ID: 340788
Sample Name:
cqgquljtt8hkzl699g+8uk8zkt4yecmycehqq96cnsljriimoqojtkgy=
Cookbook: default.jbs
Time: 09:50:22
Date: 18/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report cqgquljtt8hkzl699g+8uk8zkt4yecmyceh…

Overview

General Information

Sample Name:	cqgquljtt8hkzl699g+8uk8zkt4yecmycehqq96cnsljriimoqojtkgy=
Analysis ID:	340788
MD5:	4842e206e4cfff2…
SHA1:	80c9820ff2efe8a…
SHA256:	2acab1228e8935..

Errors

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

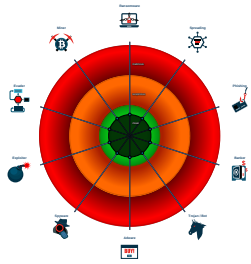
Detection

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

Signatures

No high impact signatures.

Classification



Malware Configuration

No configs have been found

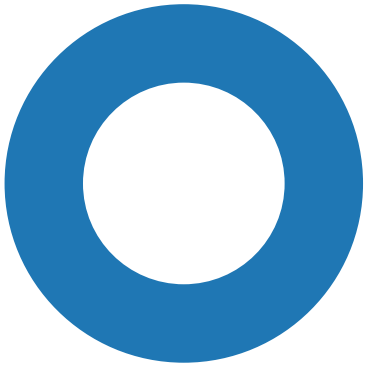
Yara Overview

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

Source	Detection	Scanner	Label	Link
cqgquljtt8hkzl699g+8uk8zkt4yecmycehqq96cnsljriimoqojtkgy=	0%	Virustotal		Browse
cqgquljtt8hkzl699g+8uk8zkt4yecmycehqq96cnsljriimoqojtkgy=	0%	Metadefender		Browse
cqgquljtt8hkzl699g+8uk8zkt4yecmycehqq96cnsljriimoqojtkgy=	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:	340788
Start date:	18.01.2021
Start time:	09:50:22

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cqgquljtt8hkzl699g+8uk8zkt4yecmycehqq96cnsljriimoqojtkgy=
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:	2
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.win@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): BackgroundTransferHost.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:	data
Entropy (8bit):	1.9219280948873623
TrID:	
File name:	cqgquljtt8hkzl699g+8uk8zkt4yecmycehqq96cnsljriimoqojtkgy=
File size:	5
MD5:	4842e206e4cfff2954901467ad54169e
SHA1:	80c9820ff2efe8aa3d361df7011ae6eee35ec4f0
SHA256:	2acab1228e8935d5dfdd1756b8a19698b6c8b786c90f8793ce9799a67a96e4e
SHA512:	ff537b1808fcb03cfb52f768fbd7e7bd66baf6a8558ee5b8f2a02f629e021aa88a1df7a8750bae1f04f3b9d86da56f0bdcba2fdbc81d366da6c97eb76ecb6cba
SSDEEP:	3:w:w
File Content Preview:	0....

File Icon

Icon Hash:	74f0e4e4e4e4e0e4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly