ID: 385484
Sample Name: Evolution des moyens de trasport.exe
Cookbook: default.jbs
Time: 15:25:46
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

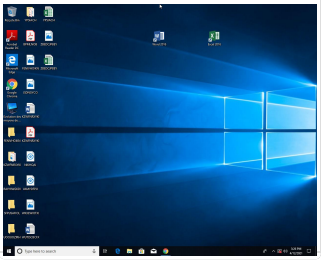
Analysis Report Evolution des moyens de trasport.exe

Overview

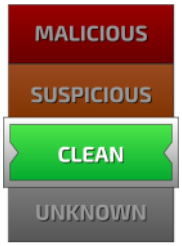
General Information

Sample Name:	Evolution des moyens de trasport.exe
Analysis ID:	385484
MD5:	e31302978d2b06..
SHA1:	2677beebffc4358..
SHA256:	f238e71f708ab19..
Infos:	

Most interesting Screenshot:



Detection

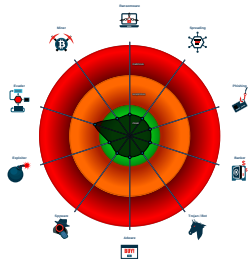


Score:	4
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Antivirus or Machine Learning detec…
- PE file contains an invalid checksum
- PE file contains strange resources
- Program does not show much activi…
- Sample file is different than original …
- Tries to load missing DLLs
- Uses 32bit PE files
- Uses code obfuscation techniques (…

Classification



Startup

- **System is w10x64**
- Evolution des moyens de trasport.exe (PID: 1256 cmdline: 'C:\Users\user\Desktop\Evolution des moyens de trasport.exe' MD5: E31302978D2B065F030279B481E32344)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

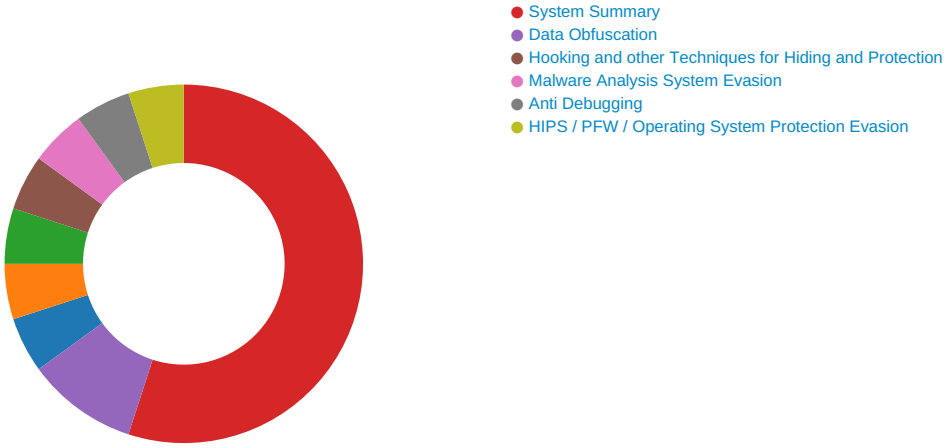
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Networking



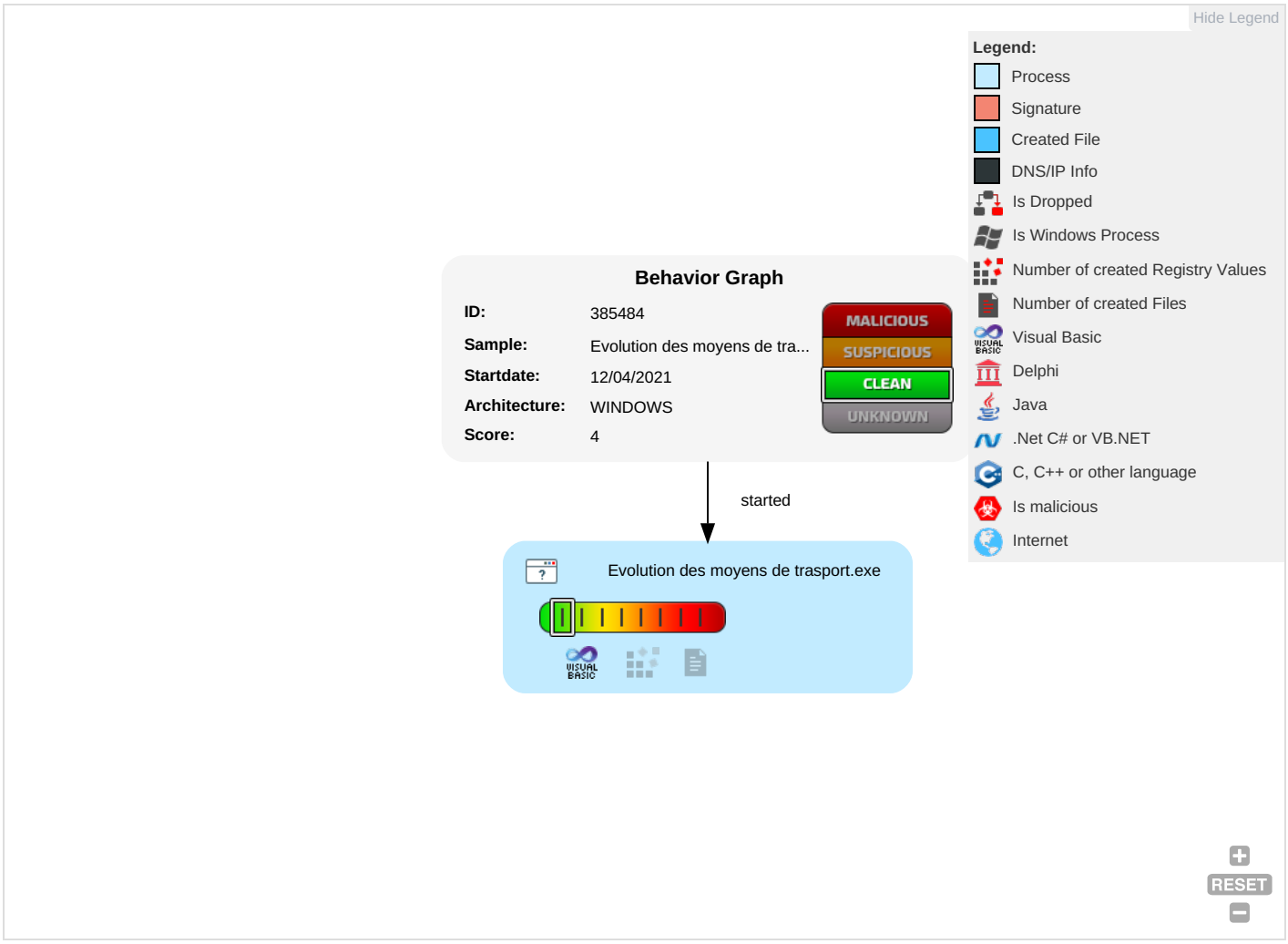
Click to jump to signature section

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	Impa
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1	Software Packing 1	OS Credential Dumping	Process Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modi Syst Parti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1	LSASS Memory	System Information 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	Devi Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Dele Devi Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carri Billin Frau

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
Evolution des moyens de trasport.exe	6%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Evolution des moyens de trasport.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
0.2.Evolution des moyens de trasport.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:	Evolution des moyens de trasport.exe	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385484
Start date:	12.04.2021
Start time:	15:25:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Evolution des moyens de trasport.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:	1
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:	clean4.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 97.9%) • Quality average: 83.4% • Quality standard deviation: 28.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated
Warnings:	Show All • VT rate limit hit for: /opt/package/joesandbox/database/analysis/385484/sample/Evolution des moyens de trasport.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):	6.736162650882512
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	Evolution des moyens de trasport.exe
File size:	4903529
MD5:	e31302978d2b065f030279b481e32344
SHA1:	2677beebffc4358d31e7eecdafa29f9ca0fffbd9
SHA256:	f238e71f708ab19db8bea0e3b69bdaa13d5b74ff6e658c00cec97ec212f22c58
SHA512:	974c009edc9526444d790432120374a934588aad2e6ad6190211051ff88fb75398c3a8e6613d70b57722ae124edf4d6f324ace1e2657014caa2081e5fb16ab04
SSDEEP:	98304:mcc0ccccocccQccccfcccccvl/bPd4WH9LBZMTJSE7RjPrxjSfc9Jo3hr7Ohr7W:MdFNB/E7R7rxOfc9JK+ctj
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...$....i.J.m...)zi.)zi.)zi.-Yd.(zi.Rich)zi.....PE..L....~.U.....@.....@.....P....@.....W.....

File Icon

Icon Hash:	c5ddccf8fcb2f870

Static PE Info

General

Entrypoint:	0x401404
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:	0x55C07EA6 [Tue Aug 4 08:58:14 2015 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:	0207dabeb8fc11ba1c54f26ac6d0c8df

Entrypoint Preview

Instruction
push 0040237Ch
call 00007F4F909B5C65h
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
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
hlt
inc ebx
adc dword ptr [edi-57B857FFh], edx
popfd
mov byte ptr [9B0A62F6h], al
bound eax, dword ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [edx], cl
dec ebp
outsd
jne 00007F4F909B5CDFh
push eax
dec esp
inc ecx
pop ecx
inc ebp
push edx
add byte ptr [ecx+00h], ch
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [ecx], dh
add byte ptr [ebx+edi*4+41h], bl

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1b4b24	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1c1000	0x67508	.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	0x220	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x19c	.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	0x1b3e14	0x1b4000	False	0.185924285049	data	3.89114007151	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1b5000	0xb2d4	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1c1000	0x67508	0x68000	False	0.160163292518	data	4.48340916271	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x21c3c0	0xa068	data		
RT_ICON	0x21bd58	0x668	dBase IV DBT of `.DBF, block length 1536, next free block index 40, next free block 33023, next used block 32512		
RT_ICON	0x21ba70	0x2e8	data		
RT_ICON	0x21b948	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x209520	0x12428	dBase IV DBT, blocks size 0, block length 8192, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x208678	0xea8	data		
RT_ICON	0x207dd0	0x8a8	data		
RT_ICON	0x207868	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1c5840	0x42028	dBase IV DBT, blocks size 0, block length 8192, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1c3298	0x25a8	data		
RT_ICON	0x1c21f0	0x10a8	data		
RT_ICON	0x1c1d88	0x468	GLS_BINARY_LSB_FIRST		
RT_STRING	0x226428	0xe0	data	English	United States
RT_GROUP_ICON	0x1c1cd8	0xb0	data		
RT_VERSION	0x1c1390	0x948	data	English	United States
RT_MANIFEST	0x226508	0x2000	XML 1.0 document, ASCII text, with CRLF, CR line terminators	English	United States

Imports

DLL	Import
MSVBVM60.DLL	EVENT_SINK_GetIDsOfNames, MethCallEngine, EVENT_SINK_Invoke, Zombie_GetTypeInfo, EVENT_SINK2_Release, EVENT_SINK_AddRef, DllFunctionCall, Zombie_GetTypeInfoCount, EVENT_SINK_Release, EVENT_SINK_QueryInterface, __vbaExceptHandler, ProcCallEngine, EVENT_SINK2_AddRef

Version Infos

Description	Data
Translation	0x0409 0x04b0
LegalCopyright	2020
InternalName	Evolution des moyens de trasport
FileVersion	0.0.0.0
CompanyName	techno-flash.com
LegalTrademarks	
Comments	
ProductName	Associer des produits un besoin
ProductVersion	0.0.0.0
FileDescription	
OriginalFilename	Evolution des moyens de trasport.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: Evolution des moyens de trasport.exe PID: 1256 Parent PID: 5804

General

Start time:	15:26:36
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Evolution des moyens de trasport.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Evolution des moyens de trasport.exe'
Imagebase:	0x400000
File size:	4903529 bytes
MD5 hash:	E31302978D2B065F030279B481E32344
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

Disassembly

Code Analysis