ID: 383467
Sample Name: documentos.exe
Cookbook: default.jbs
Time: 20:37:41
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

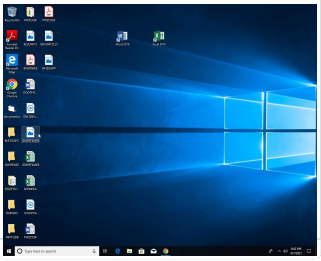
Analysis Report documentos.exe

Overview

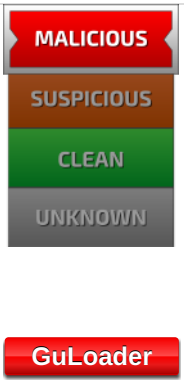
General Information

Sample Name:	documentos.exe
Analysis ID:	383467
MD5:	71d102249808e4..
SHA1:	b0538afec6fe730..
SHA256:	1b1622ce9c633a..
Infos:	

Most interesting Screenshot:



Detection

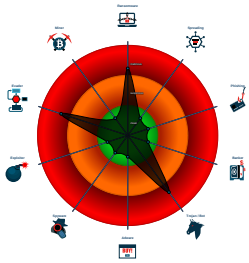


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- Executable has a suspicious name (…
- Found potential dummy code loops (…
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Detected potential crypto function
- Found large amount of non-executed…

Classification



Startup

- **System is w10x64**
- documentos.exe (PID: 7124 cmdline: 'C:\Users\user\Desktop\documentos.exe' MD5: 71D102249808E46DE207BA5D1E1441EE)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

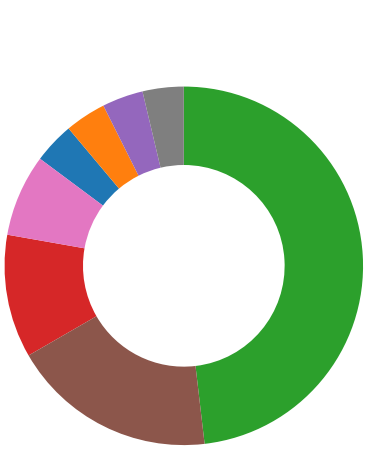
Source	Rule	Description	Author	Strings
Process Memory Space: documentos.exe PID: 7124	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: documentos.exe PID: 7124	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

System Summary:

Potential malicious icon found

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

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:

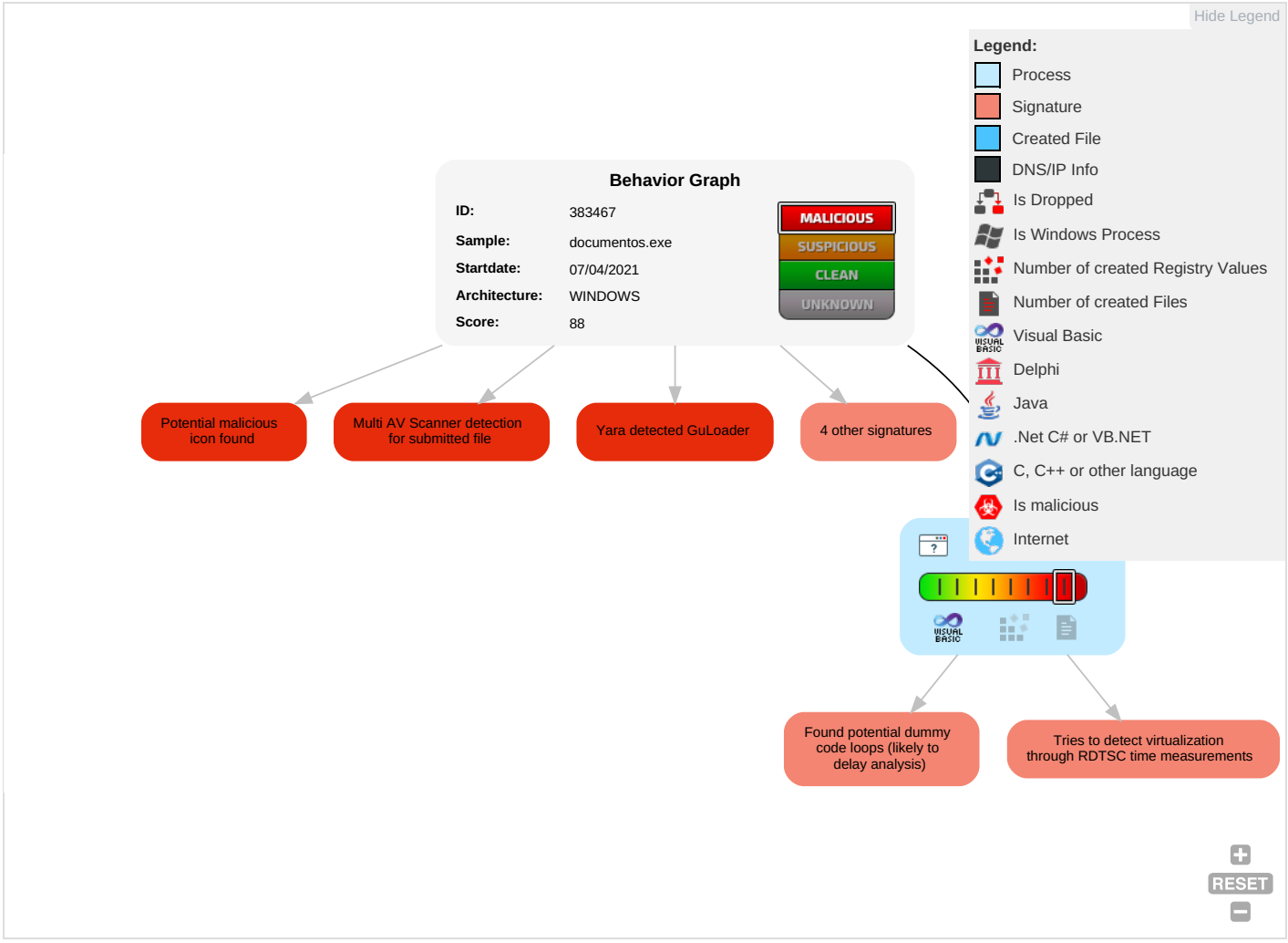
Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
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	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
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	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Copyright Joe Security LLC 2021

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
documentos.exe	32%	Virustotal		Browse
documentos.exe	10%	ReversingLabs	Win32.Backdoor.Remcos	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2021

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:	383467
Start date:	07.04.2021
Start time:	20:37:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	documentos.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:	15
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.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 11.1% (good quality ratio 9.8%) • Quality average: 52.1% • Quality standard deviation: 22.9%
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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe

Simulations

Behavior and APIs

No simulations

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):	5.800179475931607
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:	documentos.exe
File size:	155648
MD5:	71d102249808e46de207ba5d1e1441ee
SHA1:	b0538afec6fe730a0e01b8fd81febf68e03d2f54
SHA256:	1b1622ce9c633a2c53dac43aaea43712544b7385d457b05574d4754cf850293c
SHA512:	27a3229760a9d5a2f8324ea094daa9be596ce8fb576c2f592c2d67df7c8843268fe2edbd571bea5fda30dcfacbdfb4ef0d808cc213c75d31f03a25710180b386
SSDEEP:	1536:/siCE7hAX1SvRtlo02gPS2QY4qNw+6dbg3Oad/HfGRXuNbNnvwD7IoG5QzI6mUQp:UpE7yXetag2xhZzd/HfiYZnvmzLRQpz
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....hm`.....0...0.....d.....@....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401564
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:	0x606D688C [Wed Apr 7 08:08:44 2021 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:	545536ea1fbc91386e1294093d2f717e

Entrypoint Preview

Instruction
push 00401740h
call 00007FB684A89825h
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 bh, dh
popad
pushfd
jns 00007FB684A8986Bh
fistp word ptr [eax+4Dh]
movsb
or eax, dword ptr [eax+3Ch]
pushad
fbstp [esi+000000BCh]
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+64h], ah
adc dword ptr [ebx], eax
jnc 00007FB684A898A6h
jc 00007FB684A89893h
outsb
jnc 00007FB684A8989Eh
popad
add byte ptr fs:[eax], ah
or byte ptr [ecx+00h], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp

Instruction
xor dword ptr [eax], eax
add eax, 59164BAAh
mov bh, byte ptr [edx+edx*2-4AC754B9h]
mov word ptr [ebp+35h], cs
push ds
rcr dword ptr [eax-17h], 7Dh
and bh, byte ptr [ebx-7DB36973h]
jne 00007FB684A8984Fh
fadd dword ptr [eax+3A978C9Fh]
dec edi
lodsd
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
sub eax, dword ptr [ecx]
add byte ptr [eax], al
push eax
add byte ptr [eax], al
add byte ptr [eax], al
push cs
add byte ptr [ebx+6Fh], cl
outsb
jbe 00007FB684A89897h
outsb
je 00007FB684A8989Bh
outsd
outsb
insb
insb
add byte ptr [53000A01h], cl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x23834	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26000	0x9d8	.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	

Copyright Joe Security LLC 2021

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	0x17c	.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	0x22e04	0x23000	False	0.348597935268	data	6.03854398613	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x24000	0x1194	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x26000	0x9d8	0x1000	False	0.179443359375	data	2.13350863125	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x268a8	0x130	data		
RT_ICON	0x265c0	0x2e8	data		
RT_ICON	0x26498	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x26468	0x30	data		
RT_VERSION	0x26150	0x318	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaI2I4, __vbaObjVar, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, EVENT_SINK_Release, __vbaUI1I2, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaI2Str, __vbaVarErrI4, __vbaFPException, __vbaInStrVar, __vbaStrVarVal, _CIlog, __vbaErrorOverflow, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, __vbaDerefAry1, _adj_fdivr_m32, _adj_fdiv_r, __vbaI4Var, __vbaVarAdd, __vbaLateMemCall, __vbaVarDup, __vbaFpI4, _CIatan, __vbaUI1Str, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0404 0x04b0
LegalCopyright	Collutions
InternalName	Outpiped
FileVersion	1.00
CompanyName	Collutions
LegalTrademarks	Collutions
Comments	Collutions
ProductName	Collutions
ProductVersion	1.00
FileDescription	Creepy Collutions
OriginalFilename	Outpiped.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: documentos.exe PID: 7124 Parent PID: 5908

General

Start time:	20:38:26
Start date:	07/04/2021
Path:	C:\Users\user\Desktop\documentos.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\documentos.exe'
Imagebase:	0x400000
File size:	155648 bytes
MD5 hash:	71D102249808E46DE207BA5D1E1441EE
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