JoeSandbox Cloud BASIC

ID: 383843
Sample Name: New Text Document.exe
Cookbook: defaultandroidfilecookbook.jbs
Time: 10:58:04
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

Analysis Report New Text Document.exe

Overview

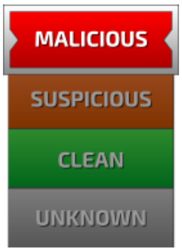
General Information

Sample Name:	New Text Document.exe
Analysis ID:	383843
MD5:	4e79b531f4f6813..
SHA1:	addcb0a2aac14b..
SHA256:	9445838c514498..

Errors

⚠ Setup command "_JBInstrumentAPK" failed: Invalid APK

Detection

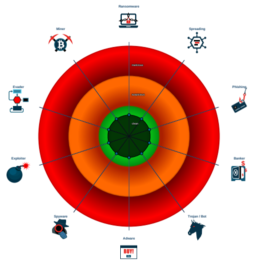


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm…

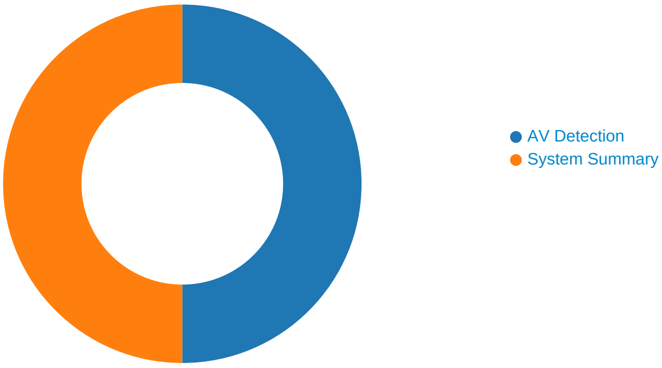
Classification



Yara Overview

No yara matches

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Mitre Att&ck Matrix

No Mitre Att&ck techniques found

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
New Text Document.exe	14%	Virustotal		Browse

Dropped 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:	383843
Start date:	08.04.2021
Start time:	10:58:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New Text Document.exe
Cookbook file name:	defaultandroidfilecookbook.jbs
Analysis system description:	Android 9 (Pie)
Analysis Mode:	default
APK Instrumentation enabled:	true
Detection:	MAL
Classification:	mal48.andEXE@0/0@0/0
Warnings:	Show All • No dynamic data available • Static analyzation failed: null
Errors:	• Setup command "_JBInstrumentAPK" failed: Invalid APK

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):	6.662141005544995
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:	New Text Document.exe
File size:	894976
MD5:	4e79b531f4f6813cc8e21894a13c5537
SHA1:	addcb0a2aac14befcb9f8c9185e365c47a86b40c
SHA256:	9445838c51449888abaeac1c5d1953212a0205a6b4038e 6a404ca752cbda3f2f
SHA512:	aae6406f2feedfbae51433a697bbaf3d7a80570c0f86a1f5f 9e09ac2699651049fbd882d27de21ede2ffa215e28ed73d 8b3a16aca003c2213ebcfe421a581cde
SSDEEP:	24576:aAHnh+eWsN3skA4RV1Hom2KXMmHahxl5:th+ZkldoPK8YahV
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........s..R...R...R....C..P.....;.S..._@#.a..._@......_@..g...[j..[...[jo.w...R...r.............#.S..._@'.S...R.k.S.....".S...RichR..

Static APK Info

General

Label:	
Version Code:	
Version Name:	
Package Name:	
Is Activity:	
Is Receiver:	

General

Is Service:	
Requests System Level Permissions:	
Play Store Compatible:	

Receivers

Permission Requested

Certificate

Name:	
Issuer:	
Subject:	

Resources

Name	Type	Size

Network Behavior

No network behavior found

APK Behavior

Installation

Miscellaneous

System Calls

By Permission (executed)

By Permission (non-executed)

Disassembly

0 Executed Methods

0 Non-Executed Methods