ID: 791298
Sample Name: file.exe
Cookbook: default.jbs
Time: 09:51:07
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

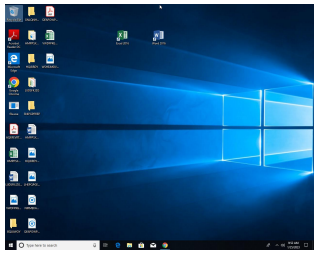
Windows Analysis Report

file.exe

Overview

General Information

Sample Name:	file.exe
Analysis ID:	791298
MD5:	3fd36473a356b2..
SHA1:	711acfd53e4d3f4..
SHA256:	bf36f4fdd2382cc…
Tags:	exe



Errors

- No process behavior to analyse as no analysis process or sample was found
- Corrupt sample or wrongly selected analyser. Details: 000000a4

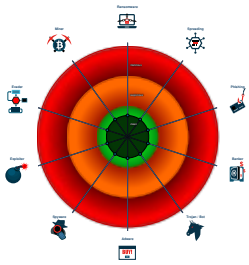
Detection

Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- PE file overlay found
- Uses 32bit PE files
- PE file does not import any functions
- PE file contains sections with non-s…
- PE file contains an invalid checksum

Classification



Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

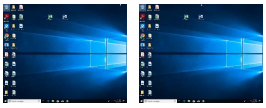
Mitre Att&ck Matrix

No Mitre Att&ck techniques found

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

No Antivirus matches

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

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	791298
Start date and time:	2023-01-25 09:51:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	0
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown2.winEXE@0/0@0/0
Cookbook Comments:	• Found application associated with file extension: .exe • Unable to launch sample, stop analysis

Errors

- No process behavior to analyse as no analysis process or sam ple was found
- Corrupt sample or wrongly sele cted analyzer. Details: C000007B

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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):	6.642103838248304
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:	file.exe
File size:	34864
MD5:	3fd36473a356b2574dee24283f6d3bf1
SHA1:	711acfd53e4d3f48896565bc4d3428fc761304cd
SHA256:	bf36f4fdd2382cc5869fd3833c42a73ab638ae73457a268713099888a7de6b00
SHA512:	6fdd039f44f2bcc0e2694593c99c28ee33f161b886d432706b30737948de005aa1cb0ea1bc4da6a046ac4bc6d7b93fb23ea9ecaa4d9ad93e8f099d8ef8318a8f
SSDEEP:	768:xhrMgpxtC4QjYVMHSe2wnqP3vj+cN6gSfN4ZuQxkbLTGdj:vJpxtC4Ulz2+w6JN4ZuQ2Ladj

TLSH:	5CF27C32FAE184B2C69B45B488B4D992BF1E251122F0D9436F6C1A7A5F317D2837731B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E...+E..+E..+E...E..+E...E..+E...E..+E.3PE..+E..*E..+E...E..+E...E..+E...E..+ERich..+E.....PE..L.....b.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40453f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x62E31E17 [Thu Jul 28 23:39:03 2022 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:	

Entrypoint Preview

Instruction
mov dword ptr [ebp-14h], ebx
jne 00007F5EACC850CDh
mov ebx, dword ptr [ebp+08h]
mov ecx, dword ptr [ebp-14h]
and dword ptr [ebx+04h], ecx
jmp 00007F5EACC850C5h
mov ebx, dword ptr [ebp+08h]
cmp dword ptr [ebp-08h], 00000000h
mov ecx, dword ptr [edx+08h]
mov edi, dword ptr [edx+04h]
mov dword ptr [ecx+04h], edi
mov ecx, dword ptr [edx+04h]
mov edi, dword ptr [edx+08h]
mov dword ptr [ecx+08h], edi
je 00007F5EACC85153h
mov ecx, dword ptr [ebp-0Ch]
lea ecx, dword ptr [ecx+esi*8]
mov edi, dword ptr [ecx+04h]
mov dword ptr [edx+08h], ecx
mov dword ptr [edx+04h], edi
mov dword ptr [ecx+04h], edx
mov ecx, dword ptr [edx+04h]
mov dword ptr [ecx+08h], edx
mov ecx, dword ptr [edx+04h]
cmp ecx, dword ptr [edx+08h]
jne 00007F5EACC85120h
mov cl, byte ptr [esi+eax+04h]

Instruction
mov byte ptr [ebp+0Bh], cl
inc cl
cmp esi, 20h
mov byte ptr [esi+eax+04h], cl
jnl 00007F5EACC850E5h
cmp byte ptr [ebp+0Bh], 00000000h
jne 00007F5EACC850CDh
mov edi, 80000000h
mov ecx, esi
shr edi, cl
or dword ptr [ebx], edi
mov ecx, esi
mov edi, 80000000h
shr edi, cl
mov ecx, dword ptr [ebp-04h]
or dword ptr [eax+ecx*4+44h], edi
jmp 00007F5EACC850EBh
cmp byte ptr [ebp+0Bh], 00000000h
jne 00007F5EACC850CFh
lea ecx, dword ptr [esi-20h]
mov edi, 80000000h
shr edi, cl
or dword ptr [ebx+04h], edi
mov ecx, dword ptr [ebp-04h]
lea edi, dword ptr [eax+ecx*4+000000C4h]
lea ecx, dword ptr [esi-20h]
mov esi, 80000000h
shr esi, cl
or dword ptr [edi], esi
mov ecx, dword ptr [ebp-08h]
test ecx, ecx
je 00007F5EACC850CDh
mov dword ptr [edx], ecx
mov dword ptr [ecx+edx-04h], ecx
jmp 00007F5EACC850C5h
mov ecx, dword ptr [ebp-08h]
mov esi, dword ptr [ebp-10h]
add edx, ecx
lea ecx, dword ptr [esi+01h]

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10b64	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2f000	0x2b298	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5b000	0xb98	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x11d0	0x1c	.text
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	0x2de0	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x190	.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	0x104a0	0x10600	False	0.5606973995271868	data	6.7119685674250125	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x12000	0x19100	0x16e00	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.gimu	0x2c000	0x270	0x400	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ripojut	0x2d000	0x2d3	0x400	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.diva	0x2e000	0x3c3	0x400	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2f000	0x2b298	0x2b400	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5b000	0x1912	0x1a00	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

No system behavior

Disassembly

No disassembly