ID: 395503
Sample Name: VENTANASBRISA SL, COMPROBANTE DE TRANSFERENCIA PENDIENTE DE PAGO.exe
Cookbook: default.jbs
Time: 15:54:49
Date: 22/04/2021
Version: 31.0.0 Emerald

Table of Contents

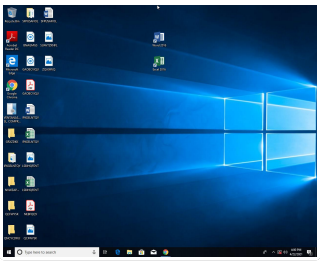
Analysis Report VENTANASBRISA SL, COMPROBANTE…

Overview

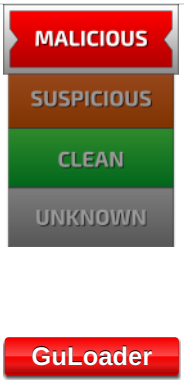
General Information

Sample Name:	VENTANASBRISA SL, COMPROBANTE DE TRANSFERENCIA PENDIENTE DE PAGO.exe
Analysis ID:	395503
MD5:	b1b0e80b7df8ae6.
SHA1:	53c2f6377d7cc97.
SHA256:	ec455e6dcab1f95.
Infos:	

Most interesting Screenshot:



Detection



Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Tries to detect virtualization through…
- PE file contains an invalid checksum
- PE file contains strange resources
- Program does not show much activi…
- Sample file is different than original …
- Uses 32bit PE files
- Uses code obfuscation techniques (…

Classification

Startup

- **System is w10x64**
- VENTANASBRISA SL, COMPROBANTE DE TRANSFERENCIA PENDIENTE DE PAGO.exe (PID: 5476 cmdline: 'C:\Users\user\Desktop\VENTANASBRISA SL, COMPROBANTE DE TRANSFERENCIA PENDIENTE DE PAGO.exe' MD5: B1B0E80B7DF8AE67ED83E366F46B265B)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1eFQiCYQnU0gxJtdFGliDTfHvfIG3lmKt",
  "Injection Process": [
    "RegAsm.exe",
    "RegSvcs.exe",
    "MSBuild.exe"
  ]
}
```


Yara Overview

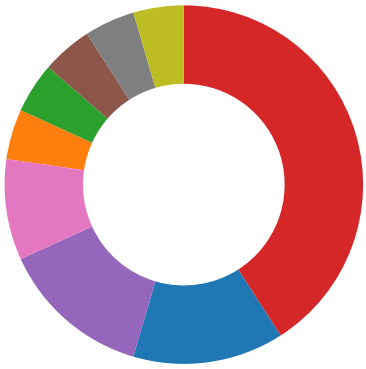
Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.810709106.0000000000580000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

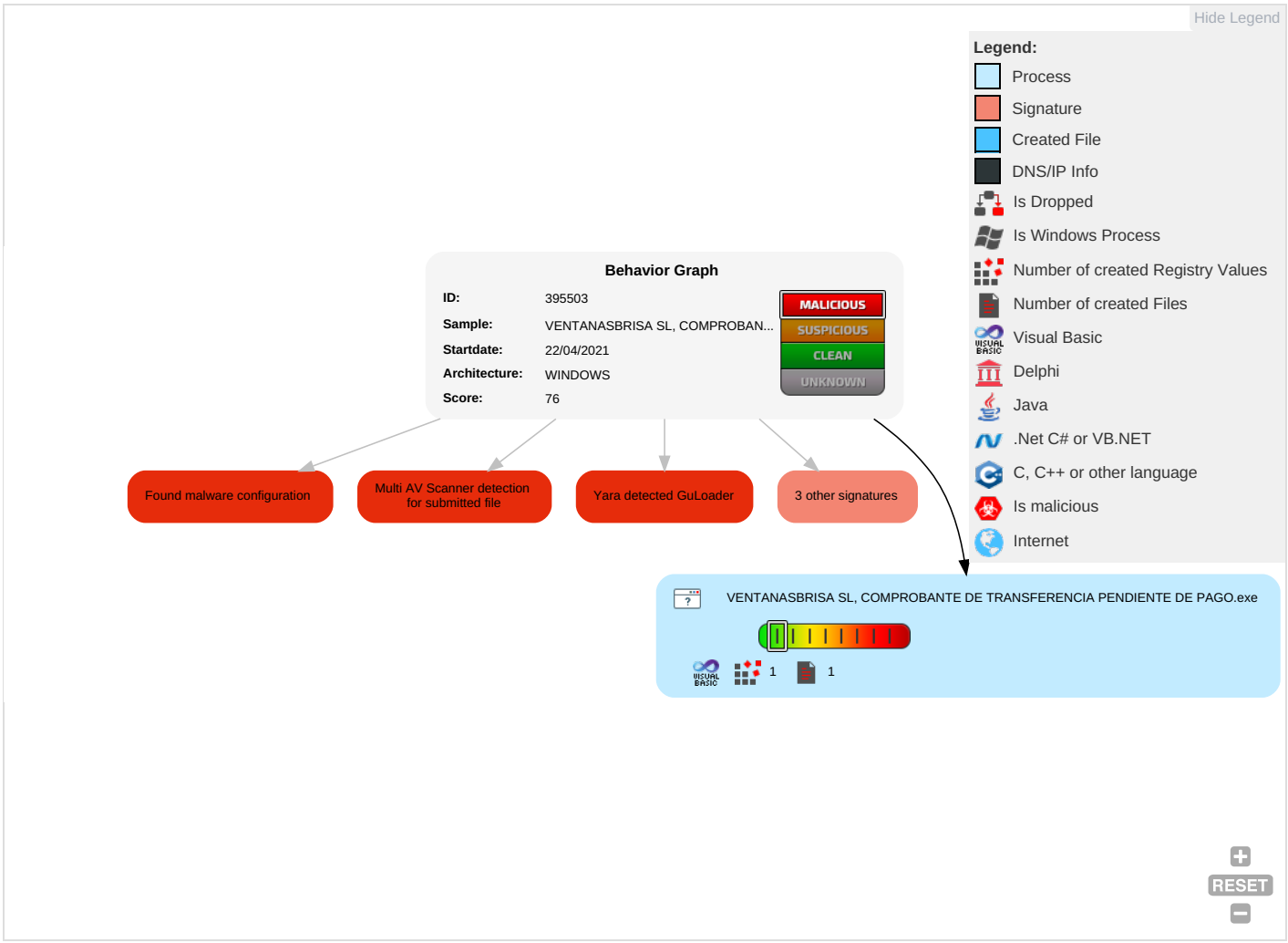
Malware Analysis System Evasion:

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	In
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Process Injection 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
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	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 1 1	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

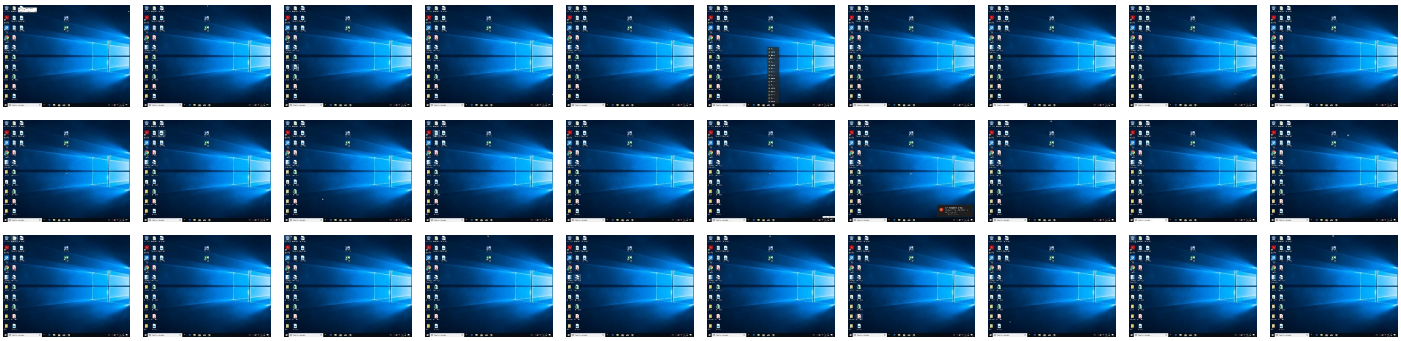
Behavior Graph



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
VENTANASBRISA SL, COMPROBANTE DE TRANSFERENCIA PENDIENTE DE PAGO.exe	21%	Virustotal		Browse
VENTANASBRISA SL, COMPROBANTE DE TRANSFERENCIA PENDIENTE DE PAGO.exe	19%	ReversingLabs		
VENTANASBRISA SL, COMPROBANTE DE TRANSFERENCIA PENDIENTE DE PAGO.exe	100%	Joe Sandbox ML		

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:	395503
Start date:	22.04.2021
Start time:	15:54:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VENTANASBRISA SL, COMPROBANTE DE TRANSFERENCIA PENDIENTE DE PAGO.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:	28
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:	mal76.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 84.7% (good quality ratio 51.2%) • Quality average: 37.5% • Quality standard deviation: 33.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.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):	5.862205071482885
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:	VENTANASBRISA SL, COMPROBANTE DE TRANSFERENCIA PENDIENTE DE PAGO.exe
File size:	155648
MD5:	b1b0e80b7df8ae67ed83e366f46b265b
SHA1:	53c2f6377d7cc97ccb2c718eeabbf16e00830656
SHA256:	ec455e6dcab1f953bd685bc9674dbe7e2fbf7afcbef4d731edd9a818048f2227
SHA512:	e7262d9270796a6b815d6fd405b8b02db85b16531d1aa510a4976fa163722930f5006449d48d37ac57788bba0b218d2d26fa23917088dc6008a987f3f98688f7
SSDEEP:	3072:jLPrJP47wFh/t9iQ2rSjVffNeYWf7M/v3w:jJP47CRzdxNfv3
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...n.yW.....`.....x.....@.....

File Icon

Icon Hash:	dadadadaeeced8da

Static PE Info

General

Entrypoint:	0x401c78
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:	0x5779156E [Sun Jul 3 13:38:54 2016 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:	1fa6aac839727b3340226df771ac8ef4

Entrypoint Preview

Instruction
push 0040FCB0h
call 00007F45D4F74625h
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 [edx], bl
sti
clc
mov dword ptr [bx], edx
jbe 00007F45D4F74678h
mov bh, 7Bh
ret
and byte ptr [esi], dl
retf 0000h
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
push ebp
push 6F6D7261h
outsb
imul esp, dword ptr [ebp+72h], 0000656Eh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
dec esp
xor dword ptr [eax], eax
push cs
sbb dh, bl
call far 9F42h : 1AEE2F58h
leave
xlatb
pop ds
fadd qword ptr [edi+584300E6h]
jc 00007F45D4F745CAh
xor al, D8h
push edi
inc edx
xchg eax, esi
and ecx, dword ptr [ebx-40B64F1Ch]
enter 4F3Ah, ADh
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x206b4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x23000	0x3916	.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	0x174	.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1fcf4	0x20000	False	0.36799621582	data	6.10209072911	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x21000	0x1254	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x23000	0x3916	0x4000	False	0.354858398438	data	5.2522569983	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x252ee	0x1628	dBase IV DBT of \200.DBF, blocks size 0, block length 4608, next free block index 40, next free block 4294901758, next used block 4294901758		
RT_ICON	0x24246	0x10a8	data		
RT_ICON	0x238be	0x988	data		
RT_ICON	0x23456	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x23418	0x3e	data		
RT_VERSION	0x23180	0x298	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaRecAnsiToUni, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFPFix, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaAryConstruct2, __vbaObjVar, __vbaI2I4, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, __vbaRecUniToAnsi, EVENT_SINK_Release, __vbaUI1I2, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaVarErrI4, __vbaFPException, _CIlog, __vbaNew2, __vbaR8Str, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, __vbaDerefAry1, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaLateMemCall, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	Vitiations3
FileVersion	1.00
CompanyName	SoftSignal
Comments	SoftSignal
ProductName	SoftSignal
ProductVersion	1.00
FileDescription	SoftSignal
OriginalFilename	Vitiations3.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: VENTANASBRISA SL, COMPROBANTE DE TRANSFERENCIA PENDIENTE DE PAGO.exe PID: 5476 Parent PID: 5628

General

Start time:	15:55:41
Start date:	22/04/2021
Path:	C:\Users\user\Desktop\VENTANASBRISA SL, COMPROBANTE DE TRANSFERENCIA PENDIENTE DE PAGO.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\VENTANASBRISA SL, COMPROBANTE DE TRANSFERENCIA PENDIENTE DE PAGO.exe'
Imagebase:	0x7ff724940000
File size:	155648 bytes
MD5 hash:	B1B0E80B7DF8AE67ED83E366F46B265B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000000.00000002.810709106.0000000000580000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis