ID: 358575
Sample Name: a11256078 (1).TIF
Cookbook: default.jbs
Time: 21:28:07
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

Analysis Report a11256078 (1).TIF

Overview

General Information

Sample Name:	a11256078 (1).TIF
Analysis ID:	358575
MD5:	ca9fb7fe10246c3..
SHA1:	4c305aa67e3615..
SHA256:	a4a531d12b3888..

Errors

- Nothing to analyse, Joe Sandbox has not found any analysis process or sample
- Corrupt sample or wrongly selected analyzer. Details: 80040153

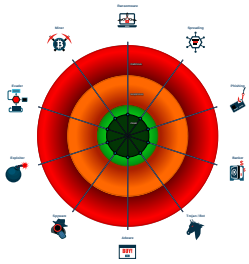
Detection

Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Malware Configuration

No configs have been found

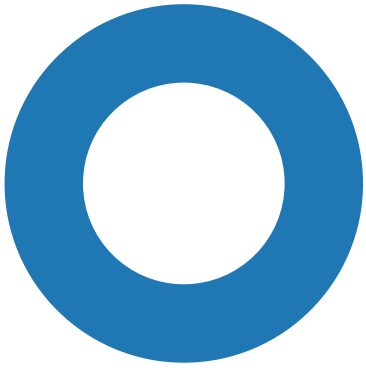
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



● System Summary

Click to jump to signature section

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

Mitre Att&ck Matrix

No Mitre Att&ck techniques found

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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358575
Start date:	25.02.2021
Start time:	21:28:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 25s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	a11256078 (1).TIF
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:	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:	unknown0.winTIF@0/0@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .TIF • Unable to launch sample, stop analysis
Errors:	• Nothing to analyse, Joe Sandbox has not found any analysis process or sample • Corrupt sample or wrongly selected analyzer. Details: 80040153

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:	TIFF image data, little-endian, direntries=15, height=637, bps=55942, compression=LZW, PhotometricInterpretation=RGB, width=778
Entropy (8bit):	7.953376461538839
TrID:	• Tagged Image File Format Bitmap (little endian) (4004/1) 100.00%
File name:	a11256078 (1).TIF
File size:	188230
MD5:	ca9fb7fe10246c36bdcaceefee879b6b
SHA1:	4c305aa67e3615c2289c860d6933f6a6c50bc012
SHA256:	a4a531d12b3888152968fc8e374a9dff71fa4a8e020b1f160fa9de0b940b2d2b
SHA512:	485d324498189ede95b10e5bc599bdb0b739455fb04ce66fb4709fb4ccc1fe6fda5228f14ce1c3c96dc50c04e927183de7adf0c2875e8812e653f02ab46288d1
SSDEEP:	3072:OgzzHf6RAKt1Iia67HvnwYqP2XMwfjnNmA+N3s+FvzNEdxVgewfMK:JzHfWA61IlcXZcINm1N3siOdxVgew
File Content Preview:	II*.....?.P8$....BaP.d6...DbQ8.V-..FcQ..v=..HdR9$.M'.JeR.d.]/.LfS9..m7.NgS...}?.PhT:%..G.RiT.e6.O.TjU:.V.W.VkU..v._.XlV;%..g.ZmV.e..o.\nW;...w.^oW.....`pX<&....bqX.f7...drY<.W-..J. .?.P8$....BaP.d6...DbQ8.V-..FcQ..v=..HdR9$.M'.JeR.d.]/.LfS9..m7.NgS...}?

File Icon

Icon Hash:	208e869a8ab2ae00

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly