ID: 385486
Sample Name: TPZi2Evolution des moyens de trasport.exe
Cookbook: default.jbs
Time: 15:26:52
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright Joe Security LLC 2021

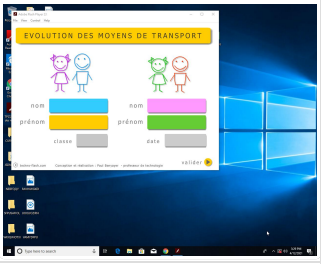
Analysis Report TPZi2Evolution des moyens de traspor…

Overview

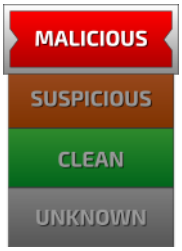
General Information

Sample Name:	TPZi2Evolution des moyens de trasport.exe
Analysis ID:	385486
MD5:	3ffead9503aef3d…
SHA1:	94596dc41a99f7e.
SHA256:	fc3adb1a06fb6e6..
Infos:	

Most interesting Screenshot:



Detection

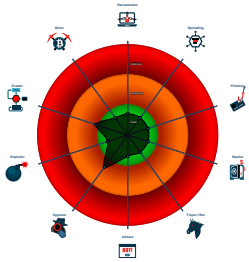


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Icon mismatch, binary includes an ic…
- Creates a DirectInput object (often fo…
- Installs a global mouse hook
- Monitors certain registry keys / valu…
- PE file contains an invalid checksum
- PE file contains sections with non-s…
- PE file contains strange resources
- Sample file is different than original …
- Tries to load missing DLLs
- Uses 32bit PE files

Classification



Startup

- **System is w10x64**
- TPZi2Evolution des moyens de trasport.exe (PID: 6724 cmdline: 'C:\Users\user\Desktop\TPZi2Evolution des moyens de trasport.exe' MD5: 3FFEAD9503AEF3DD3C60FC58B0C41D01)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

● Compliance

Copyright Joe Security LLC 2021

Click to jump to signature section

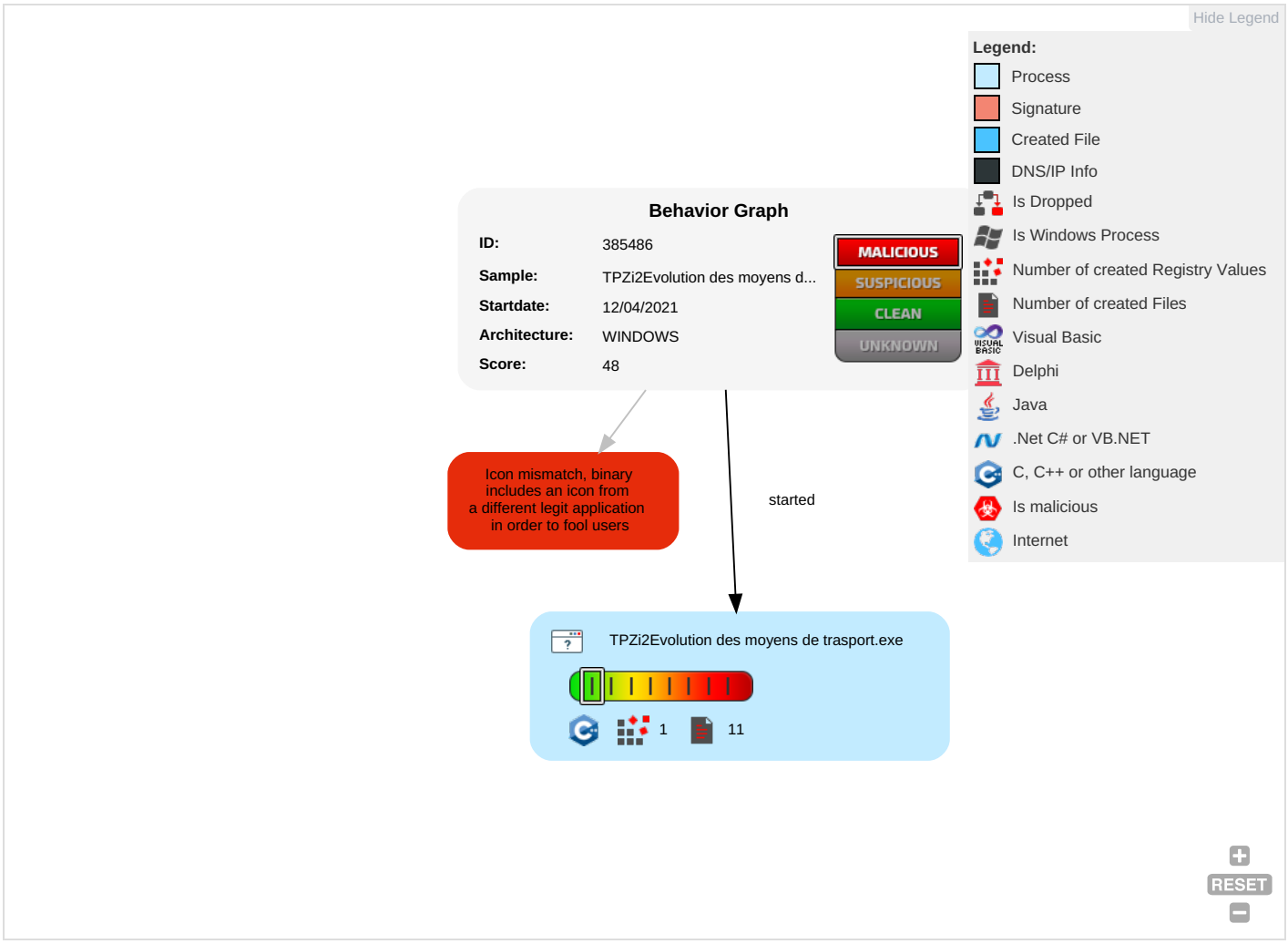
Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

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	I
Valid Accounts	Command and Scripting Interpreter 2	DLL Side-Loading 1	Process Injection 1	Masquerading 1 1	Input Capture 2	Query Registry 1	Remote Services	Input Capture 2	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S F
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 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	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D

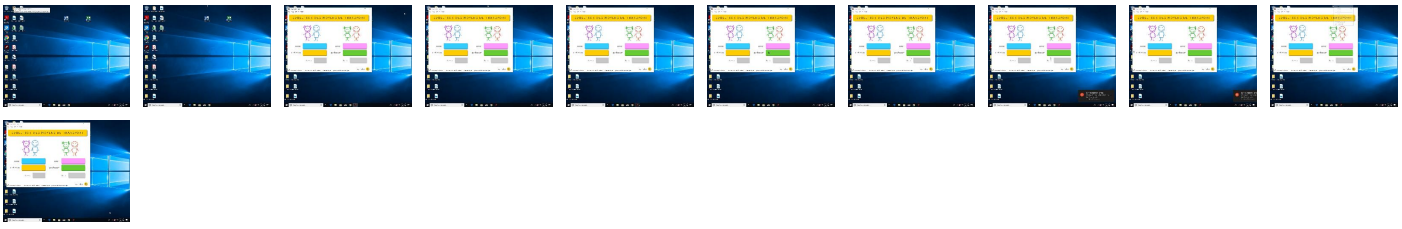
Behavior Graph

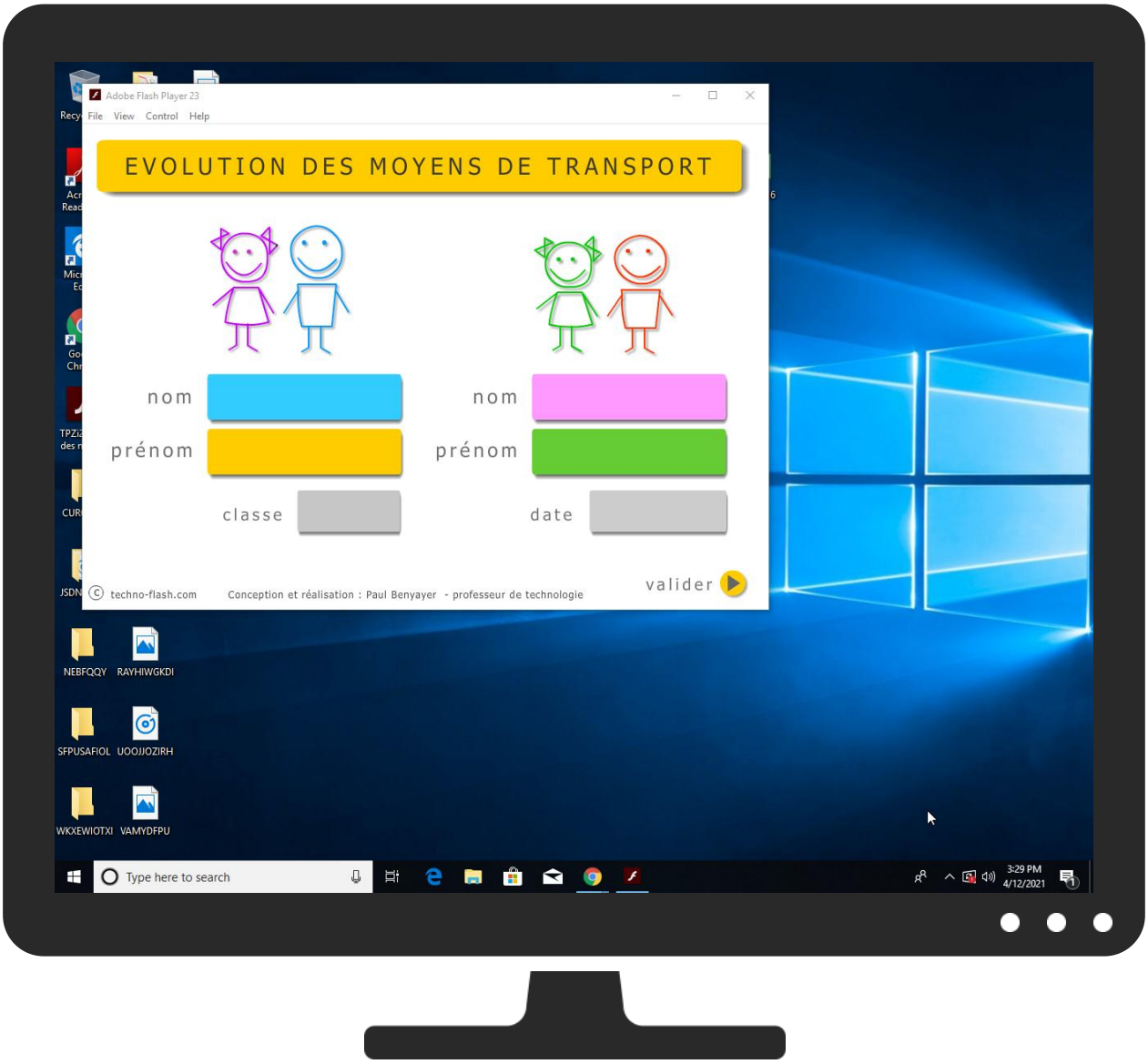


Screenshots

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
TPZi2Evolution des moyens de trasport.exe	0%	Virustotal		Browse
TPZi2Evolution des moyens de trasport.exe	2%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://auth.adobefpl.com/1/	0%	Virustotal		Browse
http://https://auth.adobefpl.com/1/	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://https://primetimeenablement.sc.omtrdc.net/b/ss//6primesample2	0%	Avira URL Cloud	safe	
http://%shttp://a.SharedObject.BadPersistenceSharedObject.UriMismatchpending.heu.swz	0%	Avira URL Cloud	safe	
http://cdn2.auditude.com/assets/3p/vService	0%	Avira URL Cloud	safe	
http://ad./adserver/e?type=playererrorhttp://ad.auditude.com/adserver/e?type=playererror//_.dashmpd&	0%	Avira URL Cloud	safe	
http://dashif.org/guidelines/trickmode1	0%	Avira URL Cloud	safe	
http://www.macromedia.comhttps://www.macromedia.com/support/flashplayer/sys/&	0%	Avira URL Cloud	safe	
http://https://primetimeenablement.sc.omtrdc.net/b/ss//6	0%	Avira URL Cloud	safe	
http://ad.auditude.com/adserver/e?type=playererror	0%	Avira URL Cloud	safe	
http://dashif.org/guidelines/trickmode	0%	Avira URL Cloud	safe	
http://ad./adserver?tm=15&u=&u=&l=&z=&of=1.4&g=Auditude	0%	Avira URL Cloud	safe	
http://cdn2.auditude.com/assets/3p/v	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://www.macromedia.com	TPZi2Evolution des moyens de trasport.exe	false		high
http://https://www.macromedia.com/support/flashplayer/sys/x	TPZi2Evolution des moyens de trasport.exe, 00000001.00000002.612301693.0000000005815000.00000004.00000040.sdmp	false		high
http://https://auth.adobefpl.com/1/	TPZi2Evolution des moyens de trasport.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.macromedia.com/support/flashplayer/sys/rs	TPZi2Evolution des moyens de trasport.exe, 00000001.00000002.612301693.0000000005815000.00000004.00000040.sdmp	false		high
http://ocsp.thawte.com0	TPZi2Evolution des moyens de trasport.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.macromedia.com/support/flashplayer/sys/.	TPZi2Evolution des moyens de trasport.exe, 00000001.00000002.612301693.0000000005815000.00000004.00000040.sdmp	false		high
http://https://primetimeenablement.sc.omtrdc.net/b/ss//6primesample2	TPZi2Evolution des moyens de trasport.exe	false	• Avira URL Cloud: safe	unknown
http://%shttp://a.SharedObject.BadPersistenceSharedObject.UriMismatchpending.heu.swz	TPZi2Evolution des moyens de trasport.exe	false	• Avira URL Cloud: safe	low
http://s3.amazonaws.com/venkat-test/ads/camry/file-640k.m3u82L	TPZi2Evolution des moyens de trasport.exe	false		high
http://cdn2.auditude.com/assets/3p/vService	TPZi2Evolution des moyens de trasport.exe	false	• Avira URL Cloud: safe	unknown
http://s3.amazonaws.com/venkat-test/ads/camry/file-640k.m3u8	TPZi2Evolution des moyens de trasport.exe	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	TPZi2Evolution des moyens de trasport.exe	false		high
http://www.macromedia.com/go/player_settings_	TPZi2Evolution des moyens de trasport.exe	false		high
http://ad./adserver/e?type=playererrorhttp://ad.auditude.com/adserver/e?type=playererror//_.dashmpd&	TPZi2Evolution des moyens de trasport.exe	false	• Avira URL Cloud: safe	unknown
http://dashif.org/guidelines/trickmode1	TPZi2Evolution des moyens de trasport.exe	false	• Avira URL Cloud: safe	unknown
http://fpdownload2.macromedia.com/get/	TPZi2Evolution des moyens de trasport.exe	false		high
http://www.macromedia.comhttps://www.macromedia.com/support/flashplayer/sys/&	TPZi2Evolution des moyens de trasport.exe	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://primetimeenablement.sc.omtrdc.net/b/ss//6	TPZi2Evolution des moyens de trasport.exe	false	• Avira URL Cloud: safe	unknown
http://ad.auditude.com/adserver/e?type=playererror	TPZi2Evolution des moyens de trasport.exe	false	• Avira URL Cloud: safe	unknown
http://dashif.org/guidelines/trickmode	TPZi2Evolution des moyens de trasport.exe	false	• Avira URL Cloud: safe	unknown
http://https://ats.macromedia.com/Players/ATS/ATS10AS3/Shipping/html/Security/ProtectedMode/PenTestDriverDL	TPZi2Evolution des moyens de trasport.exe	false		high
http://www.macromedia.com/go/player_settings_.Unmuted.MutedCamera.UnmutedCamera.MutedMicrophone.Unmu	TPZi2Evolution des moyens de trasport.exe	false		high
http://ad./adserver?tm=15&u=&u=&l=&z=&of=1.4&g=Auditude	TPZi2Evolution des moyens de trasport.exe	false	• Avira URL Cloud: safe	unknown
http://https://www.macromedia.com/bin/flashdownload.cgi	TPZi2Evolution des moyens de trasport.exe	false		high
http://https://www.macromedia.com/support/flashplayer/sys/	TPZi2Evolution des moyens de trasport.exe	false		high
http://https://fpdownload.macromedia.com/get/	TPZi2Evolution des moyens de trasport.exe	false		high
http://cdn2.auditude.com/assets/3p/v	TPZi2Evolution des moyens de trasport.exe	false	• Avira URL Cloud: safe	unknown
http://fpdownload2.macromedia.com/get/https://fpdownload.macromedia.com/get/https://www.macromedia.c	TPZi2Evolution des moyens de trasport.exe	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385486
Start date:	12.04.2021
Start time:	15:26:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TPZi2Evolution 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:	22
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:	mal48.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed

Copyright Joe Security LLC 2021

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

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

C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sxx	
Process:	C:\Users\user\Desktop\TPZi2Evolution des moyens de trasport.exe
File Type:	data
Category:	dropped
Size (bytes):	3058
Entropy (8bit):	4.522136039388766
Encrypted:	false
SSDEEP:	48:rFyq96326q6pA6pR6p9s6p9CiHF6p9Cid6p9Ciy6p9CiG6p9Ci+:KFhher3rCJrCHrC0rCErC
MD5:	2B7040E47AF0BF2F2571CB0D62915E24
SHA1:	992CF691BC68865A9A0C38FF3FD204ACD2AEB28E
SHA-256:	B54E96CCD7489B3ACDD276B7853F91167E3BBF1584F66653945BE17909442FD0
SHA-512:	B35D7279523DE13D9C995AE374DE51C4EF291737ED3835BBEC6E39668E7E696323921AFCAF39FFDD5AC1F62F836B286E6C8FEF6623C04E82853753B184A6471

C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sxx	
Malicious:	false
Reputation:	low
Preview:	.....(TCSO.....settings.....gain.@I.....<TCSO.....settings.....gain.@I.....echosuppression.....STCSO.....settings.....gain.@I.....echosuppression.....defaultmicrophone.....fTCSO.....settings.....gain.@I.....echosuppression.....defaultmicrophone.....defaultcamera.....TCSO.....settings.....gain.@I.....echosuppression.....defaultmicrophone.....defaultcamera.....defaultklimit.@Y.....TCSO.....settings.....gain.@I.....echosuppression.....defaultmicrophone.....defaultcamera.....defaultklimit.@Y.....defaultalways.....TCSO.....settings.....gain.@I.....echosuppression.....defaultmicrophone.....defaultcamera.....defaultklimit.@Y.....defaultalways.....windowlessDisable.....TCSO.....settings.....gain.@I.....echosuppression.....defaultmicrophone.....defaultcamera.....defaultklimit.@Y.....defaultalways.....windowlessDisable.....crossdomainAllow.....TCSO.....settings.....gain.@I.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.987146009315598
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:	TPZi2Evolution des moyens de trasport.exe
File size:	17140460
MD5:	3ffead9503aef3dd3c60fc58b0c41d01
SHA1:	94596dc41a99f7e6c3f5209e3d65d797082ec93b
SHA256:	fc3adb1a06fb6e66dc53ad01726b85af4c296a3438a49df73b98b7d481f6d154
SHA512:	029d2d3e473aa3242b3ed1e744c243366b8126c11dfa349a5fb71c7696a48348ac85f30d2961b0f5752e036c8f5af3543d782ffa0332f2d4cc1495fee5a7010a
SSDEEP:	393216:zmZhRuI5NoDil/XS8SOzzX/Zi3+Af1oRSqnmaBJ7:zmZhRTl9Dyf12SB4d
File Content Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....[.E.:...:...:...uz..:...By..:...:...:...Be...:.....:.....:..k5...:...:..(8.....:...Bo.6;...hh..:...Bh.O>...B~..:...hx..:.

File Icon

Icon Hash:	92eae4b2d8889608

Static PE Info

General

Entrypoint:	0xc969e2
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x57C4C9DD [Mon Aug 29 23:48:45 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	ac44d030aac7077131ee014b7adc735c

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

Instruction
call 00007F1584EB828Dh
jmp 00007F1584EAD95Dh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov esi, ecx
mov byte ptr [esi+0Ch], 00000000h
test eax, eax
jne 00007F1584EADB45h
call 00007F1584EB713Eh
mov dword ptr [esi+08h], eax
mov ecx, dword ptr [eax+6Ch]
mov dword ptr [esi], ecx
mov ecx, dword ptr [eax+68h]
mov dword ptr [esi+04h], ecx
mov ecx, dword ptr [esi]
cmp ecx, dword ptr [00FFB9D0h]
je 00007F1584EADAF4h
mov ecx, dword ptr [00FFB8ECh]
test dword ptr [eax+70h], ecx
jne 00007F1584EADAE9h
call 00007F1584EB8C70h
mov dword ptr [esi], eax
mov eax, dword ptr [esi+04h]
cmp eax, dword ptr [00FFB7F0h]
je 00007F1584EADAF8h
mov eax, dword ptr [esi+08h]
mov ecx, dword ptr [00FFB8ECh]
test dword ptr [eax+70h], ecx
jne 00007F1584EADAEAh
call 00007F1584EB84E4h
mov dword ptr [esi+04h], eax
mov eax, dword ptr [esi+08h]
test byte ptr [eax+70h], 00000002h
jne 00007F1584EADAF6h
or dword ptr [eax+70h], 02h
mov byte ptr [esi+0Ch], 00000001h
jmp 00007F1584EADAECh
mov ecx, dword ptr [eax]
mov dword ptr [esi], ecx
mov eax, dword ptr [eax+04h]
mov dword ptr [esi+04h], eax
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp

Copyright Joe Security LLC 2021

Instruction
mov ebp, esp
sub esp, 10h
push dword ptr [ebp+0Ch]
lea ecx, dword ptr [ebp-10h]
call 00007F1584EADA4Bh
mov eax, dword ptr [ebp-10h]
cmp dword ptr [eax+000000ACh], 01h
jle 00007F1584EADAF8h
lea eax, dword ptr [ebp-10h]
push eax
push 00000103h
push dword ptr [ebp+08h]
call 00007F1584EB8C6Fh
add esp, 0Ch
jmp 00007F1584EADAF4h
mov eax, dword ptr [eax+00000000h]

Rich Headers

Programming Language:	• [ASM] VS2008 SP1 build 30729 • [C] VS2008 SP1 build 30729 • [C] VS2005 build 50727 • [C++] VS2005 build 50727 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [C++] VS2008 build 21022 • [EXP] VS2008 SP1 build 30729 • [C++] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xb2e2e0	0xd2	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb2ce6c	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xcec000	0x1c1044	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xe2b800	0x18f8	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xeae000	0x542a0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x956a00	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xaf7d40	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x956000	0x38c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0xb2a5b8	0x220	.rdata
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	0x952ada	0x952c00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rodata	0x954000	0x10e0	0x1200	False	0.215277777778	data	4.16783024928	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x956000	0x1d83b2	0x1d8400	False	0.435927367324	data	6.53070366078	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xb2f000	0x1bc188	0xcec00	False	0.745528123111	data	7.53274240162	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xcec000	0x1c1044	0x1c1200	False	0.057476669044	data	4.32823409135	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xeae000	0x6f3b0	0x6f400	False	0.323817152388	data	5.57559035468	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xcedd08	0x134	data	English	United States
RT_CURSOR	0xcede3c	0xb4	data	English	United States
RT_CURSOR	0xcedef0	0x134	data	English	United States
RT_ICON	0xcee024	0x42028	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xd3004c	0x25a8	data	English	United States
RT_ICON	0xd325f4	0x10a8	data	English	United States
RT_ICON	0xd3369c	0x988	data	English	United States
RT_ICON	0xd34024	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xd3448c	0xea8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xd35334	0x8a8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xd35bdc	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xd36144	0x42028	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xd7816c	0x25a8	data	English	United States
RT_ICON	0xd7a714	0x10a8	data	English	United States
RT_ICON	0xd7b7bc	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xd7bc24	0xea8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xd7cacc	0x8a8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xd7d374	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xd7d8dc	0x42028	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xdbf904	0x25a8	data	English	United States
RT_ICON	0xdc1eac	0x10a8	data	English	United States
RT_ICON	0xdc2f54	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xdc33bc	0xea8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xdc4264	0x8a8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xdc4b0c	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xdc5074	0x42028	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xe0709c	0x25a8	data	English	United States
RT_ICON	0xe09644	0x10a8	data	English	United States
RT_ICON	0xe0a6ec	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xe0ab54	0xea8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xe0b9fc	0x8a8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xe0c2a4	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xe0c80c	0x42028	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xe4e834	0x25a8	data	English	United States
RT_ICON	0xe50ddc	0x10a8	data	English	United States
RT_ICON	0xe51e84	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xe522ec	0xea8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xe53194	0x8a8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xe53a3c	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xe53fa4	0x42028	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xe95fcc	0x25a8	data	English	United States
RT_ICON	0xe98574	0x10a8	data	English	United States
RT_ICON	0xe9961c	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_MENU	0xe99a84	0x300	data		
RT_MENU	0xe99d84	0x284	data	Chinese	Taiwan
RT_MENU	0xe9a008	0x358	data	Czech	Czech Republic
RT_MENU	0xe9a360	0x34e	data	German	Germany
RT_MENU	0xe9a6b0	0x2d4	data	English	United States
RT_MENU	0xe9a984	0x344	data	French	France
RT_MENU	0xe9acc8	0x314	data	Italian	Italy
RT_MENU	0xe9afdc	0x2b2	data	Japanese	Japan
RT_MENU	0xe9b290	0x2a0	data	Korean	North Korea

Name	RVA	Size	Type	Language	Country
RT_MENU	0xe9b290	0x2a0	data	Korean	South Korea
RT_MENU	0xe9b530	0x35a	data	Dutch	Netherlands
RT_MENU	0xe9b88c	0x330	data	Polish	Poland
RT_MENU	0xe9bbbc	0x33e	data	Portuguese	Brazil
RT_MENU	0xe9befc	0x366	data	Russian	Russia
RT_MENU	0xe9c264	0x300	data	Turkish	Turkey
RT_MENU	0xe9c564	0x27a	data	Chinese	China
RT_MENU	0xe9c7e0	0x30c	data		
RT_MENU	0xe9caec	0x23a	data		
RT_MENU	0xe9cd28	0x136	data	Chinese	Taiwan
RT_MENU	0xe9ce60	0x250	data	Czech	Czech Republic
RT_MENU	0xe9d0b0	0x236	data	German	Germany
RT_MENU	0xe9d2e8	0x1f0	data	English	United States
RT_MENU	0xe9d4d8	0x244	data	French	France
RT_MENU	0xe9d71c	0x228	data	Italian	Italy
RT_MENU	0xe9d944	0x158	data	Japanese	Japan
RT_MENU	0xe9da9c	0x15c	data	Korean	North Korea
RT_MENU	0xe9da9c	0x15c	data	Korean	South Korea
RT_MENU	0xe9dbf8	0x258	data	Dutch	Netherlands
RT_MENU	0xe9de50	0x246	data	Polish	Poland
RT_MENU	0xe9e098	0x24a	data	Portuguese	Brazil
RT_MENU	0xe9e2e4	0x26c	data	Russian	Russia
RT_MENU	0xe9e550	0x216	data	Turkish	Turkey
RT_MENU	0xe9e768	0x142	data	Chinese	China
RT_MENU	0xe9e8ac	0x220	data		
RT_MENU	0xe9eacc	0x92	data		
RT_MENU	0xe9eb60	0x6a	data	Chinese	Taiwan
RT_MENU	0xe9ebcc	0x8a	data	Czech	Czech Republic
RT_MENU	0xe9ec58	0x9c	data	German	Germany
RT_MENU	0xe9ecf4	0x70	data	English	United States
RT_MENU	0xe9ed64	0x90	data	French	France
RT_MENU	0xe9edf4	0x88	data	Italian	Italy
RT_MENU	0xe9ee7c	0x7a	data	Japanese	Japan
RT_MENU	0xe9eef8	0x78	data	Korean	North Korea
RT_MENU	0xe9eef8	0x78	data	Korean	South Korea
RT_MENU	0xe9ef70	0x9c	data	Dutch	Netherlands
RT_MENU	0xe9f00c	0x82	data	Polish	Poland
RT_MENU	0xe9f090	0x8a	data	Portuguese	Brazil
RT_MENU	0xe9f11c	0x92	data	Russian	Russia
RT_MENU	0xe9f1b0	0x76	data	Turkish	Turkey
RT_MENU	0xe9f228	0x6a	data	Chinese	China
RT_MENU	0xe9f294	0x8c	data		
RT_MENU	0xe9f320	0x50	data		
RT_MENU	0xe9f370	0x34	data	Chinese	Taiwan
RT_MENU	0xe9f3a4	0x5e	data	Czech	Czech Republic
RT_MENU	0xe9f404	0x6a	data	German	Germany
RT_MENU	0xe9f470	0x4c	data	English	United States
RT_MENU	0xe9f4bc	0x62	data	French	France
RT_MENU	0xe9f520	0x5e	data	Italian	Italy
RT_MENU	0xe9f580	0x3e	data	Japanese	Japan
RT_MENU	0xe9f5c0	0x38	data	Korean	North Korea
RT_MENU	0xe9f5c0	0x38	data	Korean	South Korea
RT_MENU	0xe9f5f8	0x60	data	Dutch	Netherlands
RT_MENU	0xe9f658	0x58	data	Polish	Poland
RT_MENU	0xe9f6b0	0x52	data	Portuguese	Brazil
RT_MENU	0xe9f704	0x6e	data	Russian	Russia
RT_MENU	0xe9f774	0x5c	data	Turkish	Turkey
RT_MENU	0xe9f7d0	0x34	data	Chinese	China
RT_MENU	0xe9f804	0x60	data		
RT_DIALOG	0xe9f864	0x1ea	data		
RT_DIALOG	0xe9fa50	0x1e2	data	Chinese	Taiwan
RT_DIALOG	0xe9fc34	0x1e2	data	Czech	Czech Republic
RT_DIALOG	0xe9fe18	0x1e2	data	German	Germany
RT_DIALOG	0xe9fffc	0x1e2	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0xea01e0	0x1e2	data	French	France
RT_DIALOG	0xea03c4	0x1e2	data	Italian	Italy
RT_DIALOG	0xea05a8	0x1e6	data	Japanese	Japan
RT_DIALOG	0xea0790	0x1e2	data	Korean	North Korea
RT_DIALOG	0xea0790	0x1e2	data	Korean	South Korea
RT_DIALOG	0xea0974	0x1e6	data	Dutch	Netherlands
RT_DIALOG	0xea0b5c	0x1e2	data	Polish	Poland
RT_DIALOG	0xea0d40	0x1e6	data	Portuguese	Brazil
RT_DIALOG	0xea0f28	0x1e6	data	Russian	Russia
RT_DIALOG	0xea1110	0x1e6	data	Turkish	Turkey
RT_DIALOG	0xea12f8	0x1e6	data	Chinese	China
RT_DIALOG	0xea14e0	0x1ee	data		
RT_DIALOG	0xea16d0	0x1a4	data		
RT_DIALOG	0xea1874	0x138	data	Chinese	Taiwan
RT_DIALOG	0xea19ac	0x1dc	data	Czech	Czech Republic
RT_DIALOG	0xea1b88	0x1d0	data	German	Germany
RT_DIALOG	0xea1d58	0x1ca	data	English	United States
RT_DIALOG	0xea1f24	0x1b8	data	French	France
RT_DIALOG	0xea20dc	0x1c0	data	Italian	Italy
RT_DIALOG	0xea229c	0x170	data	Japanese	Japan
RT_DIALOG	0xea240c	0x148	data	Korean	North Korea
RT_DIALOG	0xea240c	0x148	data	Korean	South Korea
RT_DIALOG	0xea2554	0x1de	data	Dutch	Netherlands
RT_DIALOG	0xea2734	0x1ce	data	Polish	Poland
RT_DIALOG	0xea2904	0x1ca	data	Portuguese	Brazil
RT_DIALOG	0xea2ad0	0x1d0	data	Russian	Russia
RT_DIALOG	0xea2ca0	0x1b0	data	Turkish	Turkey
RT_DIALOG	0xea2e50	0x138	data	Chinese	China
RT_DIALOG	0xea2f88	0x1ce	data		
RT_DIALOG	0xea3158	0x60	data	English	United States
RT_DIALOG	0xea31b8	0x456	data		
RT_DIALOG	0xea3610	0x2b2	data	Chinese	Taiwan
RT_DIALOG	0xea38c4	0x466	data	Czech	Czech Republic
RT_DIALOG	0xea3d2c	0x4b2	data	German	Germany
RT_DIALOG	0xea41e0	0x434	data	English	United States
RT_DIALOG	0xea4614	0x4dc	data	French	France
RT_DIALOG	0xea4af0	0x48c	data	Italian	Italy
RT_DIALOG	0xea4f7c	0x32a	data	Japanese	Japan
RT_DIALOG	0xea52a8	0x32a	data	Korean	North Korea
RT_DIALOG	0xea52a8	0x32a	data	Korean	South Korea
RT_DIALOG	0xea55d4	0x47c	data	Dutch	Netherlands
RT_DIALOG	0xea5a50	0x4b0	data	Polish	Poland
RT_DIALOG	0xea5f00	0x46e	data	Portuguese	Brazil
RT_DIALOG	0xea6370	0x46a	data	Russian	Russia
RT_DIALOG	0xea67dc	0x442	data	Turkish	Turkey
RT_DIALOG	0xea6c20	0x2ba	data	Chinese	China
RT_DIALOG	0xea6edc	0x2b2	data	Chinese	China
RT_DIALOG	0xea7190	0x47a	data		
RT_STRING	0xea760c	0x26e	data		
RT_STRING	0xea787c	0x24a	data	Chinese	Taiwan
RT_STRING	0xea7ac8	0x274	data	Czech	Czech Republic
RT_STRING	0xea7d3c	0x274	data	German	Germany
RT_STRING	0xea7fb0	0x26e	data	English	United States
RT_STRING	0xea8220	0x280	data	French	France
RT_STRING	0xea84a0	0x278	data	Italian	Italy
RT_STRING	0xea8718	0x264	data	Japanese	Japan
RT_STRING	0xea897c	0x250	data	Korean	North Korea
RT_STRING	0xea897c	0x250	data	Korean	South Korea
RT_STRING	0xea8bcc	0x294	data	Dutch	Netherlands
RT_STRING	0xea8e60	0x274	data	Polish	Poland
RT_STRING	0xea90d4	0x280	data	Portuguese	Brazil
RT_STRING	0xea9354	0x26c	data	Russian	Russia
RT_STRING	0xea95c0	0x276	data	Turkish	Turkey
RT_STRING	0xea9838	0x24a	data	Chinese	China

Name	RVA	Size	Type	Language	Country
RT_STRING	0xea9a84	0x286	data		
RT_STRING	0xea9d0c	0x11c	data		
RT_STRING	0xea9e28	0x6c	data	Chinese	Taiwan
RT_STRING	0xea9e94	0x138	data	Czech	Czech Republic
RT_STRING	0xea9fcc	0x14e	data	German	Germany
RT_STRING	0xeaa11c	0x106	data	English	United States
RT_STRING	0xeaa224	0x152	data	French	France
RT_STRING	0xeaa378	0x138	data	Italian	Italy
RT_STRING	0xeaa4b0	0xb0	data	Japanese	Japan
RT_STRING	0xeaa560	0xa0	data	Korean	North Korea
RT_STRING	0xeaa560	0xa0	data	Korean	South Korea
RT_STRING	0xeaa600	0x162	data	Dutch	Netherlands
RT_STRING	0xeaa764	0x15a	data	Polish	Poland
RT_STRING	0xeaa8c0	0x110	data	Portuguese	Brazil
RT_STRING	0xeaa9d0	0x140	data	Russian	Russia
RT_STRING	0xeaab10	0x122	data	Turkish	Turkey
RT_STRING	0xeaac34	0x74	data	Chinese	China
RT_STRING	0xeaaca8	0x138	data		
RT_STRING	0xeaade0	0xec	data		
RT_STRING	0xeaaecc	0x7a	data	Chinese	Taiwan
RT_STRING	0xeaaf48	0x154	data	Czech	Czech Republic
RT_STRING	0xeab09c	0x10c	data	German	Germany
RT_STRING	0xeab1a8	0xca	data	English	United States
RT_STRING	0xeab274	0x106	data	French	France
RT_STRING	0xeab37c	0xfa	data	Italian	Italy
RT_STRING	0xeab478	0x8e	data	Japanese	Japan
RT_STRING	0xeab508	0x7c	data	Korean	North Korea
RT_STRING	0xeab508	0x7c	data	Korean	South Korea
RT_STRING	0xeab584	0x134	data	Dutch	Netherlands
RT_STRING	0xeab6b8	0xe4	data	Polish	Poland
RT_STRING	0xeab79c	0xf2	data	Portuguese	Brazil
RT_STRING	0xeab890	0x114	data	Russian	Russia
RT_STRING	0xeab9a4	0xb8	data	Turkish	Turkey
RT_STRING	0xeaba5c	0x6e	data	Chinese	China
RT_STRING	0xeabacc	0x138	data		
RT_STRING	0xeabc04	0x80	data		
RT_STRING	0xeabc84	0x52	data	Chinese	Taiwan
RT_STRING	0xeabcd8	0x9a	data	Czech	Czech Republic
RT_STRING	0xeabd74	0xaa	data	German	Germany
RT_STRING	0xeabe20	0x98	data	English	United States
RT_STRING	0xeabeb8	0xd6	data	French	France
RT_STRING	0xeabf90	0xaa	data	Italian	Italy
RT_STRING	0xeac03c	0x72	data	Japanese	Japan
RT_STRING	0xeac0b0	0x5a	data	Korean	North Korea
RT_STRING	0xeac0b0	0x5a	data	Korean	South Korea
RT_STRING	0xeac10c	0xa4	data	Dutch	Netherlands
RT_STRING	0xeac1b0	0x9c	data	Polish	Poland
RT_STRING	0xeac24c	0xb2	data	Portuguese	Brazil
RT_STRING	0xeac300	0x92	data	Russian	Russia
RT_STRING	0xeac394	0x98	data	Turkish	Turkey
RT_STRING	0xeac42c	0x52	data	Chinese	China
RT_STRING	0xeac480	0x52	data	Chinese	China
RT_STRING	0xeac4d4	0xc8	data		
RT_ACCELERATOR	0xeac59c	0x70	data	English	United States
RT_GROUP_CURSOR	0xeac60c	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0xeac630	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0xeac644	0x4c	data	English	United States
RT_GROUP_ICON	0xeac690	0x68	data	English	United States
RT_GROUP_ICON	0xeac6f8	0x68	data	English	United States
RT_GROUP_ICON	0xeac760	0x68	data	English	United States
RT_GROUP_ICON	0xeac7c8	0x68	data	English	United States
RT_GROUP_ICON	0xeac830	0x68	data	English	United States
RT_VERSION	0xeac898	0x4f8	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0xeacd90	0x2b2	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	WaitForSingleObject, GetProcAddress, GetModuleHandleW, ReadFile, SetFilePointer, GetFileSize, CreateFileW, GetModuleFileNameA, GetCommandLineW, SetEndOfFile, WriteFile, CreateFileA, GetFileAttributesA, GetStartupInfoW, GetCommandLineA, ExitProcess, RemoveDirectoryW, CopyFileW, GetModuleFileNameW, GetCPInfo, GetACP, IsDBCSLeadByte, HeapSize, DeviceIoControl, CreateProcessA, GetTempPathA, FindNextFileW, GetSystemWow64DirectoryW, ExpandEnvironmentStringsA, WideCharToMultiByte, MultiByteToWideChar, lstrlenW, GetLongPathNameW, CreateProcessW, GetTempFileNameA, CreateDirectoryA, DeleteFileA, GetFileAttributesW, CreateMutexA, SetFilePointerEx, GetFileSizeEx, GetFileAttributesExW, GetFileInformationByHandle, GetVolumeInformationW, MoveFileExW, GetCurrentDirectoryW, SetCurrentDirectoryW, GetFullPathNameW, ExpandEnvironmentStringsW, OutputDebugStringA, LoadLibraryA, GetSystemDirectoryA, FreeLibrary, GetVersionExW, GetCurrentProcess, VirtualQuery, ExitThread, GetUserDefaultLangID, GetUserDefaultUILanguage, VerifyVersionInfoW, VerSetConditionMask, GlobalFree, CreateThread, LockResource, LoadResource, FindResourceExA, FindResourceExW, GlobalAlloc, DebugBreak, GlobalUnlock, GlobalLock, QueryPerformanceCounter, QueryPerformanceFrequency, GlobalSize, QueueUserAPC, OpenThread, SleepEx, SetUnhandledExceptionFilter, GetCurrentProcessId, GetProcessTimes, RaiseException, FlushInstructionCache, SetLastError, TerminateThread, CreateEventW, SetEvent, ResetEvent, WaitForMultipleObjects, GetExitCodeProcess, GetTickCount, SetThreadPriority, GetTimeZoneInformation, GetSystemTime, SystemTimeToFileTime, GetLocaleInfoW, LCMapStringW, GetExitCodeThread, DuplicateHandle, GetCurrentThread, MapViewOfFile, UnmapViewOfFile, CompareFileTime, LocalFree, ReleaseMutex, CreateFileMappingA, ReleaseSemaphore, CreateSemaphoreW, SetThreadAffinityMask, CreateEventA, CreateWaitableTimerA, SetWaitableTimer, CancelWaitableTimer, InterlockedExchangeAdd, GetVersionExA, GetVersion, VirtualAlloc, VirtualFree, FlushFileBuffers, GlobalMemoryStatusEx, IsDebuggerPresent, SetSystemTime, FileTimeToSystemTime, TlsAlloc, TlsFree, ResumeThread, CreateTimerQueueTimer, DeleteTimerQueueTimer, CreateSemaphoreA, HeapAlloc, HeapFree, HeapUnlock, HeapWalk, HeapLock, HeapCreate, HeapDestroy, VirtualProtect, GetNumberFormatW, GetCurrencyFormatW, CompareStringW, GetDateFormatW, GetTimeFormatW, GetUserDefaultLCID, EnumSystemLocalesW, GetProcessHeap, GetProcessAffinityMask, IsProcessorFeaturePresent, GetStartupInfoA, RtlUnwind, UnhandledExceptionFilter, HeapReAlloc, GetSystemTimeAsFileTime, GetStdHandle, TerminateProcess, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetFileType, GetOEMCP, IsValidCodePage, LCMapStringA, GetConsoleCP, GetConsoleMode, InitializeCriticalSectionAndSpinCount, SetStdHandle, GetLocaleInfoA, GetStringTypeA, GetStringTypeW, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, CompareStringA, SetEnvironmentVariableA, LocalAlloc, CloseHandle, FindFirstFileW, FindClose, GetSystemDirectoryW, LoadLibraryW, GetModuleHandleA, GetTempPathW, GetTempFileNameW, GetLastError, DeleteFileW, CreateDirectoryW, GetSystemInfo, SwitchToThread, TlsGetValue, TlsSetValue, GetCurrentThreadId, LeaveCriticalSection, EnterCriticalSection, TryEnterCriticalSection, DeleteCriticalSection, InitializeCriticalSection, InterlockedDecrement, InterlockedIncrement, InterlockedExchange, InterlockedCompareExchange, CreateWaitableTimerW, Sleep
ADVAPI32.dll	CryptEncrypt, CryptDestroyKey, CryptImportKey, CryptSetKeyParam, CryptGetHashParam, CryptHashData, CryptDestroyHash, CryptAcquireContextA, CryptCreateHash, RegOpenKeyA, CryptAcquireContextW, CryptGenRandom, CryptReleaseContext, RegOpenKeyExA, RegQueryValueExW, RegSetValueExW, RegCreateKeyExW, RegSetValueExA, RegQueryValueExA, RegCloseKey, RegCreateKeyExA, RegOpenKeyExW, CryptDecrypt

Exports

Name	Ordinal	Address
IAEModule_AEModule_PutKernel	1	0x923ed0
IAEModule_IAEKernel_LoadModule	2	0x920150
IAEModule_IAEKernel_UnloadModule	3	0x9201d0
_WinMainSandboxed@20	4	0x41efc7

Version Infos

Description	Data
LegalCopyright	Adobe Flash Player. Copyright 1996-2016 Adobe Systems Incorporated. All Rights Reserved. Adobe and Flash are either trademarks or registered trademarks in the United States and/or other countries.
InternalName	Adobe Flash Player 23.0
FileVersion	23,0,0,162
CompanyName	Adobe Systems, Inc.
LegalTrademarks	Adobe Flash Player
ProductName	Shockwave Flash
ProductVersion	23,0,0,162
FileDescription	Adobe Flash Player 23.0 r0
OriginalFilename	SAFlashPlayer.exe
Debugger	0
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
English	United States	
Chinese	Taiwan	
Czech	Czech Republic	
German	Germany	
French	France	
Italian	Italy	
Japanese	Japan	
Korean	North Korea	
Korean	South Korea	
Dutch	Netherlands	
Polish	Poland	

Copyright Joe Security LLC 2021

Language of compilation system	Country where language is spoken	Map
Portuguese	Brazil	
Russian	Russia	
Turkish	Turkey	
Chinese	China	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: TPZi2Evolution des moyens de trasport.exe PID: 6724 Parent PID: 5868

General

Start time:	15:27:44
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\TPZi2Evolution des moyens de trasport.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TPZi2Evolution des moyens de trasport.exe'
Imagebase:	0x12d0000
File size:	17140460 bytes
MD5 hash:	3FFEAD9503AEF3DD3C60FC58B0C41D01
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Adobe\Flash Player\AssetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1322F42	CreateDirectoryW
C:\Users\user\AppData\Roaming\Adobe\Flash Player\AssetCache\USCRKX6F	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1322F42	CreateDirectoryW
C:\Users\user\AppData\Roaming\Macromedia	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1322F42	CreateDirectoryW
C:\Users\user\AppData\Roaming\Macromedia\Flash Player	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1322F42	CreateDirectoryW
C:\Users\user\AppData\Roaming\Macromedia\Flash Player\#SharedObjects	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1322F42	CreateDirectoryW
C:\Users\user\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\FKMANJZ6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1322F42	CreateDirectoryW
C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1322F42	CreateDirectoryW
C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1322F42	CreateDirectoryW
C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1322F42	CreateDirectoryW
C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1322F42	CreateDirectoryW
C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sxx	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | random access	success or wait	15	1321EAE	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol	success or wait	14	1322354	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sxx	C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol	success or wait	15	13223CD	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sxx	unknown	46	00 bf 00 00 00 28 54 43 53 4f 00 04 00 00 00 00 00 00 08 73 65 74 74 69 6e 67 73 00 00 00 00 00 04 67 61 69 6e 00 40 49 00 00 00 00 00 00 00	.....(TCSO.....settings....gain.@I.....	success or wait	15	1321CE9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\TPZi2Evolution des moyens de trasport.exe	unknown	8	success or wait	1	12EDA66	ReadFile
C:\Users\user\Desktop\TPZi2Evolution des moyens de trasport.exe	unknown	1	success or wait	1	12EDB24	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis

Copyright Joe Security LLC 2021