

JOeSandbox Cloud BASIC



ID: 796586

Sample Name:

z__Desktop__.lnk

Cookbook: default.jbs

Time: 00:28:34

Date: 02/02/2023

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report z____Desktop____.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
Screenshots	4
Thumbnails	4
Antivirus, Machine Learning and Genetic Malware Detection	4
Initial Sample	5
Dropped Files	5
Unpacked PE Files	5
Domains	5
URLs	5
Domains and IPs	5
Contacted Domains	5
World Map of Contacted IPs	5
General Information	5
Errors	6
Simulations	6
Behavior and APIs	6
Joe Sandbox View / Context	6
IPs	6
Domains	6
ASNs	6
JA3 Fingerprints	6
Dropped Files	6
Created / dropped Files	6
Static File Info	6
General	6
File Icon	7
Static Windows Shortcut Info	7
General	7
Network Behavior	7
Statistics	7
System Behavior	7
Disassembly	7

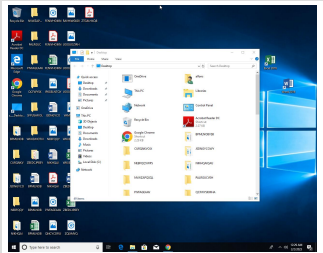
Windows Analysis Report

z__Desktop__.lnk


Overview

General Information

Sample Name:	z__Desktop__.lnk
Analysis ID:	796586
MD5:	9af17609ac270..
SHA1:	827e35ff6956a...
SHA256:	aee7021ddb18...
Tags:	lnk



Errors

 No process behavior to analyse as no analysis process or sample was found

Detection

MALICIOUS

SUSPICIOUS

CLEAN

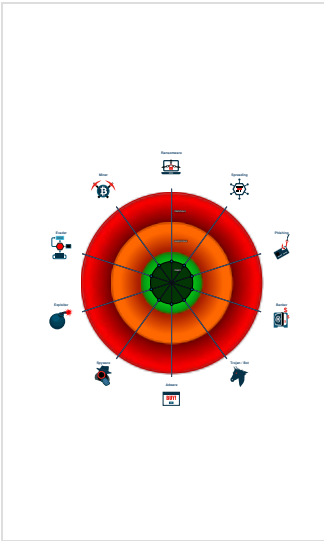
UNKNOWN

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](#).

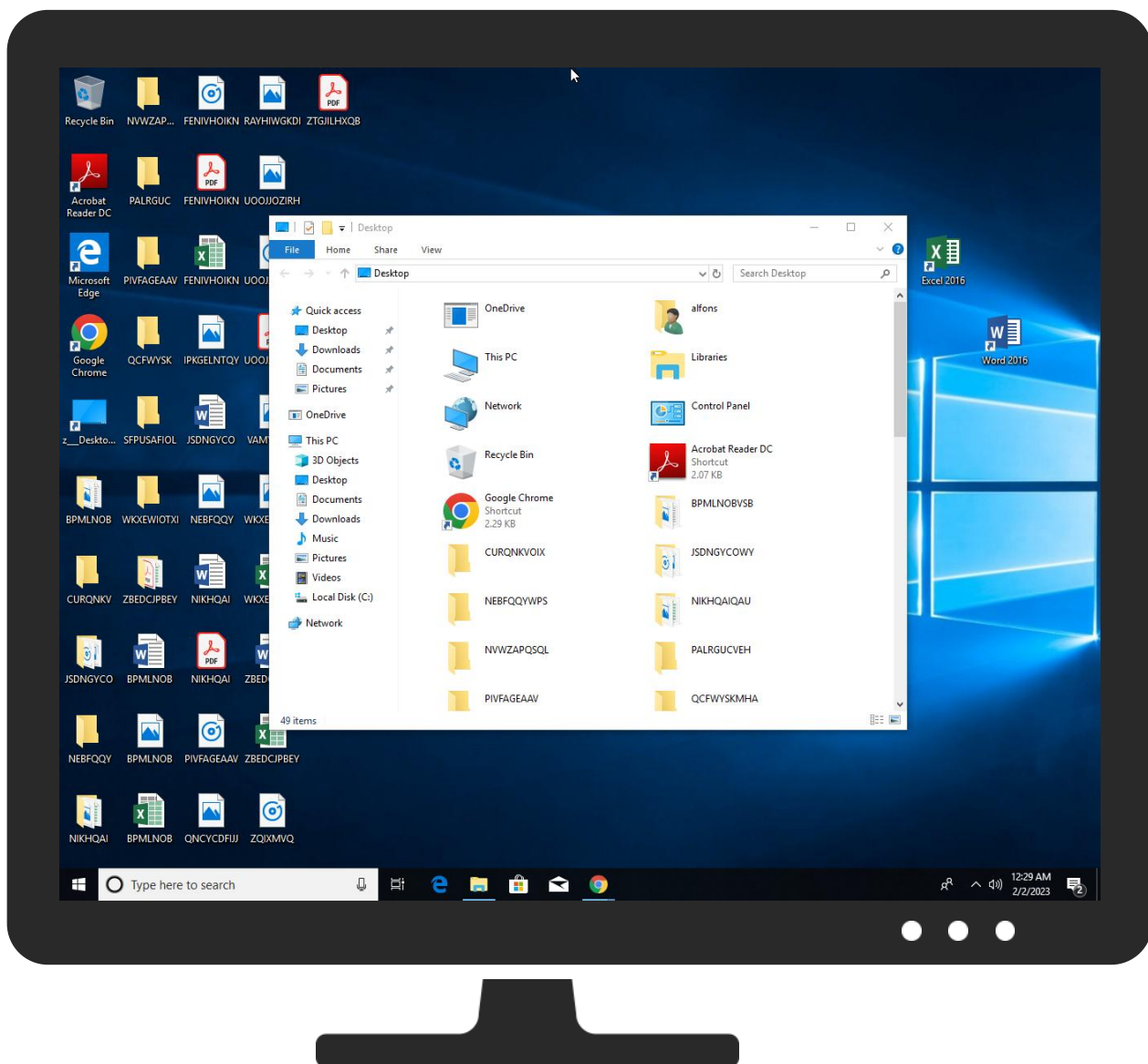
Mitre Att&ck Matrix

 No Mitre Att&ck techniques found

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
z__Desktop__.lnk	0%	ReversingLabs		
z__Desktop__.lnk	0%	Virustotal		Browse


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:	796586
Start date and time:	2023-02-02 00:28:34 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 18s
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:	z__Desktop__.lnk
Detection:	UNKNOWN
Classification:	unknown0.winLNK@0/0@0/0

Cookbook Comments:

- Found application associated with file extension: .lnk
- Stop behavior analysis, all processes terminated

Errors

- No process behavior to analyse as no analysis process or sample was found

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 Relative path, Read-Only, Directory, ctime= Tue Oct 8 07:41:12 2013, mtime= Wed Mar 11 01:45:54 2015, atime= Wed Mar 11 02:13:22 2015, length=40960, window=hide
Entropy (8bit):	4.469872682170529
TrID:	<ul style="list-style-type: none">• Windows Shortcut (20020/1) 100.00%
File name:	z_ Desktop_.lnk
File size:	438
MD5:	9af17609ac27044d1c1cd25916b855cc
SHA1:	827e35ff6956a8b7b4e714f36844acad912da76d
SHA256:	aee7021ddb18891a3af1226f0e4138e1374e405fc7956a8c2a8118c0c5a7398d
SHA512:	ce80dc6279b7e9b31ea47cc4be19e60974e6959c7dadd3dbcf5db9206433f3d56957e2ecc0065602a27998fd5c5da01e554044b0dc4cb37ee65b7320c86b39b9

SSDEEP:	6:4xtQlkuC+TColjeljtjOdWNAWclQRnINcXWS0GV9BhulUP0WzrN+IqMs+IqMjl:8bT+TC4je5tMOXdVhulUP0IOcYl
TLSH:	EEF068426176AB11C3384732C3F68247E13878539D99F7089021931648E8A15C0FF608
File Content Preview:	L.....F.....y..\$...C..~.[.....T. [.....J.....3.....l.....0.....System.C:\Users\ThuD\Desktop.....\D.e.s.k.t.o.p.....=...1SPS0.%.G....`...!.....D.e.s.k.t.o.p.....Y...1SPS.j

File Icon

	
Icon Hash:	00b29a8a8e898d0d


Static Windows Shortcut Info

General	
Relative Path:	..\Desktop
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
--