ID: 321443
Sample Name: images
Cookbook: default.jbs
Time: 06:39:43
Date: 22/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

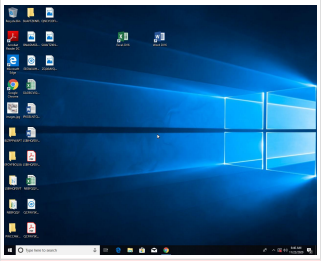
Analysis Report images

Overview

General Information

Sample Name:	images (renamed file extension from none to jpg)
Analysis ID:	321443
MD5:	59970734c2ced5..
SHA1:	ad77f5553c948d7.
SHA256:	470f7d73791524b.

Most interesting Screenshot:



Errors

Nothing to analyse, Joe Sandbox has not found any analysis process or sample

Corrupt sample or wrongly selected analyzer. Details: 80040153

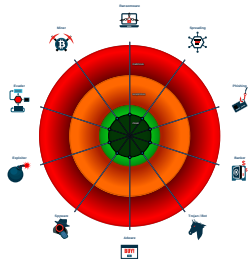
Detection

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

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

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
images.jpg	0%	Virustotal		Browse
images.jpg	0%	ReversingLabs		

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 Red Diamond
Analysis ID:	321443
Start date:	22.11.2020
Start time:	06:39:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	images (renamed file extension from none to jpg)
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:	4
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.winJPG@0/0@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Unable to launch sample, stop analysis
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe
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:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 225x225, frames 3
Entropy (8bit):	7.92304031672807

General

TrID:	• JFIF JPEG Bitmap (4007/3) 50.02% • JPEG Bitmap (3003/1) 37.49% • MP3 audio (1001/1) 12.50%
File name:	images.jpg
File size:	10481
MD5:	59970734c2ced5d8c23907174bf6d08a
SHA1:	ad77f5553c948d77b4a8eb5ca943e1daa13a9272
SHA256:	470f7d73791524b0bd8a33ea2b6619c9d33ed570dc1e2ee0e1490de90ea36897
SHA512:	4e077fe74dee33099fc3bcf444bd6375029e9071b6ffcb8545f15cd2de19c6c334e6bcc93d79dd4a53c855ce614c97a81b484f5a072f952e4d28f3b8db91acfc
SSDEEP:	192:MH+VPXmNy7umPAeY1OoCjYZ70tKDavyWoVSUwhWPQU2PpINV+731t4FppteZ2RJt:MEX3imPAeloCjYB0MUyWYS3AgB+c73cf
File Content Preview:	......JFIF..... ....W....."#3.2BC.RScrs.... .$b.

File Icon

Icon Hash:	74f0f0e4c6d6e0e4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly