

JOeSandbox Cloud BASIC



ID: 796057

Sample Name: SecureCloud+ Limited.l

Cookbook: default.jbs

Time: 15:59:24

Date: 01/02/2023

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report SecureCloud+ Limited.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
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
Warnings	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

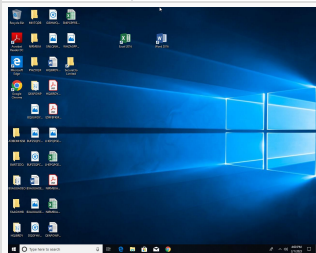
Windows Analysis Report

SecureCloud+ Limited.lnk

Overview

General Information

Sample Name:	SecureCloud+ Limited.lnk (renamed file extension from l to lnk)
Analysis ID:	796057
MD5:	7095da7ff9839...
SHA1:	ad0991994756...
SHA256:	434c0b82e1ec...



Errors

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

Corrupt sample or wrongly selected analyzer. Details: 00010007

Malware Configuration

No configs have been found

Detection

MALICIOUS

SUSPICIOUS

CLEAN

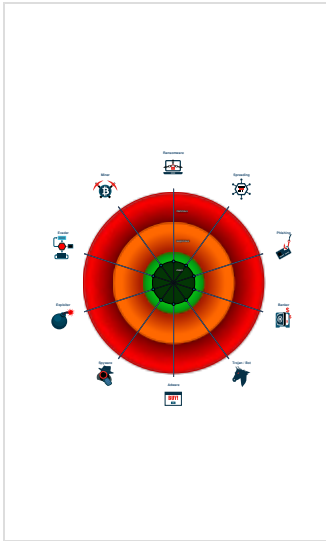
UNKNOWN

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

Signatures

No high impact signatures.

Classification



Yara 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](#).

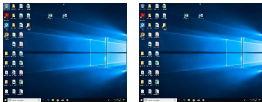
Mitre Att&ck Matrix

 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
<div> <div></div> <div>No Antivirus matches</div> </div>

Dropped Files
<div> <div></div> <div>No Antivirus matches</div> </div>

Unpacked PE Files
<div> <div></div> <div>No Antivirus matches</div> </div>

Domains
<div> <div></div> <div>No Antivirus matches</div> </div>

URLs
<div> <div></div> <div>No Antivirus matches</div> </div>

Domains and IPs
Contacted Domains
<div> <div></div> <div>No contacted domains info</div> </div>

World Map of Contacted IPs
<div> <div></div> <div>No contacted IP infos</div> </div>

General Information	
Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	796057
Start date and time:	2023-02-01 15:59:24 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 13s
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:	SecureCloud+ Limited.Ink (renamed file extension from I to Ink)
Detection:	UNKNOWN
Classification:	unknown0.winLNK@0/0@0/0
Cookbook Comments:	<ul style="list-style-type: none"> 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, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Wed Jan 4 11:37:06 2023, mtime=Wed Feb 13:26:09 2023, atime=Wed Feb 1 09:42:56 2023, length=0, window=hide
Entropy (8bit):	5.15915180453579
TrID:	<ul style="list-style-type: none">Windows Shortcut (20020/1) 100.00%
File name:	SecureCloud+ Limited.Ink
File size:	863
MD5:	7095da7ff983987d9d94f3bd79605f68
SHA1:	ad09919947567602a0bc72501706906704dc4b79

SHA256:	434c0b82e1ecc2af340e556a29034a9e2b432d64661d7593d360d971c0eb6d24
SHA512:	17980fa2e496a1f727dc0d1b90a56aeecf14efa8d00d0dd81af61a571ae134a279555dac329e9e35cc00ebd4c04730d3aebbcd8ea4f5bc5ebeba4d3d10bbe1
SSDEEP:	12:82DUyHCk4pxNY1MCVh4SSgpkEjCtVOIC5O31+GGJJ2IAt8g54UNwuLCbh/fDCOIC:82wxtYpaQCHpCE3gGG32I6jibhuYPSm
TLSH:	6D11D01997CA1B6AE3F1917D88690756BB21B473F4F20F2D154466450CAB7818850F0F
File Content Preview:	L.....F.....PA9 ...U. l6....)6.....:..DG..Yr?.D..U..k0.&...&.....G~...x..)6.....G6.....t...CFSF..1.....AVJU..SECURE~1....t.Y^...H.g.3.. (.....gVA.G..k..Z.....\$V.dAVfm....8.....S.e.c

File Icon



Icon Hash:

30b4b4b464696d0d

Static Windows Shortcut Info	
General	
Relative Path:	..\..\..\IbukunJerry-Sodipe\SecureCloud+ Limited
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