ID: 606090
Sample Name: download.php
Cookbook: default.jbs
Time: 23:54:27
Date: 08/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

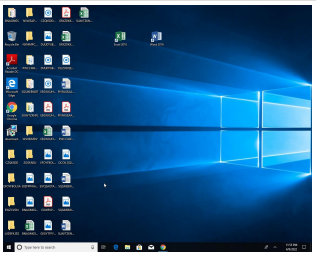
Windows Analysis Report

download.php

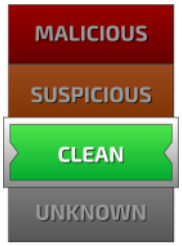
Overview

General Information

Sample Name:	download.php (renamed file extension from php to exe)
Analysis ID:	606090
MD5:	a2c883b0e7a1b0..
SHA1:	0ed075b4c2163c..
SHA256:	27d4749a0db6fff..
Infos:	



Detection

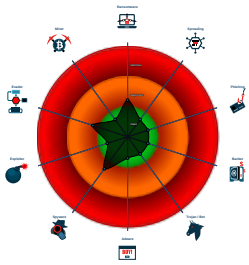


Score:	5
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to query local…
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Detected potential crypto function
- Contains functionality to query CPU…
- Program does not show much activi…

Classification



Process Tree

- **System is w10x64**
- download.exe (PID: 7116 cmdline: "C:\Users\user\Desktop\download.exe" MD5: A2C883B0E7A1B002B088F52F647F2E2F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

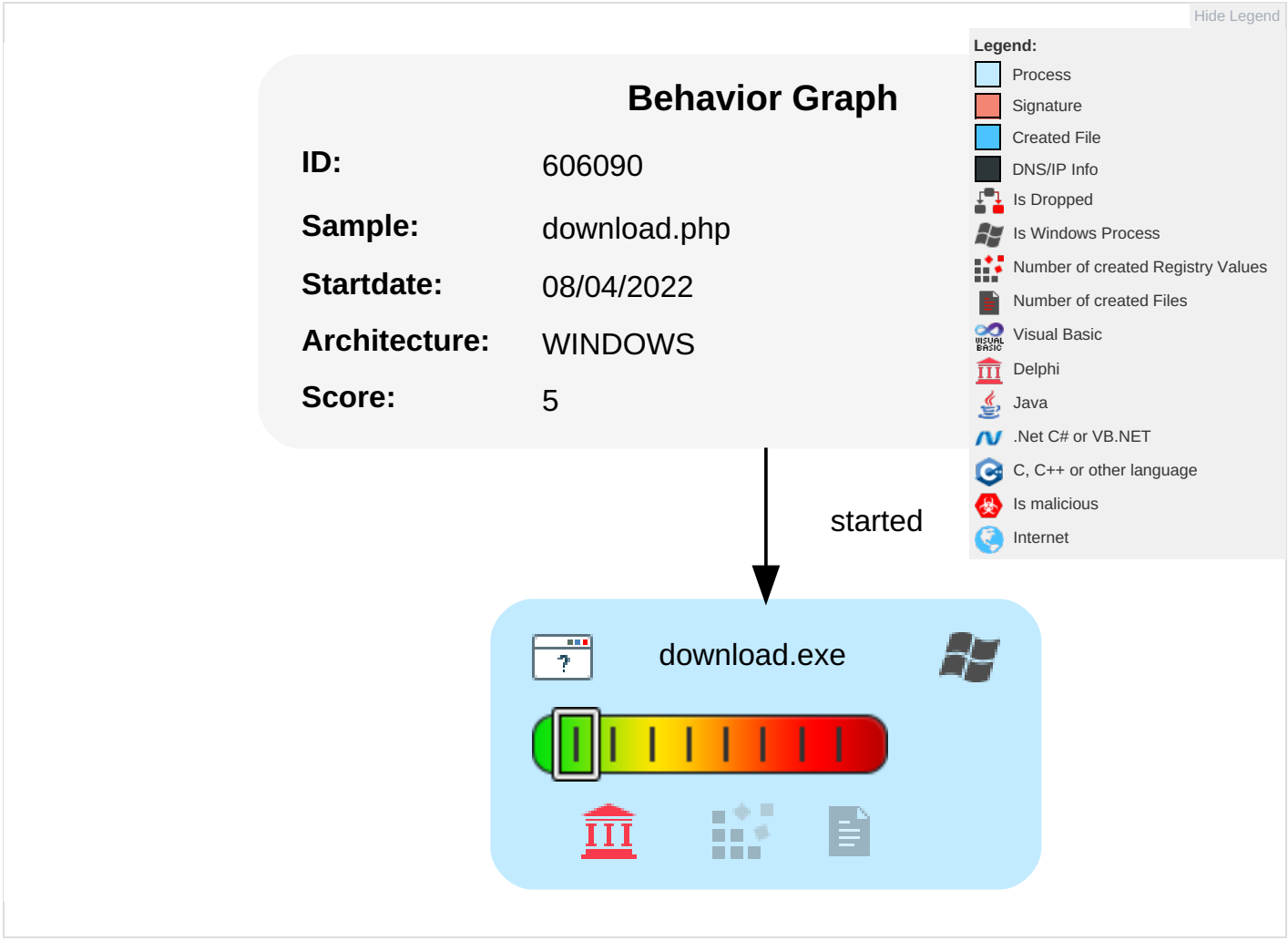
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	2 5 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
download.exe	4%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://jrsoftware.org/ishelp/index.php?topic=setupcmdlineSetupU	download.exe	false		high
http://https://jrsoftware.org/ishelp/index.php?topic=setupcmdline	download.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	606090
Start date and time: 08/04/202223:54:27	2022-04-08 23:54:27 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	download.php (renamed file extension from php to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	2
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean5.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 19.7% (good quality ratio 19.4%) • Quality average: 77.1% • Quality standard deviation: 23.1%
HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.547049237301527
TrID:	• Win32 Executable (generic) a (10002005/4) 98.04% • Inno Setup installer (109748/4) 1.08% • InstallShield setup (43055/19) 0.42% • Win32 EXE PECompact compressed (generic) (41571/9) 0.41% • Win16/32 Executable Delphi generic (2074/23) 0.02%
File name:	download.exe
File size:	1735928
MD5:	a2c883b0e7a1b002b088f52f647f2e2f
SHA1:	0ed075b4c2163cac0463f4f6b7961d0850e1fc05
SHA256:	27d4749a0db6fffdcc3744cb2ed29e8ffa8cc00140ee61faa3a4b0446d512076
SHA512:	4894c7fc90c85a1e1d62a712688e39b3809e090653cf126fc36fe055584320644361267 6ec2c9ab5a6df5cb0d62966624e4633abfe0a3f8a7a2e360f2c748dd1
SSDEEP:	24576:N4nXubIQGyxbPV0db26p2iInkk7vhTCxMLM05Zl3dWzXh35FqF+ahOIZDNJxjNh2:Nqe3f6JIPuxMA05Zl3EFqDEoN3jNhntU
TLSH:	0F85CF3FB268653FD4AE0B3245B39350997BBA61A81A8C2F07F0094DCF665701F3B656
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	a2a0b496b2caca72

Static PE Info

General

Entrypoint:	0x4b5eec
Entrypoint Section:	.itext
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FB0F96E [Sun Nov 15 09:48:30 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	1
File Version Major:	6
File Version Minor:	1
Subsystem Version Major:	6
Subsystem Version Minor:	1
Import Hash:	5a594319a0d69dbc452e748bcf05892e

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFA4h
push ebx
push esi
push edi
xor eax, eax
mov dword ptr [ebp-3Ch], eax
mov dword ptr [ebp-40h], eax
mov dword ptr [ebp-5Ch], eax
mov dword ptr [ebp-30h], eax
mov dword ptr [ebp-38h], eax
mov dword ptr [ebp-34h], eax
mov dword ptr [ebp-2Ch], eax
mov dword ptr [ebp-28h], eax
mov dword ptr [ebp-14h], eax
mov eax, 004B10F0h
call 00007FBEAC94CDD5h
xor eax, eax
push ebp
push 004B65E2h
push dword ptr fs:[eax]
mov dword ptr fs:[eax], esp
xor edx, edx
push ebp
push 004B659Eh
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
mov eax, dword ptr [004BE634h]
call 00007FBEAC9EF4FFh
call 00007FBEAC9EF052h
lea edx, dword ptr [ebp-14h]
xor eax, eax
call 00007FBEAC962848h

Instruction
mov edx, dword ptr [ebp-14h]
mov eax, 004C1D84h
call 00007FBEAC9479C7h
push 00000002h
push 00000000h
push 00000001h
mov ecx, dword ptr [004C1D84h]
mov dl, 01h
mov eax, dword ptr [004237A4h]
call 00007FBEAC9638AFh
mov dword ptr [004C1D88h], eax
xor edx, edx
push ebp
push 004B654Ah
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
call 00007FBEAC9EF587h
mov dword ptr [004C1D90h], eax
mov eax, dword ptr [004C1D90h]
cmp dword ptr [eax+0Ch], 01h
jne 00007FBEAC9F5B6Ah
mov eax, dword ptr [004C1D90h]
mov edx, 00000028h
call 00007FBEAC9641A4h
mov edx, dword ptr [004C1D90h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xc4000	0x9a	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc2000	0xf36	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc7000	0x4800	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xc6000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xc22e4	0x244	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0xc3000	0x1a4	.didata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb361c	0xb3800	False	0.344863934105	data	6.35605820433	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.itext	0xb5000	0x1688	0x1800	False	0.544921875	data	5.97275005522	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xb7000	0x37a4	0x3800	False	0.360979352679	data	5.04440056201	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0xbb000	0x6de8	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.idata	0xc2000	0xf36	0x1000	False	0.3681640625	data	4.89870464796	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.didata	0xc3000	0x1a4	0x200	False	0.345703125	data	2.75636286825	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.edata	0xc4000	0x9a	0x200	False	0.2578125	data	1.87222286659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tls	0xc5000	0x18	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0xc6000	0x5d	0x200	False	0.189453125	data	1.38389437522	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc7000	0x4800	0x4800	False	0.314832899306	data	4.41298427192	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc74c8	0x128	GLS_BINARY_LSB_FIRST	Dutch	Netherlands
RT_ICON	0xc75f0	0x568	GLS_BINARY_LSB_FIRST	Dutch	Netherlands
RT_ICON	0xc7b58	0x2e8	data	Dutch	Netherlands
RT_ICON	0xc7e40	0x8a8	data	Dutch	Netherlands
RT_STRING	0xc86e8	0x360	data		
RT_STRING	0xc8a48	0x260	data		
RT_STRING	0xc8ca8	0x45c	data		
RT_STRING	0xc9104	0x40c	data		
RT_STRING	0xc9510	0x2d4	data		
RT_STRING	0xc97e4	0xb8	data		
RT_STRING	0xc989c	0x9c	data		
RT_STRING	0xc9938	0x374	data		
RT_STRING	0xc9cac	0x398	data		
RT_STRING	0xca044	0x368	data		
RT_STRING	0xca3ac	0x2a4	data		
RT_RCDATA	0xca650	0x10	data		
RT_RCDATA	0xca660	0x2c4	data		
RT_RCDATA	0xca924	0x2c	data		
RT_GROUP_ICON	0xca950	0x3e	data	English	United States
RT_VERSION	0xca990	0x584	data	English	United States
RT_MANIFEST	0xcaf14	0x726	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
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, 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

DLL	Import
advapi32.dll	RegQueryValueExW, AdjustTokenPrivileges, LookupPrivilegeValueW, RegCloseKey, OpenProcessToken, RegOpenKeyExW

Exports

Name	Ordinal	Address
TMethodImplementationIntercept	3	0x454060
__dbk_fcall_wrapper	2	0x40d0a0
dbkFCallWrapperAddr	1	0x4be63c

Version Infos

Description	Data
LegalCopyright	
FileVersion	
CompanyName	
Comments	This installation was built with Inno Setup.
ProductName	Inno Script Studio
ProductVersion	1.0
FileDescription	Inno Script Studio Setup
OriginalFileName	
Translation	0x0000 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
Dutch	Netherlands	
English	United States	

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: download.exe PID: 7116, Parent PID: 6100

General

Target ID:	1
Start time:	23:55:24
Start date:	08/04/2022
Path:	C:\Users\user\Desktop\download.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\download.exe"

Imagebase:	0x400000
File size:	1735928 bytes
MD5 hash:	A2C883B0E7A1B002B088F52F647F2E2F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly