

JoeSandbox Cloud BASIC



ID: 487492

Sample Name: Canadian TV ad
for Covid testing.mp4

Cookbook: default.jbs

Time: 18:00:52

Date: 21/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report Canadian TV ad for Covid testing.mp4	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Jbx Signature Overview	3
Mitre Att&ck Matrix	4
Screenshots	4
Thumbnails	4
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	5
Domains	5
URLs	5
Domains and IPs	5
Contacted Domains	5
Contacted IPs	5
General Information	5
Simulations	6
Behavior and APIs	6
Joe Sandbox View / Context	6
IPs	6
Domains	6
ASN	6
JA3 Fingerprints	6
Dropped Files	6
Created / dropped Files	6
Static File Info	6
General	6
File Icon	7
Network Behavior	7
Code Manipulations	7
Statistics	7
System Behavior	7
Disassembly	7

Windows Analysis Report Canadian TV ad for Covid tes...

Overview

General Information

Sample Name:

Canadian TV ad for Covid testing.mp4

Analysis ID:

487492

MD5:

19f79239cc58af3...

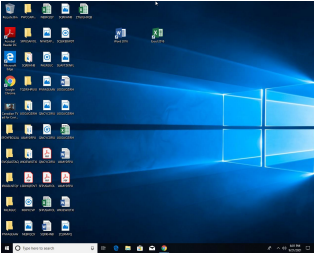
SHA1:

73cfc069af3aeec...


SHA256:


77c1f85e3fc64cc...

Most interesting Screenshot:



Errors

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

 Corrupt sample or wrongly selected analyzer. Details: 00040235

Malware Configuration

No configs have been found

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

0

Range:

0 - 100

Whitelisted:

false

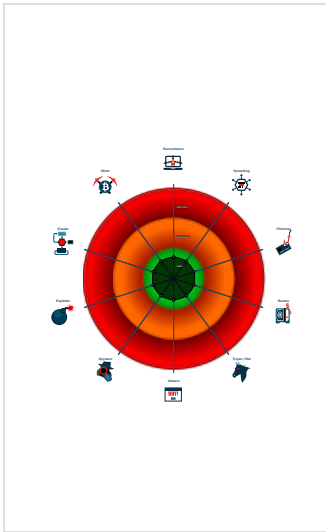
Confidence:

100%

Signatures

No high impact signatures.

Classification



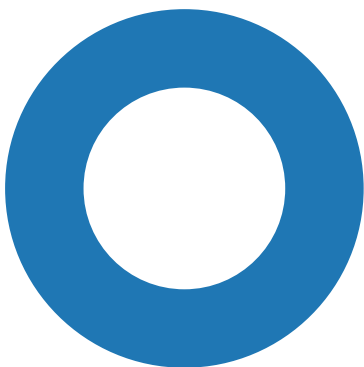
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx 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

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
Canadian TV ad for Covid testing.mp4	0%	Virustotal		Browse
Canadian TV ad for Covid testing.mp4	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:	33.0.0 White Diamond
Analysis ID:	487492
Start date:	21.09.2021
Start time:	18:00:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Canadian TV ad for Covid testing.mp4
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:	3
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:	<ul style="list-style-type: none">• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.winMP4@0/0@0/0
Cookbook Comments:	<ul style="list-style-type: none"> Adjust boot time Enable AMSI Found application associated with file extension: .mp4 Unable to launch sample, stop analysis
Warnings:	Show All <ul style="list-style-type: none"> Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe
Errors:	<ul style="list-style-type: none"> 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:	ISO Media, MP4 v2 [ISO 14496-14]
Entropy (8bit):	7.998978955168001
TrID:	<ul style="list-style-type: none"> MPEG-4 Video (70008/3) 36.74% iPhone Ringtone (63007/2) 33.07% 3GPP2 multimedia audio/video (48507/2) 25.46% QuickTime Movie (5001/1) 2.62% Generic MP4 container (3007/2) 1.58%
File name:	Canadian TV ad for Covid testing.mp4

General	
File size:	7511157
MD5:	19f79239cc58af3acd70c776a03e48df
SHA1:	73cfc069af3aeec9f009bcd2699ac2d7b99bf9c8
SHA256:	77c1f85e3fc64cc52d2d12452d696b7811a3923c7de224887bda9835eccbb395
SHA512:	510c71a60e31cac04bc5d7fe522aaaa78f36c64caf47a32cdb8c44a1510af78d5947105b3391f8269bb063c9ef1a73870346b7e62fc507546033e834519d9995
SSDEEP:	196608;j3Mp3S8Z527VMCJ0LAIQQYbxRJoP+au9mfHX923eT2;j8p3Su5Qt0TqxkgWHX2eT2
File Content Preview:ftypmp42....mp42isom....beam.....Q.moov...l mvhd.....D.\.....@.....trak...tkhd.....U.....@..

File Icon	
	
Icon Hash:	74f0dcc4c4c4e0e4

Network Behavior	
No network behavior found	

Code Manipulations	
--------------------	--

Statistics	
------------	--

System Behavior	
-----------------	--

Disassembly	
-------------	--