW

- FreeLibrary
- GetLastError
- SetEvent
- WaitForSingleObject
- CreateEventA
- Process32Next
- OpenProcess
- Process32First
- CreateToolhelp32Snapshot
- GetCurrentProcessId
- MulDiv
- GlobalFree
- GlobalAlloc
- Sleep
- GlobalUnlock
- GlobalLock
- GlobalMemoryStatus
- GetFileAttributesA
- SetPriorityClass
- GetCurrentProcess
- VirtualAlloc
- VirtualFree
- SetEndOfFile
- GetProcAddress
- HeapReAlloc
- WriteConsoleW
- GetConsoleOutputCP
- WriteConsoleA
- HeapSize
- RtlLookupFunctionEntry
- RtlVirtualUnwind
- GetLocaleInfoA
- GetStringTypeW
- GetStringTypeA
- GetConsoleMode
- GetConsoleCP
- InitializeCriticalSection
- GetSystemTimeAsFileTime

- GetTickCount
- QueryPerformanceCounter
- GetEnvironmentStringsW
- FreeEnvironmentStringsW
- GetEnvironmentStrings
- FreeEnvironmentStringsA
- LCMapStringW
- AllocConsole
- OutputDebugStringA
- WriteFile
- FlushFileBuffers
- GetLocalTime
- MoveFileA
- SetFilePointer
- CreateFileA
- GetFileSize
- ReadFile
- CloseHandle
- SizeofResource
- LoadLibraryA
- SetEnvironmentVariableA
- FindResourceA
- LoadResource
- LockResource
- ExpandEnvironmentStringsA
- lstrlenA
- GetCommandLineA
- CreateThread
- GetModuleFileNameA
- GetCurrentDirectoryA
- SetCurrentDirectoryA
- lstrcatA
- lstrcpyA
- GetFullPathNameA
- FindFirstFileA
- FindNextFileA
- MultiByteToWideChar

- WideCharToMultiByte
- LCMapStringA
- DeleteCriticalSection
- GetFileType
- SetHandleCount
- HeapFree
- HeapAlloc
- GetProcessHeap
- GetStartupInfoA
- HeapSetInformation
- HeapCreate
- ExitProcess
- TerminateProcess
- UnhandledExceptionFilter
- SetUnhandledExceptionFilter
- IsDebuggerPresent
- RtlCaptureContext
- GetCPInfo
- GetACP
- GetOEMCP
- IsValidCodePage
- FlsGetValue
- FlsSetValue
- TlsFree
- FlsFree
- SetLastError
- GetCurrentThreadId
- FlsAlloc
- RtlUnwindEx
- EnterCriticalSection
- LeaveCriticalSection

- USER32.dll
  - SetForegroundWindow
  - DefWindowProcA
  - MessageBoxA
  - PeekMessageA
  - DestroyWindow

- GetSystemMetrics
- ShowWindow
- UpdateWindow
- InvalidateRect
- GetDC
- CopyImage
- BeginPaint
- EndPaint
- EnumWindows
- DdeUninitialize
- GetWindowInfo
- GetWindowThreadProcessId
- DdeConnect
- DdeClientTransaction
- CreateWindowExA
- TranslateMessage
- DispatchMessageA
- GetMessageA
- DdeInitializeA
- DdeCreateStringHandleA
- DdeNameService
- DdeGetData
- LoadCursorA
- RegisterClassExA
- DdeFreeStringHandle

GDI32.dll

- GetObjectA
- GetDeviceCaps
- CreateFontA
- DeleteObject
- SelectObject
- BitBlt
- DeleteDC
- SetBkMode
- SetBkColor
- SetTextColor
- TextOutA

- GetStockObject
- CreateCompatibleDC

ADVAPI32.dll

- RegCloseKey
- RegEnumKeyExA
- StartServiceCtrlDispatcherA
- RegisterServiceCtrlHandlerA
- SetServiceStatus
- OpenServiceA
- DeleteService
- OpenSCManagerA
- CreateServiceA
- CloseServiceHandle
- RegOpenKeyA
- RegEnumValueA
- RegOpenKeyExA
- RegQueryValueExA
- RegDeleteKeyA
- RegCreateKeyExA
- RegSetValueExA

ole32.dll

- CoUninitialize
- CreateStreamOnHGlobal
- CoInitialize

OLEAUT32.dll

- OleLoadPicture

## PE Exports

- DDE_Ready
- INI_GetDictionary
- INI_GetProperty
- Log_LogIt
- SplashScreen_Close
- SplashScreen_GetWindowHandle
- SplashScreen_SetText
- SplashScreen_SetTextBgColor
- SplashScreen_SetTextColor
- SplashScreen_SetTextFont

## PE Resources

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