

ID: 339372
Sample Name: RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe
Cookbook: default.jbs
Time: 21:50:26
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 4
Signature Overview 5
AV Detection: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted IPs 8
General Information 8
Simulations 8
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
File Icon 10
Static PE Info 10
General 10
Entrypoint Preview 10
Data Directories 11
Sections 11
Resources 12
Imports 12
Version Infos 12
Possible Origin 12
Network Behavior 12
Code Manipulations 12
Statistics 12
System Behavior 12
Analysis Process: RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe PID: 6180 Parent

PID: 5852 13
General 13
File Activities 13
Disassembly 13
Code Analysis 13

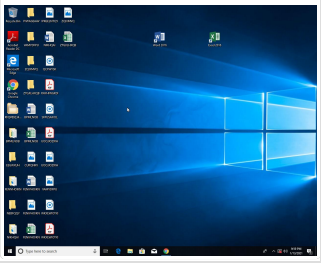
Analysis Report RFQ#89234A_2021_LISTED_ITEMS_DU…

Overview

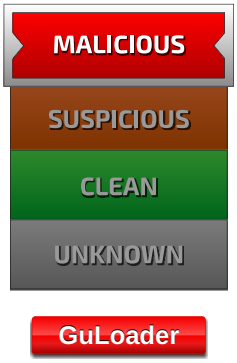
General Information

Sample Name:	RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe
Analysis ID:	339372
MD5:	754d599f8cdeb37.
SHA1:	5e48dfb313f300b..
SHA256:	7c328b51dbd9e7..
Tags:	exe GuLoader

Most interesting Screenshot:



Detection

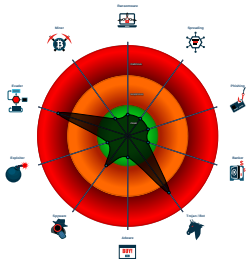


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Found potential dummy code loops (…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to query CPU …
- Contains functionality to read the PEB
- PE file contains strange resources
- Program does not show much activi…
- Sample file is different than original …

Classification



Startup

- **System is w10x64**
- RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe (PID: 6180 cmdline: 'C:\Users\user\Desktop\RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe' MD5: 754D599F8CDEB37D1F3F61764669D799)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

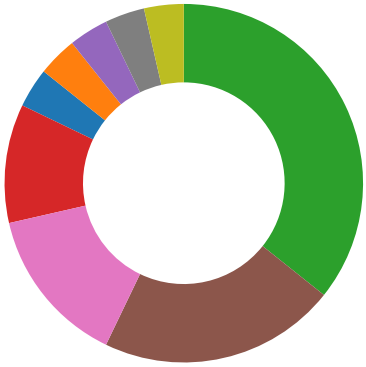
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe PID: 6180	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe PID: 6180	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

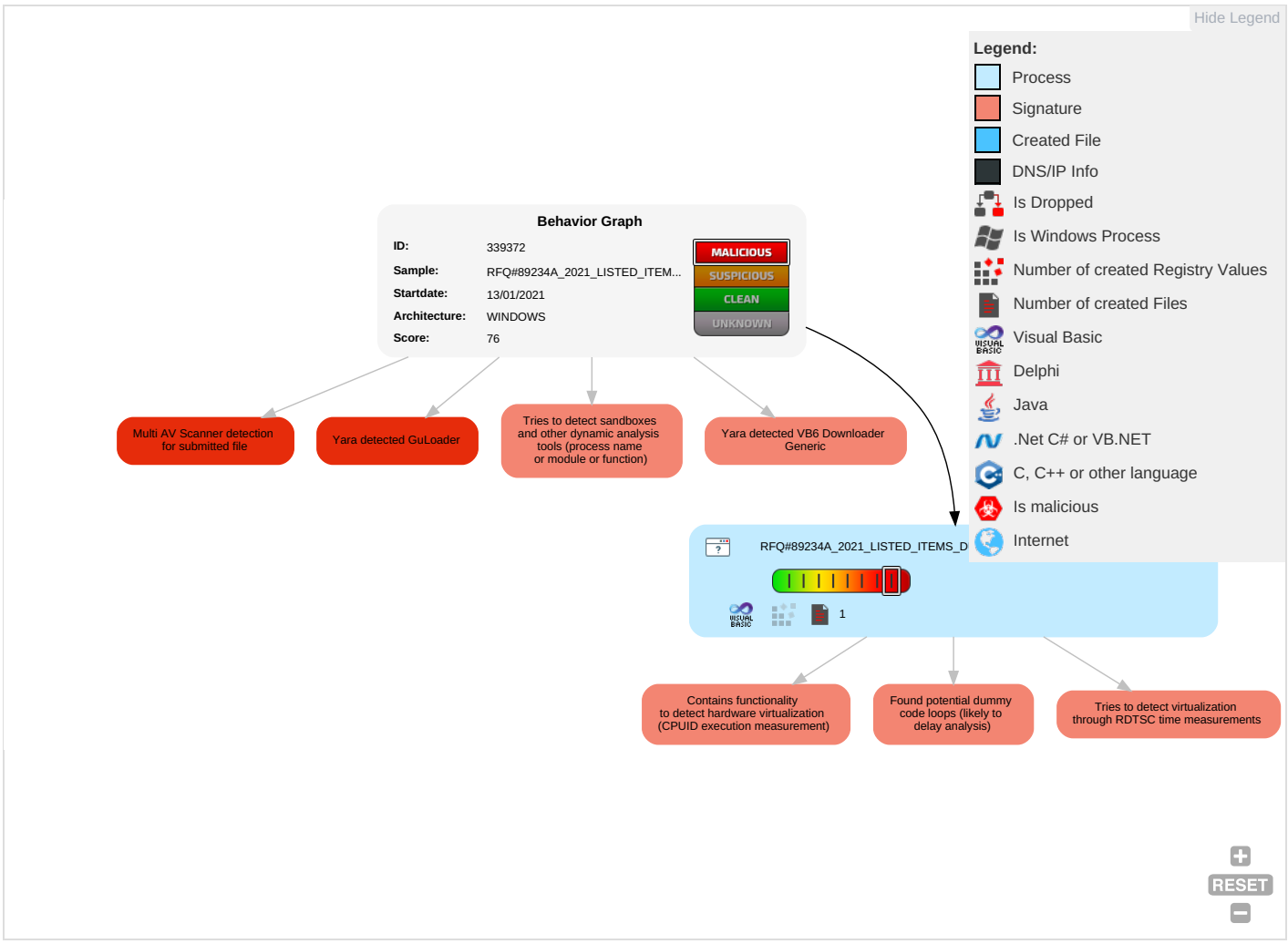
Anti Debugging:

Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 4 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

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
RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe	20%	ReversingLabs	Win32.Infostealer.PonyStealer	

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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339372
Start date:	13.01.2021
Start time:	21:50:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.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:	31
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:	MAL
Classification:	mal76.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.9% (good quality ratio 5.3%) • Quality average: 22.5% • Quality standard deviation: 31.1%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • VT rate limit hit for: /opt/package/joesandbox/database/analysis/339372/sample/RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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):	5.86757283144284
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe
File size:	81920
MD5:	754d599f8cdeb37d1f3f61764669d799
SHA1:	5e48dfb313f300b4d460e73bd25b324b88da0df7
SHA256:	7c328b51dbd9e7fb96ca2ed21358fd5112c809f9666f9287b55927302c7ac1ea
SHA512:	f1c579777f16b1536e51dcc8d6141cb59517b61129072a3bd856abecc12efbee15cd224bc8575488023f6b0c731bb283b64c9353c475b48bda3e6b8c6c20e80d
SSDEEP:	768:ETpAbB+koysOiKEQWvc+ddsx/RRr4mtXbt2+:ETpTTyLizJtdOZbDX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....._.....0..... ....@.....

File Icon



Icon Hash:	6eeed0e4a4a4e0d2

Static PE Info

General

Entrypoint:	0x40121c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5FFEBE91 [Wed Jan 13 09:34:09 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f08e2fa188bfdb85d74117a6c20b7544

Entrypoint Preview

Instruction
push 00401D04h
call 00007F9D08A10015h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [esi-7D9F66D1h], ah
pop eax
cmp dword ptr [esi-60h], ecx
into
push edx
cmp esi, dword ptr [ebp+00004EE7h]
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
outsb
imul esp, dword ptr fs:[edi+74h], 676E696Eh
outsb
jnc 00007F9D08A10022h
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
and edx, ebp

Instruction
add ebx, edx
test dword ptr [ebp-51BDDE5Ah], 4F991E50h
xchg eax, edi
test eax, 216A68AEh
outsd
enter 46DCh, BFh
mov ch, F3h
fsubrp st(2), st(0)
test dword ptr [eax], ebp
adc eax, 33AD4F3Ah
cdq
iretw
adc dword ptr [edi+00AA000Ch], esi
pushad
rcl dword ptr [ebx+00000000h], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor al, 0Ah
add byte ptr [eax], al
rol dword ptr [08000000h], cl
add byte ptr [ebx+75h], dl
bound esp, dword ptr [ebp+64h]
imul esi, dword ptr [edi+esi+00h], 0009010Dh
jnc 00007F9D08A10098h
popad
jc 00007F9D08A10092h
outsd

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x11424	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x884	.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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xcc	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Copyright null 2021

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x10838	0x11000	False	0.389059627757	data	6.32612919627	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x12000	0x1160	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0x884	0x1000	False	0.329345703125	data	3.01799002813	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1431c	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x14308	0x14	data		
RT_VERSION	0x140f0	0x218	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, _adj_fpatan, EVENT_SINK_Release, __vbaUI1I2, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarAdd, __vbaVarLateMemCallLd, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	GISELLE
FileVersion	1.00
CompanyName	Web Share.
ProductName	Decalogues2
ProductVersion	1.00
OriginalFilename	GISELLE.exe

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe PID: 6180 Parent PID: 5852

General

Start time:	21:51:23
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUCS_IMPORT_EXPORT_CO.exe'
Imagebase:	0x400000
File size:	81920 bytes
MD5 hash:	754D599F8CDEB37D1F3F61764669D799
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis