ID: 339335
Sample Name: RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUC_IMPORT_EXPORT_CO.exe
Cookbook: default.jbs
Time: 21:13:13
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

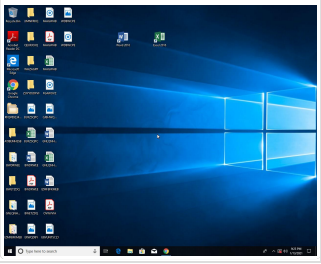
Analysis Report RFQ#89234A_2021_LISTED_ITEMS_DU…

Overview

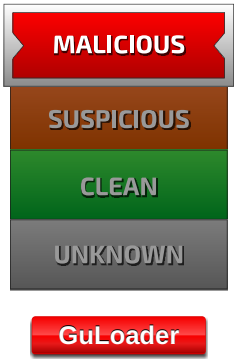
General Information

Sample Name:	RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUC_IMPORT_EXPORT_CO.exe
Analysis ID:	339335
MD5:	5a07a1d293ec00..
SHA1:	e1712e01b0945a..
SHA256:	c65e2de75fb3417.
Tags:	exe GuLoader

Most interesting Screenshot:



Detection

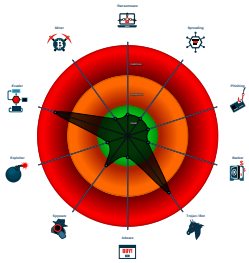


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- 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…

Classification



Startup

- **System is w10x64**
- RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUC_IMPORT_EXPORT_CO.exe (PID: 1664 cmdline: 'C:\Users\user\Desktop\RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUC_IMPORT_EXPORT_CO.exe' MD5: 5A07A1D293EC00EF9F52F9C515C95F57)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

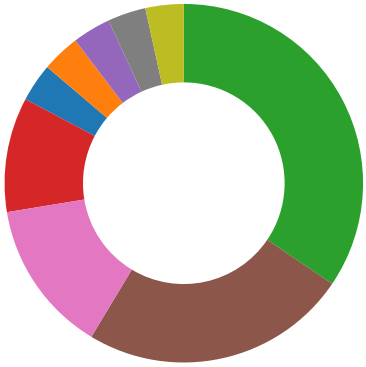
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUC_IMPORT_EXPORT_CO.exe PID: 1664	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUC_IMPORT_EXPORT_CO.exe PID: 1664	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)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

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

Tries to detect virtualization through RDTSC time measurements

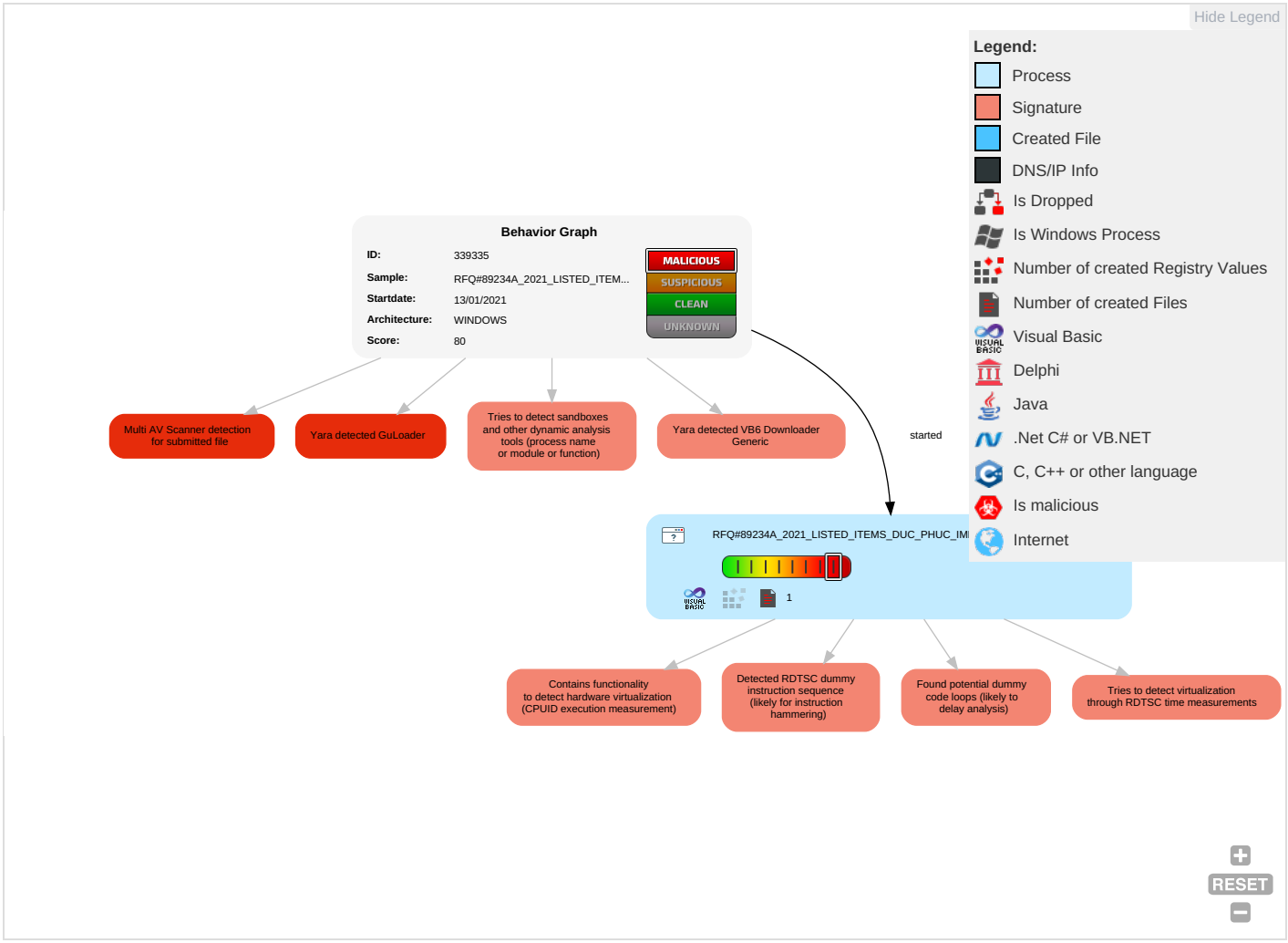
Anti Debugging:

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 5 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 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

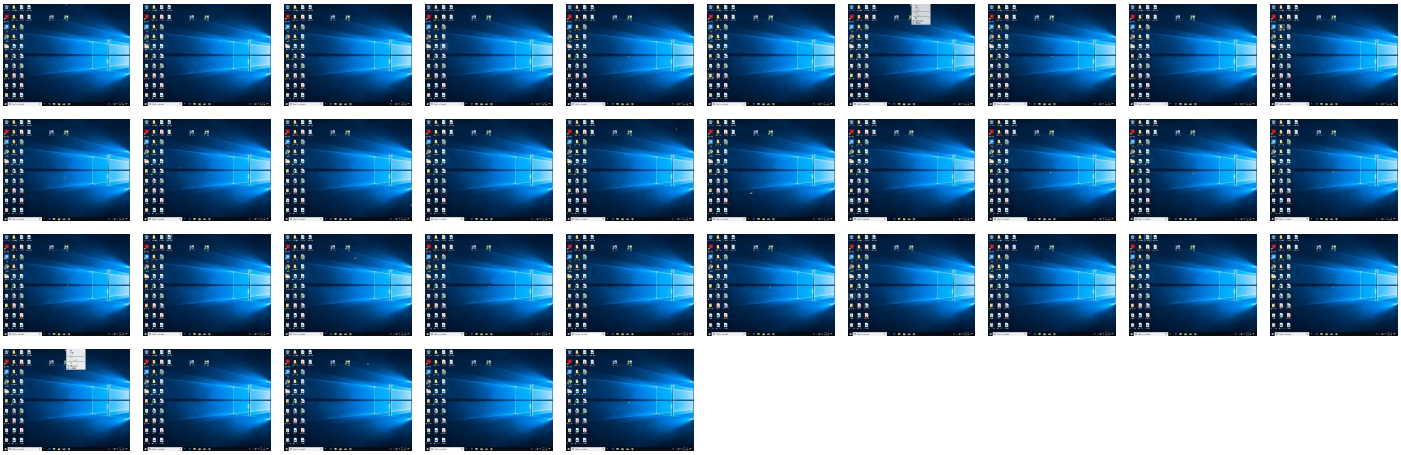
Behavior Graph



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_PHUC_IMPORT_EXPORT_CO.exe	21%	Virustotal		Browse
RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUC_IMPORT_EXPORT_CO.exe	17%	ReversingLabs	Win32.Infostealer.Generic	

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:	339335
Start date:	13.01.2021
Start time:	21:13:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUC_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:	6
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:	mal80.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
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): MusNotifyIcon.exe, svchost.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):	5.818862716387618
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_PHUC_IMPORT_EXPORT_CO.exe
File size:	81920
MD5:	5a07a1d293ec00ef9f52f9c515c95f57
SHA1:	e1712e01b0945a42e7d9b1c9dd2eca5b98c4174d
SHA256:	c65e2de75fb34171072925ff6d7c2a9fa79e5d311c4296dacf7a12d524b4167d
SHA512:	14891cec98c4e6d8b8253847073d004e4faa3c5bbfe19359f3e1dd068fdff2337e9d48ad15ecda29e33ed3933208352abfcef98cd5f687cbc16408a363b3017d
SSDEEP:	768:SLdB0W0HHvevgg/qb8d8XLrQF41dg74zIYBbVzM58/UFBcwF:GyNPWv/qb7XX+pw5zkt
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:	0x5FFE9EC4 [Wed Jan 13 07:18:28 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 00401D44h
call 00007FBB28CDED65h
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 [edi], bh
insb
push eax
push ds
lds ebp, fword ptr [eax+76h]
dec esi
sahf
xor eax, 8358DC01h
call far fword ptr [edi+00000000h]
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
jc 00007FBB28CDEDD7h
jo 00007FBB28CDEDE4h
outsd
outsd
insb
jnc 00007FBB28CDEDE6h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
and ecx, dword ptr [edi]
xchg byte ptr [edi-2Eh], bh

Instruction
xchg eax, edi
int1
insb
inc esi
mov si, es
sub esp, dword ptr [ebx-5Dh]
aam 93h
loope 00007FBB28CDED72h
xor byte ptr [esi-0Ch], bl
call 00007FBABA163C58h
add eax, ebp
cmp byte ptr [4F3A2421h+edx*2], dh
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
jnbe 00007FBB28CDED7Ch
add byte ptr [eax], al
in eax, 05h
add byte ptr [eax], al
add byte ptr [eax], bl
add byte ptr [ebx+61h], dl
insd
popad
jc 00007FBB28CDEDD4h
push 00000064h
jnc 00007FBB28CDEDDFh
jne 00007FBB28CDEDDEh
imul esp, dword ptr [edi+68h], 72656465h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x11124	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x89c	.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	

Name	Virtual Address	Virtual Size	Is in Section
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x10538	0x11000	False	0.384794347426	data	6.27283103178	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	0x89c	0x1000	False	0.331787109375	data	3.04129214275	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x14334	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x14320	0x14	data		
RT_VERSION	0x140f0	0x230	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	KROKODILLERNES
FileVersion	1.00
CompanyName	Web Share.
ProductName	Phyllos
ProductVersion	1.00
OriginalFilename	KROKODILLERNES.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_PHUC_IMPORT_EXPORT_CO.exe PID: 1664
Parent PID: 5944

General

Start time:	21:14:09
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUC_IMPORT_EXPORT_CO.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ#89234A_2021_LISTED_ITEMS_DUC_PHUC_IMPORT_EXPORT_CO.exe'
Imagebase:	0x400000
File size:	81920 bytes
MD5 hash:	5A07A1D293EC00EF9F52F9C515C95F57
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