

JoeSandbox Cloud BASIC



ID: 528760

Sample Name: JZ3FrTU0tJ.exe

Cookbook: default.jbs

Time: 18:39:01

Date: 25/11/2021

Version: 34.0.0 Boulder Opal

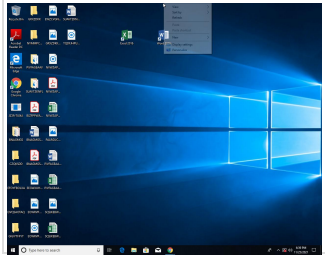
Table of Contents

Table of Contents	2
Windows Analysis Report JZ3FrTU0tJ.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Jbx Signature Overview	3
AV Detection:	3
System Summary:	3
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	4
Thumbnails	4
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	5
Domains	5
URLs	5
Domains and IPs	6
Contacted Domains	6
Contacted IPs	6
General Information	6
Simulations	6
Behavior and APIs	6
Joe Sandbox View / Context	6
IPs	6
Domains	7
ASN	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	7
Static File Info	7
General	7
File Icon	7
Static PE Info	7
General	7
Data Directories	8
Sections	8
Network Behavior	8
Code Manipulations	8
Statistics	8
System Behavior	8
Disassembly	8

Windows Analysis Report JZ3FrTU0tJ.exe

Overview

General Information

Sample Name:	JZ3FrTU0tJ.exe
Analysis ID:	528760
MD5:	57c919f3cc2729e..
SHA1:	28c18e298d8a57..
SHA256:	b6de619c946922..
Tags:	exe
Most interesting Screenshot:	
	

Errors

No process behavior to analyse as no analysis process or sample was found

Malware Configuration

Yara rule not found in the analyzer. Details: %1 is not a valid Win32 application.

No configs have been found

Detection

MALICIOUS

SUSPICIOUS

CLEAN

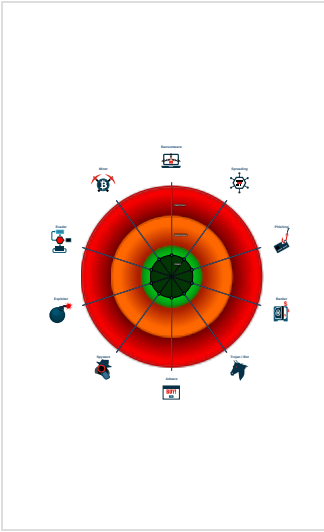
UNKNOWN

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Machine Learning detection for samp...
- PE file has nameless sections
- PE file contains section with special...
- PE file does not import any functions
- PE file overlay found
- PE file contains sections with non-s...
- Binary contains a suspicious time st...

Classification



Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

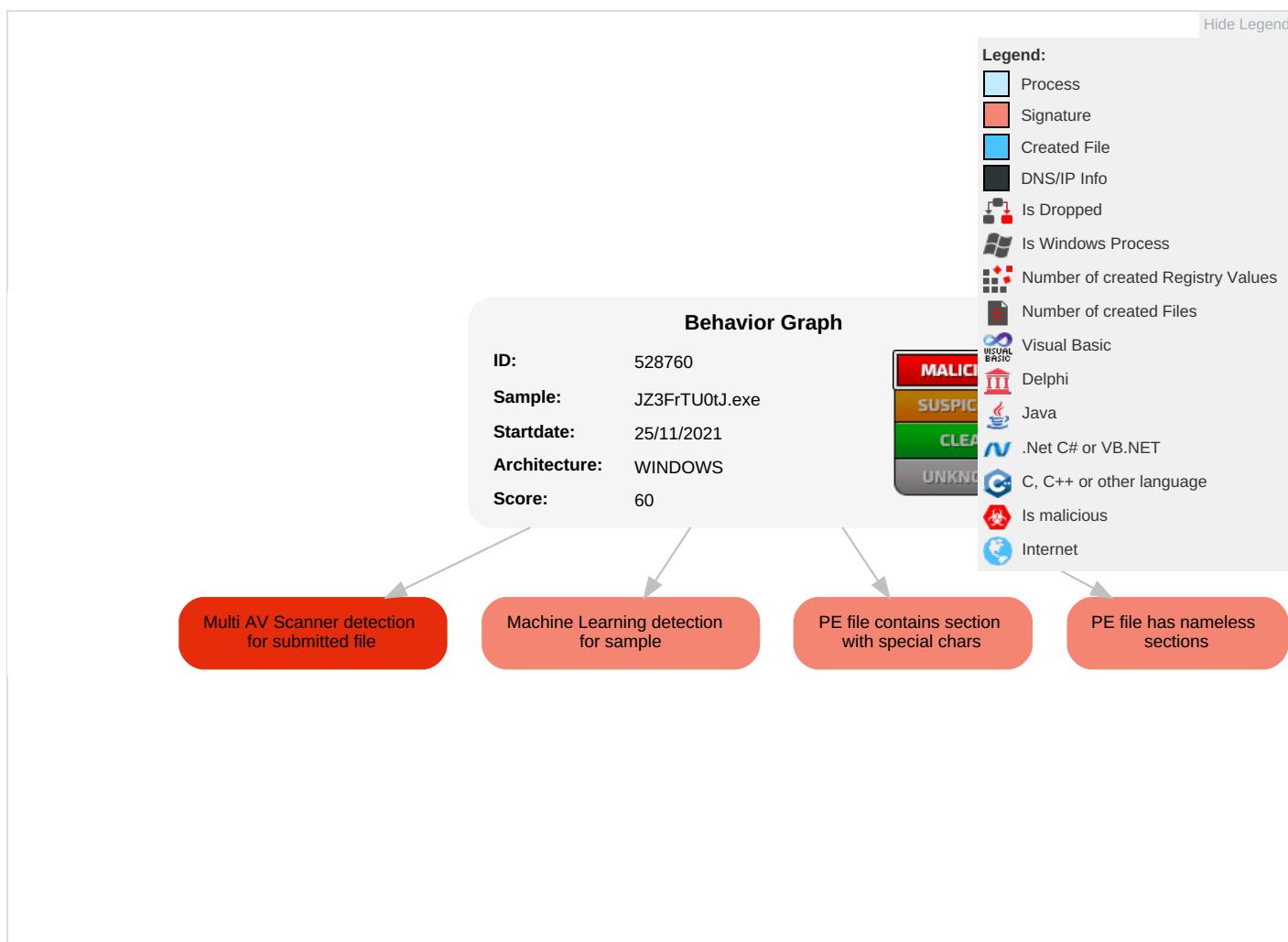
PE file has nameless sections

PE file contains section with special chars

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	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Software Packing 2	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Timestomp 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

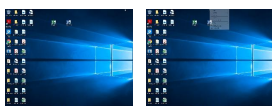
Behavior Graph



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
JZ3FrTU0tJ.exe	20%	Virustotal		Browse
JZ3FrTU0tJ.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:	34.0.0 Boulder Opal
Analysis ID:	528760
Start date:	25.11.2021
Start time:	18:39:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JZ3FrTU0tJ.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:	3
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:	<ul style="list-style-type: none">• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.winEXE@0/0@0/0
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .exe• Unable to launch sample, stop analysis
Warnings:	Show All
Errors:	<ul style="list-style-type: none">• No process behavior to analyse as no analysis process or sample was found• Corrupt sample or wrongly selected analyzer. Details: %1 is not a valid Win32 application.

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 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.062703864995128
TrID:	<ul style="list-style-type: none">Win32 Executable (generic) Net Framework (10011505/4) 50.01%Win32 Executable (generic) a (10002005/4) 49.96%Win16/32 Executable Delphi generic (2074/23) 0.01%Generic Win/DOS Executable (2004/3) 0.01%DOS Executable Generic (2002/1) 0.01%
File name:	JZ3FrTU0tJ.exe
File size:	183635
MD5:	57c919f3cc2729eef0f8cbf72aa712a9
SHA1:	28c18e298d8a579db4cbfa459c35bdde29de58ac
SHA256:	b6de619c9469226aef6d9af08b03d51e7d200d53a9acffc6adcd975e0d48e3d9
SHA512:	92833ac52b646cb0c79f1e87e5e54996a446f46442bcffd321857fc8190374d57acc74e25a53d2371be0ae2af349960182fa785b5e930003aa95e22398df1468
SSDEEP:	3072:yVaok+snqUvu3m7xAddxcrmGHlrNHjEalqIU+onEksKSm20DMxQQtYscKgoN60eZ:yVa3+sqU4/Kx6aPIU+onEksKSm20DMxG
File Content Preview:	MZ.....@.....!..!Th is program cannot be run in DOS mode....\$......PE..L...q .a....." ..0..... ..@..`..... '

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x44200a
Entrypoint Section:	

General		
Digitally signed:	false	
Imagebase:	0x400000	
Subsystem:	windows gui	
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE	
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA	
Time Stamp:	0xD261EA71 [Thu Nov 6 05:26:09 2081 UTC]	
TLS Callbacks:		
CLR (.Net) Version:	v4.0.30319	
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:		

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
[.MOak	0x2000	0xe564	0xe600	False	1.00044157609	data	7.99738998665	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0x12000	0x2c908	0x2ca00	False	0.29661927892	data	4.34882960737	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x40000	0x5d6	0x600	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x42000	0x10	0x200	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x44000	0xc	0x200	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly

