

JoeSandbox Cloud BASIC



ID: 383843

Sample Name: New Text

Document.exe

Cookbook:

defaultandroidfilecookbook.jbs

Time: 10:59:37

Date: 08/04/2021

Version: 31.0.0 Emerald


Table of Contents

Table of Contents	2
Analysis Report New Text Document.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Yara Overview	3
Signature Overview	3
AV Detection:	3
Mitre Att&ck Matrix	3
Antivirus, Machine Learning and Genetic Malware Detection	4
Initial Sample	4
Dropped Files	4
Domains	4
URLs	4
Domains and IPs	4
Contacted Domains	4
Contacted IPs	4
Public	5
General Information	5
Joe Sandbox View / Context	5
IPs	6
Domains	6
ASN	6
JA3 Fingerprints	6
Dropped Files	6
Created / dropped Files	6
Static File Info	6
General	6
Static APK Info	6
General	6
Receivers	7
Permission Requested	7
Certificate	7
Resources	7
Network Behavior	7
TCP Packets	7
APK Behavior	7
Installation	7
Miscellaneous	7
System Calls	7
By Permission (executed)	7
By Permission (non-executed)	7
Disassembly	7
0 Executed Methods	7
0 Non-Executed Methods	8


Analysis Report New Text Document.exe

Overview

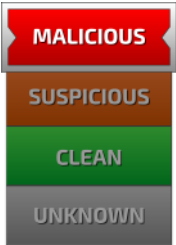
General Information

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

Errors

 Setup command "_JBInstrumentAPK" failed: Invalid APK

Detection

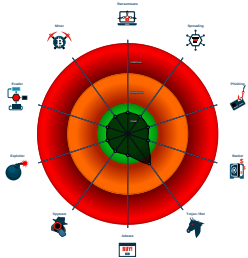


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Tries to connect to HTTP servers, b...

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

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	Direct Volume Access	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	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	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

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



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.163	unknown	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383843
Start date:	08.04.2021
Start time:	10:59:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 0m 38s
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)
Run name:	No behavior, retry without instrumentation
Analysis Mode:	default
APK Instrumentation enabled:	false
Detection:	MAL
Classification:	mal48.andEXE@0/0@0/0
Warnings:	Show All <ul style="list-style-type: none"> No dynamic data available Static analyzation failed: null
Errors:	<ul style="list-style-type: none"> Setup command "_JBInstrumentAPK" failed: Invalid APK

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:	<ul style="list-style-type: none">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:	9445838c51449888abaeac1c5d1953212a0205a6b4038e6a404ca752cbda3f2f
SHA512:	aae6406f2feedfbae51433a697bbaf3d7a80570c0f86a1f5f9e09ac2699651049fbd882d27de21ede2ffa215e28ed73d8b3a16aca003c2213ebcfe421a581cde
SSDEEP:	24576:aAHnh+eWsN3skA4RV1Hom2KXMmHahxI5:th+ZkldoPK8YahV
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode...\$.....s..R...R...R....C..P.....;S..._@#.a..._@....._@..g...[.]...[jo.w...R...f.....#..S..._@'.S...R.k.S.....".S...RichR..

Static APK Info

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

General

Is Receiver:

Is Service:

Requests System Level Permissions:

Play Store Compatible:

Receivers

Permission Requested

Certificate

Name:

Issuer:

Subject:

Resources

Name

Type

Size

Network Behavior

TCP Packets

Timestamp

Source Port

Dest Port

Source IP

Dest IP

Apr 8, 2021 10:59:54.121563911 CEST

39602

443

192.168.2.30

142.250.186.163

APK Behavior

Installation

Miscellaneous

System Calls

By Permission (executed)

By Permission (non-executed)

Disassembly

0 Executed Methods

