

JOeSandbox Cloud BASIC



ID: 795693

Sample Name:

DECIDENT.LNK.lnk

Cookbook: default.jbs

Time: 07:51:10

Date: 01/02/2023

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report DECIDENT.LNK.lnk	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Sigma Signatures	3
Snort Signatures	3
Joe Sandbox Signatures	4
AV Detection	4
Persistence and Installation Behavior	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
World Map of Contacted IPs	7
Public IPs	7
Private	7
General Information	7
Warnings	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASNs	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static Windows Shortcut Info	8
General	8
Network Behavior	9
Statistics	9
Behavior	9
System Behavior	9
Analysis Process: cmd.exePID: 1804, Parent PID: 3528	9
General	9
File Activities	9
Analysis Process: conhost.exePID: 5264, Parent PID: 1804	9
General	9
File Activities	10
Disassembly	10

