

JOeSandbox Cloud BASIC



ID: 796592

Sample Name: Files.Ink

Cookbook: default.jbs

Time: 00:33:56

Date: 02/02/2023

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report Files.Ink	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
AV Detection	3
Mitre Att&ck Matrix	4
Behavior Graph	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	6
Contacted Domains	6
World Map of Contacted IPs	6
General Information	6
Errors	6
Warnings	6
Simulations	6
Behavior and APIs	6
Joe Sandbox View / Context	7
IPs	7
Domains	7
ASNs	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	7
Static File Info	7
General	7
File Icon	7
Static Windows Shortcut Info	7
General	7
Network Behavior	8
Statistics	8
System Behavior	8
Disassembly	8

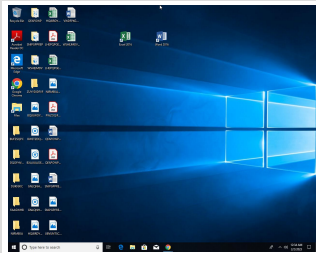
Windows Analysis Report

Files.lnk

Overview

General Information

Sample Name:	Files.lnk
Analysis ID:	796592
MD5:	b0166f01c48a7...
SHA1:	2091cc337e6a...
SHA256:	b968bc92e3f0f...
Tags:	lnk



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

Malware Configuration

No configs have been found

Detection

MALICIOUS

SUSPICIOUS

CLEAN

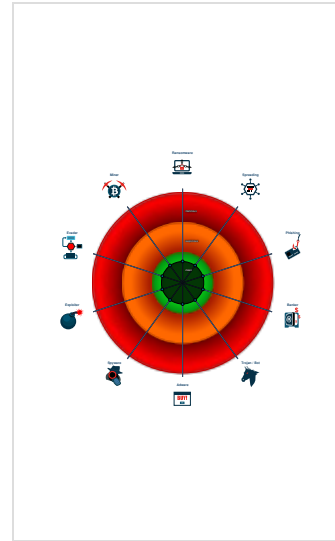
UNKNOWN

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub...
- Multi AV Scanner detection for subm...

Classification



Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Mitre Att&ck Matrix

🚫 No Mitre Att&ck techniques found

Behavior Graph

[Hide Legend](#)

Legend:

- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Behavior Graph

ID: 796592
Sample: Files.Ink
Startdate: 02/02/2023
Architecture: WINDOWS
Score: 56

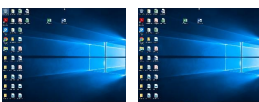
Antivirus / Scanner
detection for submitted
sample

Multi AV Scanner detection
for submitted file

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
Files.Ink	21%	ReversingLabs	Shortcut.Trojan.Ma ILink	
Files.Ink	16%	Virustotal		Browse
Files.Ink	100%	Avira	LNK/Runner.VPOY	

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:	796592
Start date and time:	2023-02-02 00:33:56 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 26s
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:	Files.Ink
Detection:	MAL
Classification:	mal56.winLNK@0/0@0/0
Cookbook Comments:	<ul style="list-style-type: none">• Found application associated with file extension: .Ink• 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

Warnings

- Excluded domains from analysis (whitelisted): fs.microsoft.com


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

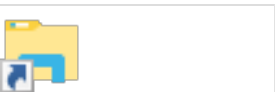
 No created / dropped files found

Static File Info

General

File type:	MS Windows shortcut, Item id list present, Has Relative path, Icon number=0, 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=hiddenormalshowminimized
Entropy (8bit):	1.6915641824581837
TrID:	<ul style="list-style-type: none">Windows Shortcut (20020/1) 100.00%
File name:	Files.Ink
File size:	1228
MD5:	b0166f01c48a7a117019d1ebdb77e8a2
SHA1:	2091cc337e6a69bf6bc5126c0e66afd12fad2514
SHA256:	b968bc92e3f0f62037ab6f29c13ba6895b6b2d78ea04f32eb1aceca9b509208a
SHA512:	a715389b3f0797bf38ead485640f6a4ccbc0f6ce884dee1048915a67f59969cfe81d4bf1bd5d375fb22ce66a5569b6af2370085261d1da97a54e289da60968ef
SSDEEP:	6:4xt/98el/t5zC7lkFw1lxcFwR+SkEMI47J6jclRaQmZAMI47tKHkWBdW:8X8K/takCwiCwEIMm9IDm1XHLY
TLSH:	1B21DF246EEB6B21EBE2D6B22071A3A54E773852F951C3CC0104AA8D203760479B9F27
File Content Preview:	L.....F.@.....P.O. ..i....+00.../C:\.....J.1.....ivy.8.....i.v.y....b.2.....texture.bat.H.....

File Icon



Icon Hash: 0c9ea2b28eb9bd0d

Static Windows Shortcut Info


General

Relative Path:	..\..\..\ivy\texture.bat
Command Line Argument:	
Icon location:	c:\windows\explorer.exe

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