

JoeSandbox Cloud BASIC



**ID:** 745704

**Sample Name:** 71e0000.dll.exe

**Cookbook:** default.jbs

**Time:** 16:52:14

**Date:** 14/11/2022

**Version:** 36.0.0 Rainbow Opal

# Table of Contents

Table of Contents	2
Windows Analysis Report 71e0000.dll.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Ursnif	4
Yara Signatures	5
Initial Sample	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Key, Mouse, Clipboard, Microphone and Screen Capturing	5
E-Banking Fraud	6
Hooking and other Techniques for Hiding and Protection	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
World Map of Contacted IPs	9
General Information	9
Warnings	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASNs	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
Static File Info	10
General	10
File Icon	10
Static PE Info	10
General	10
Entrypoint Preview	11
Data Directories	12
Sections	13
Network Behavior	13
Statistics	13
Behavior	13
System Behavior	13
Analysis Process: loadll64.exePID: 5860, Parent PID: 3452	13
General	13
File Activities	14
Analysis Process: conhost.exePID: 5968, Parent PID: 5860	14
General	14
Analysis Process: cmd.exePID: 3888, Parent PID: 5860	14
General	14
File Activities	14
Analysis Process: rundll32.exePID: 5304, Parent PID: 5860	15
General	15
File Activities	15
Analysis Process: rundll32.exePID: 5248, Parent PID: 3888	15
General	15
File Activities	15
Disassembly	15



























