

JOeSandbox Cloud BASIC



ID: 796349

Sample Name: .lnk

Cookbook: default.jbs

Time: 20:22:42

Date: 01/02/2023

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report .lnk	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Malware Configuration	3
Yara Signatures	3
Sigma Signatures	3
Snort Signatures	3
Joe Sandbox Signatures	3
Mitre Att&ck Matrix	4
Antivirus, Machine Learning and Genetic Malware Detection	4
Initial Sample	4
Dropped Files	4
Unpacked PE Files	4
Domains	4
URLs	4
Domains and IPs	4
Contacted Domains	4
World Map of Contacted IPs	4
General Information	4
Errors	5
Simulations	5
Behavior and APIs	5
Joe Sandbox View / Context	5
IPs	5
Domains	5
ASNs	5
JA3 Fingerprints	5
Dropped Files	5
Created / dropped Files	5
Static File Info	5
General	6
File Icon	6
Static Windows Shortcut Info	6
General	6
Network Behavior	6
Statistics	6
System Behavior	6
Disassembly	6

Windows Analysis Report

.lnk

Overview

General Information

Sample Name:	.lnk
Analysis ID:	796349
MD5:	c1b580576916...
SHA1:	d5aa2ca1ac10...
SHA256:	539e1a66bee8...
Errors	
⚠ No process behavior to analyse as no analysis process or sample was found	
⚠ Corrupt sample or wrongly selected analyzer. Details: C00104C7	

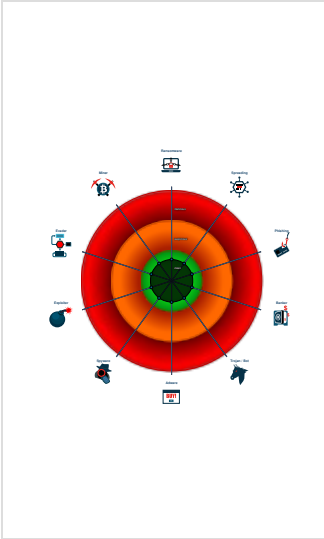
Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div>	
Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Malware Configuration

⊘ No configs have been found

Yara Signatures

⊘ No yara matches

Sigma Signatures

⊘ No Sigma rule has matched

Snort Signatures

⊘ No Snort rule has matched

Joe Sandbox Signatures

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

World Map of Contacted IPs

 No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	796349
Start date and time:	2023-02-01 20:22:42 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, 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:	<ul style="list-style-type: none">• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	.lnk
Detection:	UNKNOWN
Classification:	unknown0.winLNK@0/0@0/0
Cookbook Comments:	<ul style="list-style-type: none">• Found application associated with file extension: .lnk• Unable to launch sample, stop analysis

Errors

- No process behavior to analyse as no analysis process or sample was found
- Corrupt sample or wrongly selected analyzer. Details: C00104C7


Simulations

Behavior and APIs


 No simulations

Joe Sandbox View / Context


IPs

 No context


Domains

 No context


ASNs

 No context


JA3 Fingerprints

 No context

Dropped Files


 No context

Created / dropped Files

 No created / dropped files found


Static File Info


General	
File type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Entropy (8bit):	3.7144042381061304
TrID:	<ul style="list-style-type: none">Windows Shortcut (20020/1) 100.00%
File name:	.lnk
File size:	722
MD5:	c1b58057691608ec91813b89e1a9e938
SHA1:	d5aa2ca1ac10139f5fabbd77ee1fafd745c8b016
SHA256:	539e1a66bee8e5d745c23a0eb58be35f4506ad3b3a782ad267109f7d26c0829b
SHA512:	c8e0b1db003f399de6a9843719538f557b6950d868199db243c86838a04de52a76377e848d1c6846474e6d6384a6b1ec84a6d35720bdf8d3a49e8b4d64e6f027
SSDEEP:	12:8Rhur0ADJnSc6tOSwU1AeMlwTIDEjaWE0ADJkNr:8arvDJSc6pwUYIs0avvDJkB
TLSH:	D801AB0016D62300E925437805B41F05C963BA93E032671D329C4858937FA62EF3EF2E
File Content Preview:	L.....F.U.../...../D:\.....t.Y^...H.g.3...(w,.../..J...>V.h... 2.....EEO Acknowledgement Letter For Ms. Joanne Douglas (1.31.2023)


File Icon	
	
Icon Hash:	74ecccdcd6c9c9fd

Static Windows Shortcut Info	
General	
Relative Path:	
Command Line Argument:	
Icon location:	

Network Behavior	
Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.	

Statistics	
 No statistics	

System Behavior	
 No system behavior	

Disassembly	
 No disassembly	