

JOeSandbox Cloud BASIC



ID: 356153

Sample Name: cigar.exe

Cookbook: default.jbs

Time: 16:54:40

Date: 22/02/2021

Version: 31.0.0 Emerald

Table of Contents

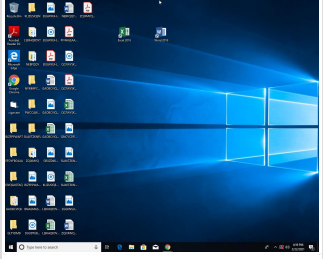
Table of Contents	2
Analysis Report cigar.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Memory Dumps	4
Sigma Overview	4
Signature Overview	4
AV Detection:	5
Compliance:	5
System Summary:	5
Data Obfuscation:	5
Malware Analysis System 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	8
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	10
Sections	11
Resources	11
Imports	11
Version Infos	11
Possible Origin	11
Network Behavior	11
Code Manipulations	11
Statistics	12

System Behavior	12
Analysis Process: cigar.exe PID: 6472 Parent PID: 5684	12
General	12
File Activities	12
Disassembly	12
Code Analysis	12

Analysis Report cigar.exe

Overview

General Information

Sample Name:	cigar.exe
Analysis ID:	356153
MD5:	57261d6b5337c8..
SHA1:	9f2855adb0a71a6.
SHA256:	ee41c208f648cc4..
Most interesting Screenshot:	
	

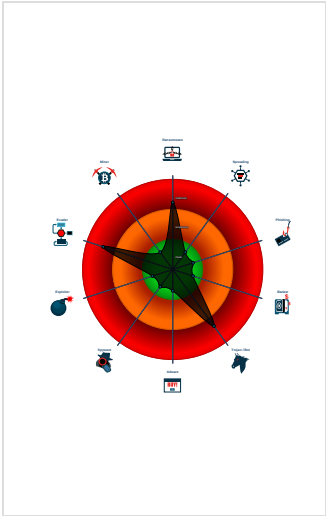
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN GuLoader	
Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm...
Potential malicious icon found
Yara detected GuLoader
Contains functionality to detect hard...
Detected RDTSC dummy instruction...
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 read the PEB
PE file contains strange resources

Classification



Startup

- System is w10x64
-  **cigar.exe** (PID: 6472 cmdline: 'C:\Users\user\Desktop\cigar.exe' MD5: 57261D6B5337C8D9F838617F2EFD6C19)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

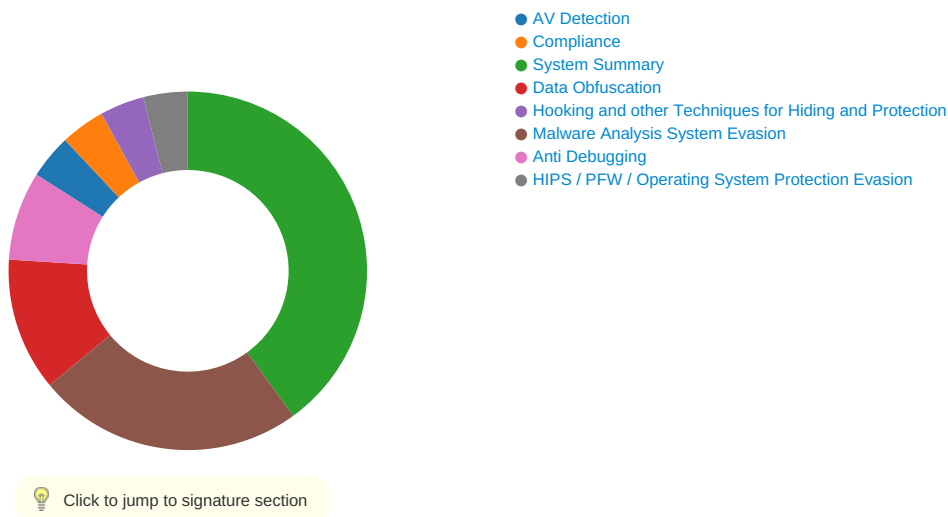
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: cigar.exe PID: 6472	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: cigar.exe PID: 6472	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



AV Detection:



Multi AV Scanner detection for submitted file

Compliance:



Uses 32bit PE files

System Summary:



Potential malicious icon found

Data Obfuscation:



Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:



Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

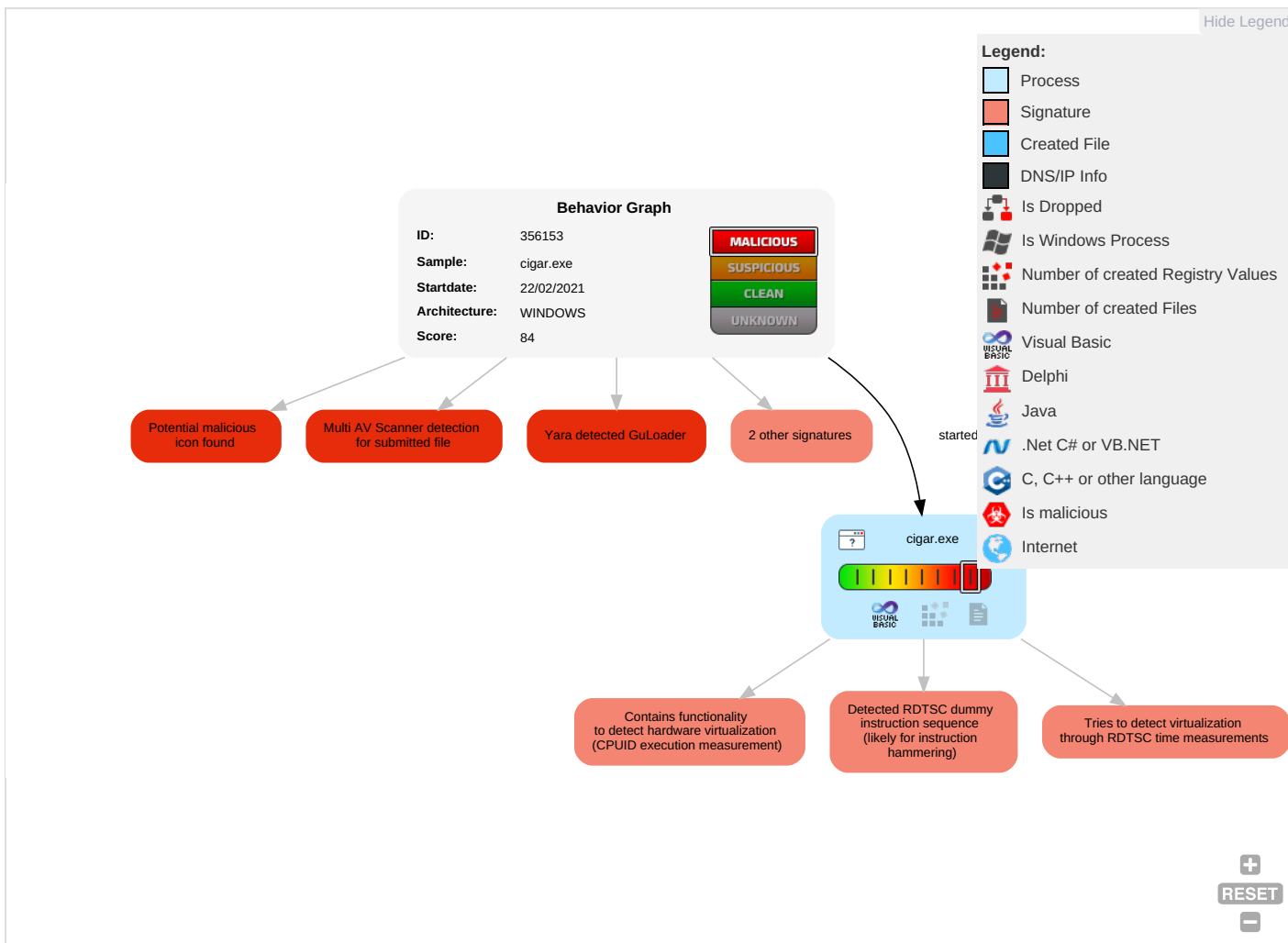
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Process Injection 1	OS Credential Dumping	Security Software Discovery 4 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

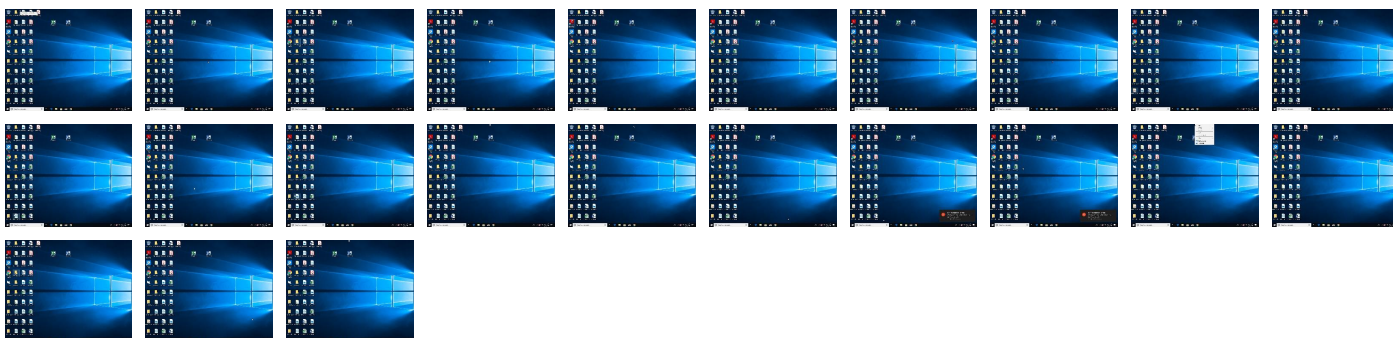
Behavior Graph



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
cigar.exe	22%	Virustotal		Browse
cigar.exe	11%	Metadefender		Browse
cigar.exe	17%	ReversingLabs	Win32.Trojan.Vebzenpak	

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:	356153
Start date:	22.02.2021
Start time:	16:54:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cigar.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:	29
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:	mal84.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 38.9% (good quality ratio 29%) • Quality average: 42.6% • Quality standard deviation: 33.1%
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): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, Usoclient.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):	4.943112440364119
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:	cigar.exe
File size:	61440
MD5:	57261d6b5337c8d9f838617f2efd6c19
SHA1:	9f285adb0a71a6079bcbe73438e1212b51f0bed
SHA256:	ee41c208f648cc461bf54a5d9e40040a25e51ebde8e9721937ca152d964bb10f
SHA512:	a78e7cea98c8c47e05769beabfa0e75446ca04436ce24855a472fcd1359bb73a11c0e7e42b611c291a9f61e1736fc3a5b7e9d445209b2bf614389defd11efb4f
SSDEEP:	768:aZMuALMxEZYqNxh5Ran9a+Kge1eulY1Eu8cohd628fN6:fHCjqNj5Ral2l6Rdo
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....N.Y.....0.....@.....

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4012c4
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:	0x591E4E86 [Fri May 19 01:46:46 2017 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:	f8fb5be8a6ea86fb9d04da61d8bfeb3a

Entrypoint Preview

Instruction

push 004014FCh
call 00007FFBD87830B3h
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 ch, bh
push es
mov edi, dword ptr [ecx+4D59FBEEh]
test bl, bl
int3
dec ebp
xlatb

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc444	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf000	0x994	.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	0xd0	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xb818	0xc000	False	0.468892415365	data	5.67760393294	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xd000	0x118c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xf000	0x994	0x1000	False	0.17822265625	data	2.07916773939	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xf864	0x130	data		
RT_ICON	0xf57c	0x2e8	data		
RT_ICON	0xf454	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xf424	0x30	data		
RT_VERSION	0xf150	0x2d4	data	Hungarian	Hungary

Imports

DLL	Import
MSVBVM60.DLL	_CltCos, _adj_fptan, __vbaVarMove, __vbaAryMove, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CltSin, __vbaChkstk, EVENT_SINK_AddRef, _adj_fptan, EVENT_SINK_Release, _CltSqrt, EVENT_SINK_QueryInterface, __vbaExceptionHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CltLog, __vbaErrorOverflow, __vbaNew2, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaVarDup, _Cltatan, __vbaCastObj, _allmul, _Cltan, _Cltexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x040e 0x04b0
LegalCopyright	Copyright (C) AC
InternalName	cigar
FileVersion	1.00
CompanyName	AC
LegalTrademarks	Copyright (C) AC
Comments	AC
ProductName	AC
ProductVersion	1.00
FileDescription	AC
OriginalFilename	cigar.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Hungarian	Hungary	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: cigar.exe PID: 6472 Parent PID: 5684

General

Start time:	16:55:20
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\cigar.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\cigar.exe'
Imagebase:	0x400000
File size:	61440 bytes
MD5 hash:	57261D6B5337C8D9F838617F2EFD6C19
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Disassembly

Code Analysis