ID: 343196
Sample Name: Proforma Invoice.exe
Cookbook: default.jbs
Time: 14:49:45
Date: 22/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Proforma Invoice.exe 4
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 4
AV Detection: 5
Compliance: 5
System Summary: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 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 8
Domains and IPs 8
Contacted Domains 8
Contacted IPs 8
General Information 8
Simulations 9
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 12
Resources 12
Imports 12
Version Infos 12
Possible Origin 12
Network Behavior 12
Code Manipulations 13
Statistics 13

System Behavior 13
Analysis Process: Proforma Invoice.exe PID: 2952 Parent PID: 5692 13
General 13
File Activities 13
Disassembly 13
Code Analysis 13

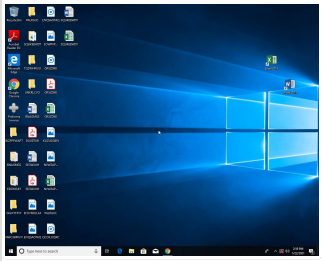
Analysis Report Proforma Invoice.exe

Overview

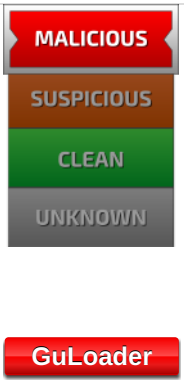
General Information

Sample Name:	Proforma Invoice.exe
Analysis ID:	343196
MD5:	6479f35608769db…
SHA1:	1ffc79fde43e746…
SHA256:	e97a63a8f54270a…
Tags:	GuLoader

Most interesting Screenshot:



Detection

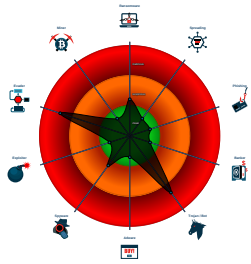


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Executable has a suspicious name (…
- Initial sample is a PE file and has a …
- 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 call native f…
- Contains functionality to query CPU …

Classification



Startup

- **System is w10x64**
- Proforma Invoice.exe (PID: 2952 cmdline: 'C:\Users\user\Desktop\Proforma Invoice.exe' MD5: 6479F35608769DB340640D6A8F84A38D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

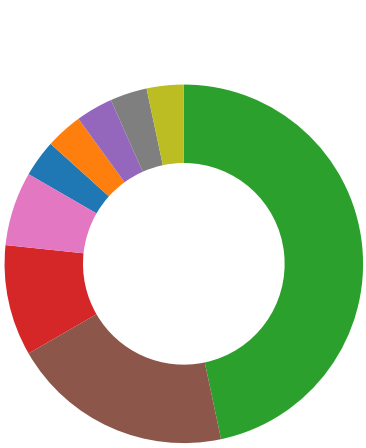
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Proforma Invoice.exe PID: 2952	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: Proforma Invoice.exe PID: 2952	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

System Summary:

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

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)

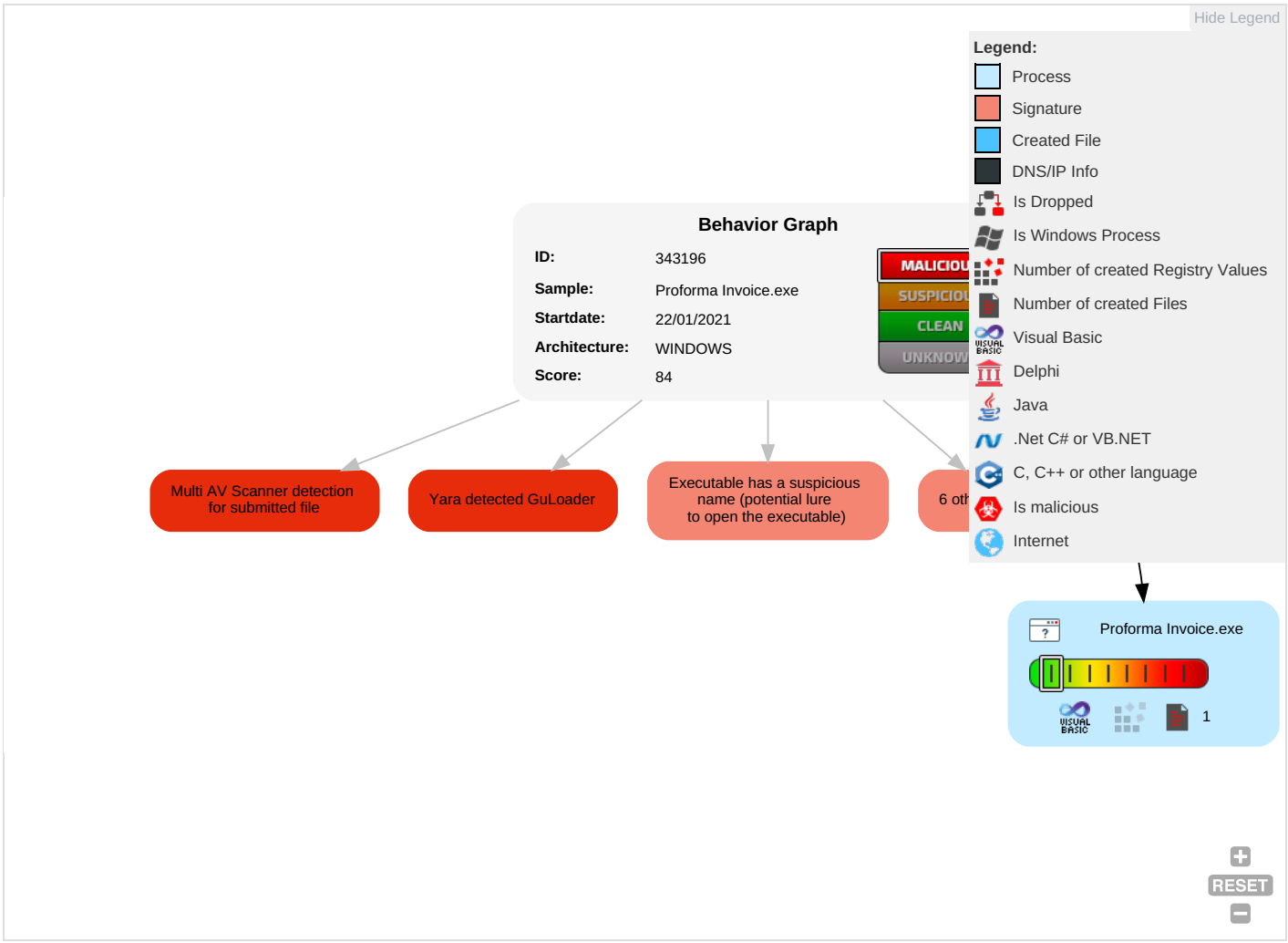
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

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
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Process Injection 1	OS Credential Dumping	Security Software Discovery 4 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 3 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

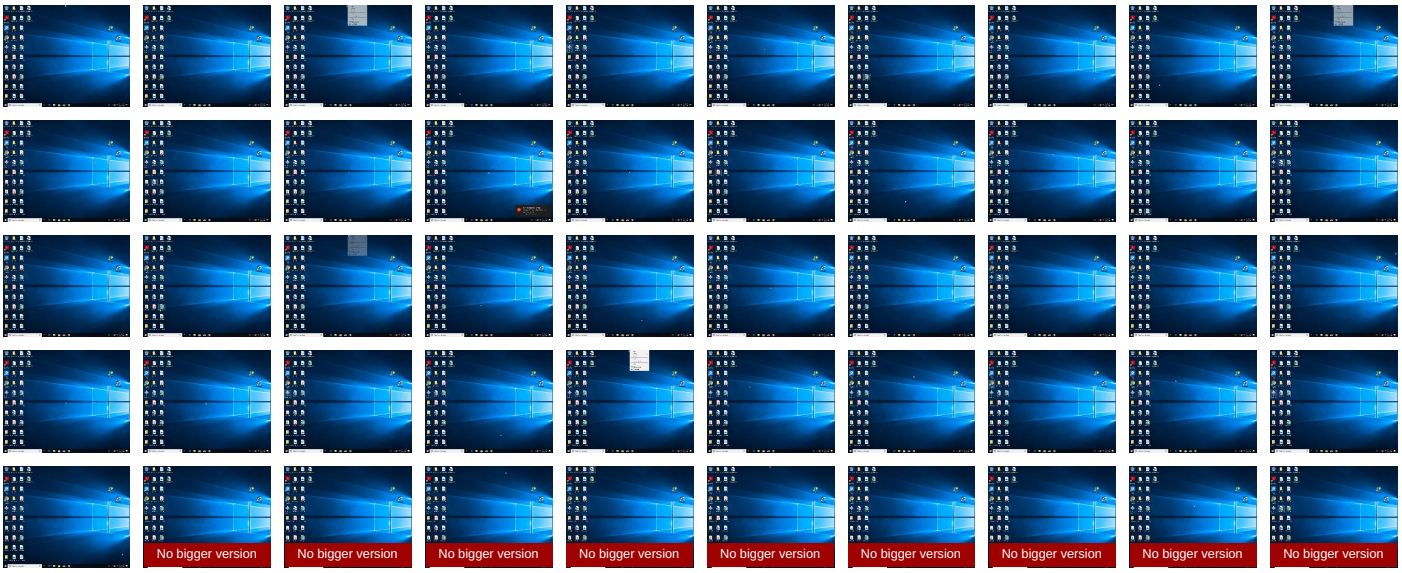
Behavior Graph

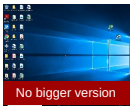


Screenshots

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
Proforma Invoice.exe	34%	Virustotal		Browse
Proforma Invoice.exe	20%	ReversingLabs	Win32.Trojan.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:	343196
Start date:	22.01.2021
Start time:	14:49:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Proforma Invoice.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:	39
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:	mal84.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.7% (good quality ratio 10%) • Quality average: 39.1% • Quality standard deviation: 36.7%
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, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.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):	5.766612306860119
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:	Proforma Invoice.exe
File size:	69632
MD5:	6479f35608769db340640d6a8f84a38d
SHA1:	1ffc79fde43e746e826f32a018e02a65fc51602e
SHA256:	e97a63a8f54270ace4969870597c7642bbdb31fc6d5d197 2d412edaf4fccd80e
SHA512:	cab95cae43799faaec6d612e4f63d363629506dd5973513 e29870e0d81e1a3a99adc86696d320ffaeeff5cc23b6f649 1cbe30052a3eff9afd303227db113054f
SSDEEP:	768:IxdbBehQZF4bp4kbKR80KQWfD5HDm0L5g5eucI1 hzRU66t:6dde0F4bekepUrZi0O5FcI1hzR+

General

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.....S.....0.....T.....@.....

File Icon

Icon Hash:	f030f0c6f030b100

Static PE Info

General

Entrypoint:	0x401354
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:	0x530B1A94 [Mon Feb 24 10:10:28 2014 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:	e22238527efb5691a1dfa3f0e707406a

Entrypoint Preview

Instruction
push 00401FECh
call 00007FD3307D24E5h
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 dh, cl
in al, dx
add edx, dword ptr [ebx+42150DA1h]
cmpsd
xchg eax, ecx
aas
test eax, CAE2F407h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
inc ecx
add byte ptr [esi+50018250h], al
jc 00007FD3307D2561h
push 00000065h
arpl word ptr [ecx+esi+00h], si
add byte ptr [eax], al

Instruction
add byte ptr [ecx+edi-01h], bl
add al, byte ptr [eax]
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
add al, 93h
sub eax, 444FEB34h
or dword ptr [edi-6Fh], ecx
add dword ptr [ebx-03792E85h], esp
adc dword ptr [ecx], ebp
sti
mov edx, BC44A82Ah
inc ecx
adc al, 0000002Fh
lahf
aad 16h
aad CCh
cmp cl, byte ptr [edi-53h]
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
add byte ptr [eax], al
in al, 0Bh
add byte ptr [eax], al
dec eax
or eax, dword ptr [eax]
add byte ptr [eax], al
or dword ptr [eax], eax
insb
popad
jnc 00007FD3307D2566h
imul esi, dword ptr [ebx+6Bh], 010D0065h
sldt word ptr [esi+69h]
jc 00007FD3307D2557h
je 00007FD3307D24F3h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe9f4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x11000	0x930	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xfc	.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	0xde48	0xe000	False	0.533761160714	data	6.42243762415	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xf000	0x1180	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x11000	0x930	0x1000	False	0.140625	data	1.4231462793	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x113c8	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x113b4	0x14	data		
RT_VERSION	0x110f0	0x2c4	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaLenBstr, __vbaEnd, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaVarForInit, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaVarTstLt, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaI4Var, __vbaVarDup, __vbaFpI4, _CIatan, __vbaCastObj, __vbaStrMove, _allmul, _CItan, __vbaVarForNext, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0404 0x04b0
LegalCopyright	Calc Theory
InternalName	ABJOINT
FileVersion	1.00
CompanyName	Calc Theory
Comments	Calc Theory
ProductName	Calc Theory
ProductVersion	1.00
FileDescription	Calc Theory
OriginalFilename	ABJOINT.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Proforma Invoice.exe PID: 2952 Parent PID: 5692

General

Start time:	14:50:35
Start date:	22/01/2021
Path:	C:\Users\user\Desktop\Proforma Invoice.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Proforma Invoice.exe'
Imagebase:	0x400000
File size:	69632 bytes
MD5 hash:	6479F35608769DB340640D6A8F84A38D
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

Disassembly

Code Analysis