ID: 358414
Sample Name: FACTURA Y ALBARANES.exe
Cookbook: default.jbs
Time: 15:36:09
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report FACTURA Y ALBARANES.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
Compliance: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
HIPS / PFW / Operating System Protection 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 7
Domains and IPs 7
Contacted Domains 8
Contacted IPs 8
General Information 8
Simulations 8
Behavior and APIs 8
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 9
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

Behavior 12
System Behavior 13
Analysis Process: FACTURA Y ALBARANES.exe PID: 7104 Parent PID: 5936 13
General 13
File Activities 13
Analysis Process: RegAsm.exe PID: 7052 Parent PID: 7104 13
General 13
File Activities 14
Analysis Process: conhost.exe PID: 1324 Parent PID: 7052 14
General 14
Disassembly 14
Code Analysis 14

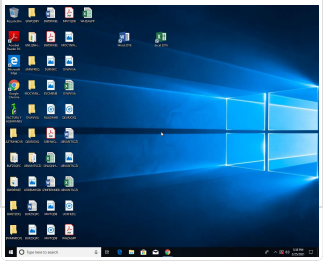
Analysis Report FACTURA Y ALBARANES.exe

Overview

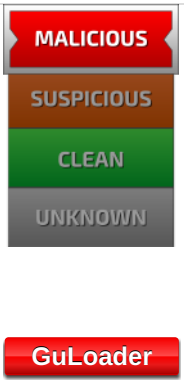
General Information

Sample Name:	FACTURA Y ALBARANES.exe
Analysis ID:	358414
MD5:	0495f304201fbe5..
SHA1:	14dd46d175d5b0..
SHA256:	31970d5ad477b5..
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection

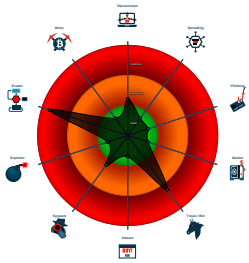


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Writes to foreign memory regions
- Abnormal high CPU Usage
- Checks if the current process is bein…
- Contains functionality for execution …

Classification



Startup

- **System is w10x64**
- FACTURA Y ALBARANES.exe (PID: 7104 cmdline: 'C:\Users\user\Desktop\FACTURA Y ALBARANES.exe' MD5: 0495F304201FBE589C3826BB8E8AB5CD)
  - RegAsm.exe (PID: 7052 cmdline: 'C:\Users\user\Desktop\FACTURA Y ALBARANES.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 1324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

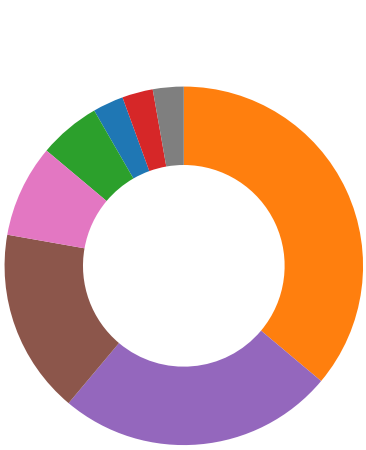
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: RegAsm.exe PID: 7052	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Compliance:

Uses 32bit PE files

Data Obfuscation:

Yara detected GuLoader

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 Any.run

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)

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

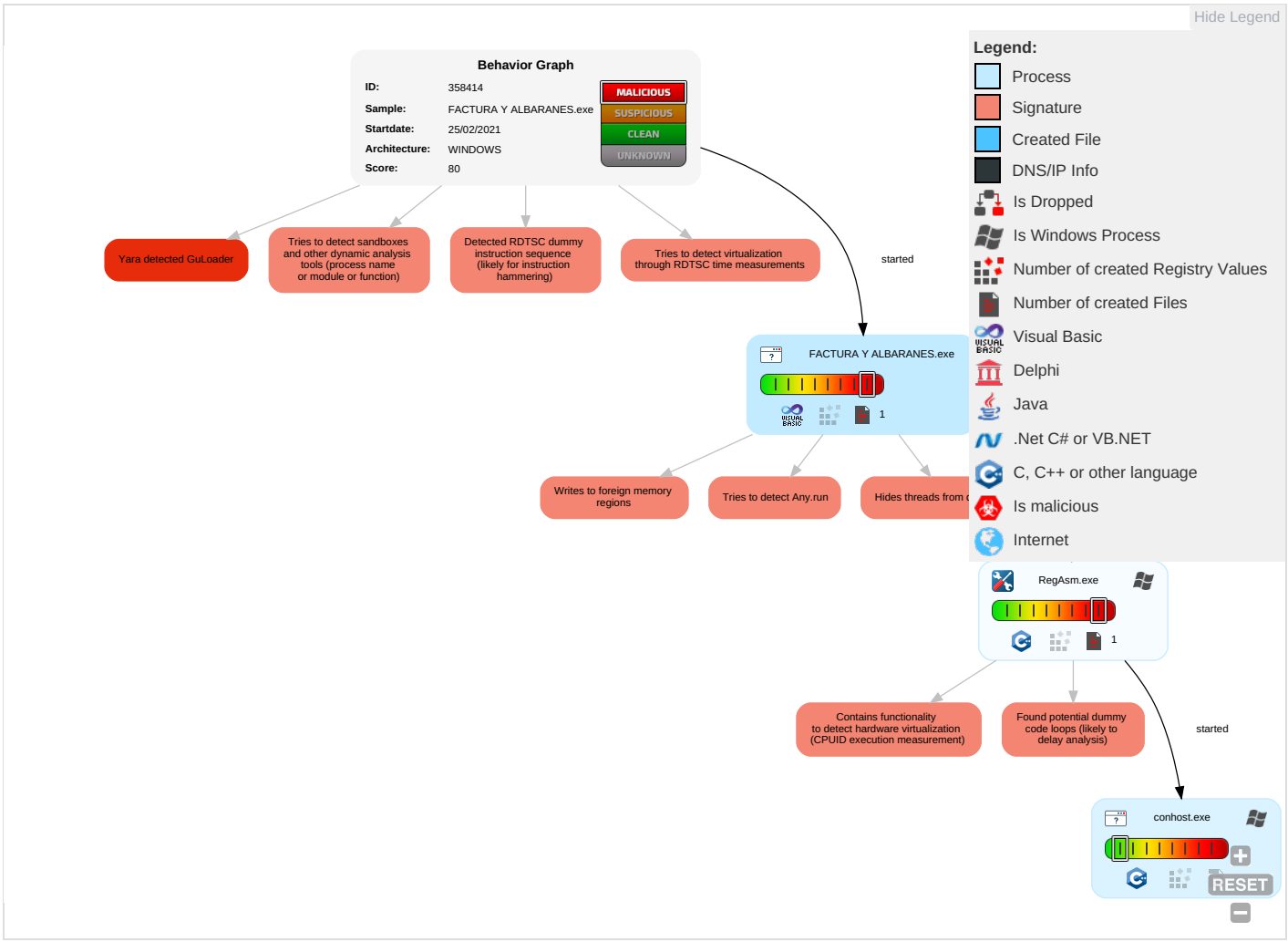
Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 3 1 1	OS Credential Dumping	Security Software Discovery 7 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Information Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

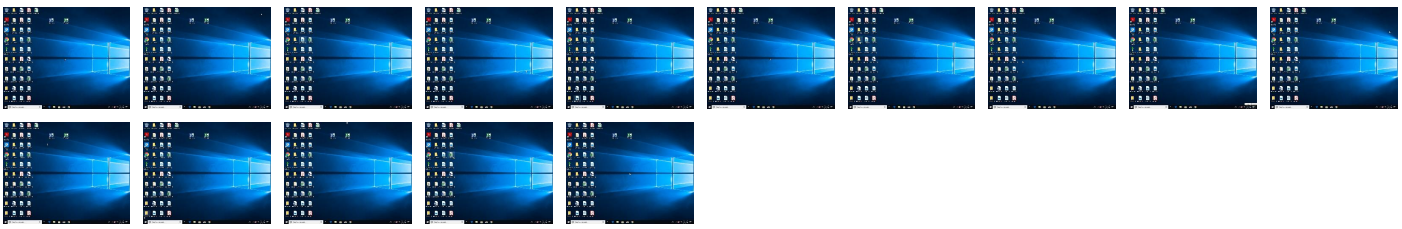
Behavior Graph



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

No Antivirus matches

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 Emerald
Analysis ID:	358414
Start date:	25.02.2021
Start time:	15:36:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FACTURA Y ALBARANES.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:	17
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@4/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 56.1% (good quality ratio 31.8%) • Quality average: 39.5% • Quality standard deviation: 38.9%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • VT rate limit hit for: /opt/package/joesandbox/database/analysis/358414/sample/FACTURA Y ALBARANES.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):	5.360541353236755
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:	FACTURA Y ALBARANES.exe
File size:	73728
MD5:	0495f304201fbe589c3826bb8e8ab5cd
SHA1:	14dd46d175d5b04c105794c4b41cc5a6fb1fca3f
SHA256:	31970d5ad477b508e0b677485fa10a588b0ece66dbf8eadee7973977ead6c07
SHA512:	a2aa4a4f9adc6e7a19fca998313d680f6342069e46f364ac34a8505a4d1ab8e2986f7fadd0361c1cbfcc42781f724b847269aead5d6a3c867d81bb1aac43b2d1
SSDEEP:	1536:nmKXDSk33jANL/9pJpMplDB1Mc1pu9oGzceKMP3gX:mKzSkHENLzJlZ51A9rzbKSg
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L.....KL.....0.....@.....

File Icon

Icon Hash:	b038b57269717938

Static PE Info

General

Entrypoint:	0x401394
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:	0x4C4BD818 [Sun Jul 25 06:22:16 2010 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:	f783b7553c2ee07b6bd756ebd3705f2c

Entrypoint Preview

Instruction
push 0040A3D0h
call 00007FE598943DC5h
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 [eax], cl
jns 00007FE598943DDEh
xchg eax, esp
jmp 00007FE554E2594Eh
out dx, eax
xchg dword ptr [edx], esi
mov ebp, 006646DBh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], bh
pop dword ptr [616E4103h]
je 00007FE598943E41h
insd
jnc 00007FE598943E04h
add byte ptr [eax], cl
inc ecx
add byte ptr [eax], ah
or byte ptr [ecx+00h], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
or dh, byte ptr [ebx+edx*2-7FE85B3Dh]
xlatb
inc ebx
mov word ptr [eax+ebp*4-29h], seg?
salc

Instruction
je 00007FE598943DF3h
in eax, dx
fidivr dword ptr [edi]
popad
ret
sbb dword ptr [ebp+6D46834Ah], ebx
dec edx
sub dword ptr [eax], 4F3A6B98h
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
cmp dword ptr [edi+0C110000h], ecx
add byte ptr [eax], al
add byte ptr [eax+eax], cl
arpl word ptr [edx+6Fh], si
jnc 00007FE598943E45h
arpl word ptr [ebp+74h], si
je 00007FE598943E3Bh
outsb
add byte ptr [di], cl
add dword ptr [edx], ecx
add byte ptr [edx+65h], ah

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xeb64	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x12000	0xf4e	.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	0x11c	.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	0xe058	0xf000	False	0.374251302083	data	5.83564120416	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x10000	0x1210	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x12000	0xf4e	0x1000	False	0.323486328125	data	3.63151348767	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x12c66	0x2e8	data		
RT_ICON	0x123be	0x8a8	data		
RT_GROUP_ICON	0x1239c	0x22	data		
RT_VERSION	0x12120	0x27c	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaHresultCheck, __vbaFreeVar, __vbaStrVarMove, __vbaLenBstr, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaSetSystemError, __vbaLenBstrB, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaErrorOverflow, __vbaNew2, __vbaR8Str, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaStrToAnsi, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	Xanthophane
FileVersion	1.00
CompanyName	Wang
ProductName	Wang Laboratories
ProductVersion	1.00
FileDescription	Wang Laboratories
OriginalFilename	Xanthophane.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

Behavior

FACTURA Y ALBARANES.exe
RegAsm.exe
conhost.exe

Click to jump to process

System Behavior

Analysis Process: FACTURA Y ALBARANES.exe PID: 7104 Parent PID: 5936

General

Start time:	15:36:56
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\FACTURA Y ALBARANES.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\FACTURA Y ALBARANES.exe'
Imagebase:	0x400000
File size:	73728 bytes
MD5 hash:	0495F304201FBE589C3826BB8E8AB5CD
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

Analysis Process: RegAsm.exe PID: 7052 Parent PID: 7104

General

Start time:	15:38:21
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\FACTURA Y ALBARANES.exe'
Imagebase:	0x670000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1324 Parent PID: 7052

General

Start time:	15:38:22
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis