ID: 379126
Sample Name: Aflytter2.exe
Cookbook: default.jbs
Time: 15:37:14
Date: 31/03/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report Aflytter2.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
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 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 8
Contacted Domains 8
Contacted IPs 8
General Information 8
Simulations 8
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: Aflytter2.exe PID: 7120 Parent PID: 6048 13
General 13
File Activities 13
Disassembly 13
Code Analysis 13

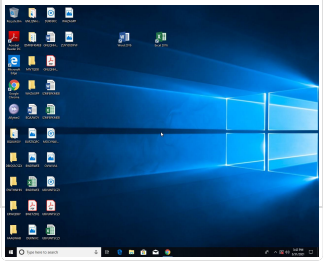
Analysis Report Aflytter2.exe

Overview

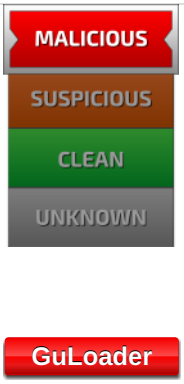
General Information

Sample Name:	Aflytter2.exe
Analysis ID:	379126
MD5:	327bdd165c67a0..
SHA1:	b9b3803795af6f6..
SHA256:	be630a75cb81b3..
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection

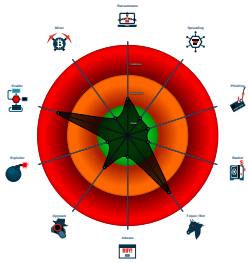


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- 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 …

Classification



Startup

- **System is w10x64**
- Aflytter2.exe (PID: 7120 cmdline: 'C:\Users\user\Desktop\Aflytter2.exe' MD5: 327BDD165C67A077606D414D038ECDA9)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

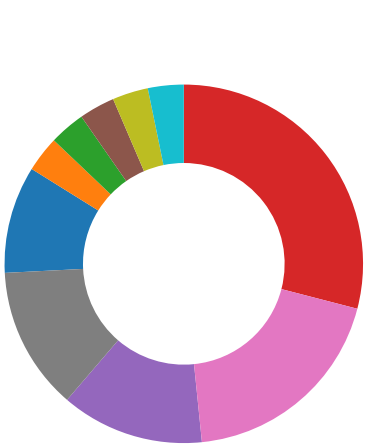
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Aflytter2.exe PID: 7120	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: Aflytter2.exe PID: 7120	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

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

Tries to detect virtualization through RDTSC time measurements

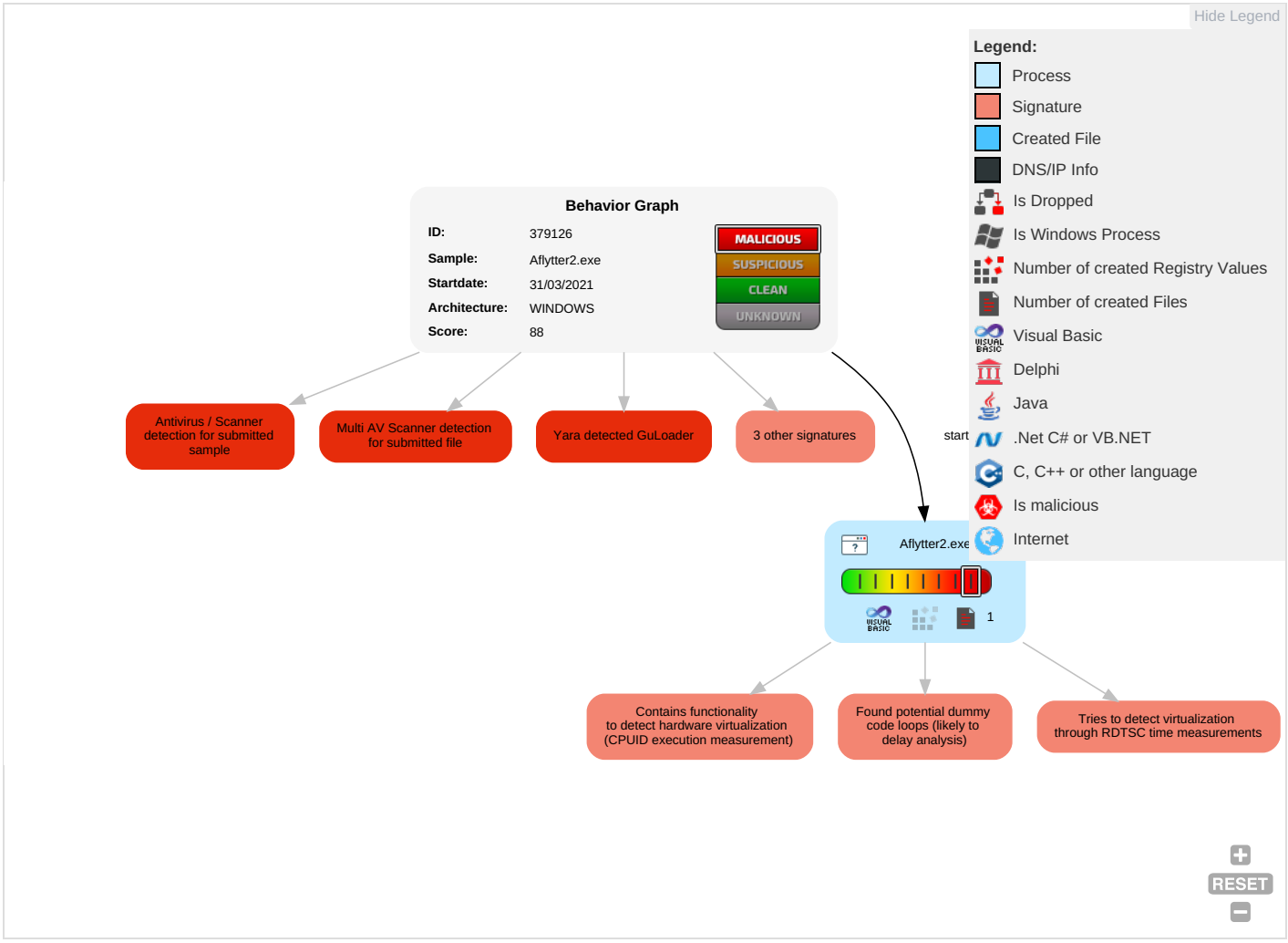
Anti Debugging:

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	Re Se Ef
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 4 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
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	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
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	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

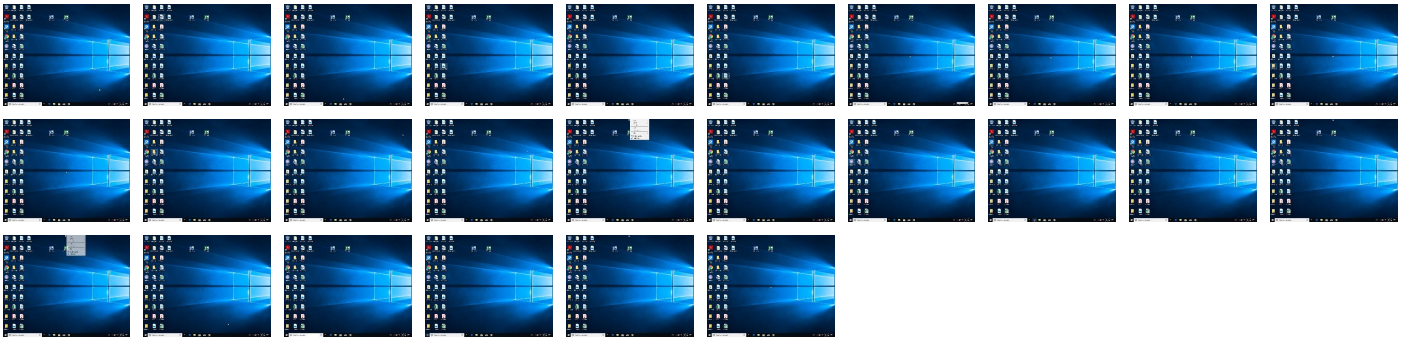
Behavior Graph



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
Aflytter2.exe	25%	ReversingLabs	Win32.Trojan.Generic	
Aflytter2.exe	100%	Avira	HEUR/AGEN.1138570	
Aflytter2.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Aflytter2.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138570		Download File
0.2.Aflytter2.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138570		Download File

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:	379126
Start date:	31.03.2021
Start time:	15:37:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Aflytter2.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:	mal88.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.8% (good quality ratio 8.6%) • Quality average: 22% • Quality standard deviation: 34.9%
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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • VT rate limit hit for: /opt/package/joesandbox/database/analysis/379126/sample/Aflytter2.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):	5.3468334683107805
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:	Aflytter2.exe
File size:	90112
MD5:	327bdd165c67a077606d414d038ecda9
SHA1:	b9b3803795af6f6c3c7e8a6c06a23652bb07769f
SHA256:	be630a75cb81b3ed6624660e3c909867771e810e0733fa a6dc8a571defa590d3
SHA512:	3887b2868dbb76b01452a384a498ea62366c0f11c217e9 0387886ef7d382e9c2d9e18b1a74134cae4dd48f561d0c7 d9d55d90d3b89600908af273799bd545625
SSDEEP:	768:TZIEf4SA56SWwOmHH9ah33VHY4badYE7qpS16 MNxz2K3byT/MK9vY:Nrk5iw/q3DbaDAmR0x
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....u...1...1. ..1.....0...~...0.....0...Rich1.....PE..L.....U..... . ...0.....0....@.....

File Icon

Icon Hash:	f1f8f6f0f0e4f831

Static PE Info

General

Entrypoint:	0x4016fc
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:	0x55FBF294 [Fri Sep 18 11:16:36 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:	c78f78af0a4b82efe93f926bf0040578

Entrypoint Preview

Instruction
push 0040CA94h
call 00007F576CD7B515h
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-517312F2h], al
jecxz 00007F576CD7B53Ah
inc ebx
call far 2F93h : 9F4A41A5h
jl 00007F576CD7B522h
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+7Ah], ah
cli
add ah, byte ptr [ebx+75h]
jnc 00007F576CD7B592h
imul esp, dword ptr [ecx+74h], 00006465h
and byte ptr [eax], cl
inc ecx
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
or cl, ah

Instruction
adc ah, dh
mov al, 99h
clc
adc al, byte ptr [ebp-54h]
leave
ret
jnbe 00007F576CD7B4F7h
cmpsb
add dword ptr [edi+edi*8-53h], eax
jnc 00007F576CD7B4B2h
out dx, al
pop esp
cmp cl, byte ptr [ebp-44h]
cmp al, byte ptr [edx+0134BD60h]
dec edi
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
mov dl, 00h
add byte ptr [edi+000000B0h], dh
adc dword ptr [eax], eax
push ebx
je 00007F576CD7B58Ch
jc 00007F576CD7B591h
jnc 00007F576CD7B58Eh
jne 00007F576CD7B586h
outsb
jnc 00007F576CD7B559h
add byte ptr [00000001h], cl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x11af4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x1412	.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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1ac	.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	0x11108	0x12000	False	0.4189453125	data	5.91686923553	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x13000	0xa64	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0x1412	0x2000	False	0.290649414062	data	3.29230979719	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x14d4a	0x6c8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x143c2	0x988	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0x143a0	0x22	data		
RT_VERSION	0x14120	0x280	data	Guarani	Paraguay

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaAryMove, __vbaLenBstr, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, __vbaLenBstrB, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaObjVar, DllFunctionCall, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaDateVar, _CIlog, __vbaFileOpen, __vbaNew2, __vbaInStr, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaLateMemCall, __vbaVarAdd, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, __vbaUI1Str, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0474 0x04b0
InternalName	Aflytter2
FileVersion	3.03
CompanyName	Panasonic
Comments	Panasonic
ProductName	Panasonic
ProductVersion	3.03
FileDescription	Panasonic
OriginalFilename	Aflytter2.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Guarani	Paraguay	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Aflytter2.exe PID: 7120 Parent PID: 6048

General

Start time:	15:38:02
Start date:	31/03/2021
Path:	C:\Users\user\Desktop\Aflytter2.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Aflytter2.exe'
Imagebase:	0x400000
File size:	90112 bytes
MD5 hash:	327BDD165C67A077606D414D038ECDA9
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