



ID: 528760

Sample Name: JZ3FrTU0tJ.exe

Cookbook: default.jbs

Time: 18:39:01 Date: 25/11/2021

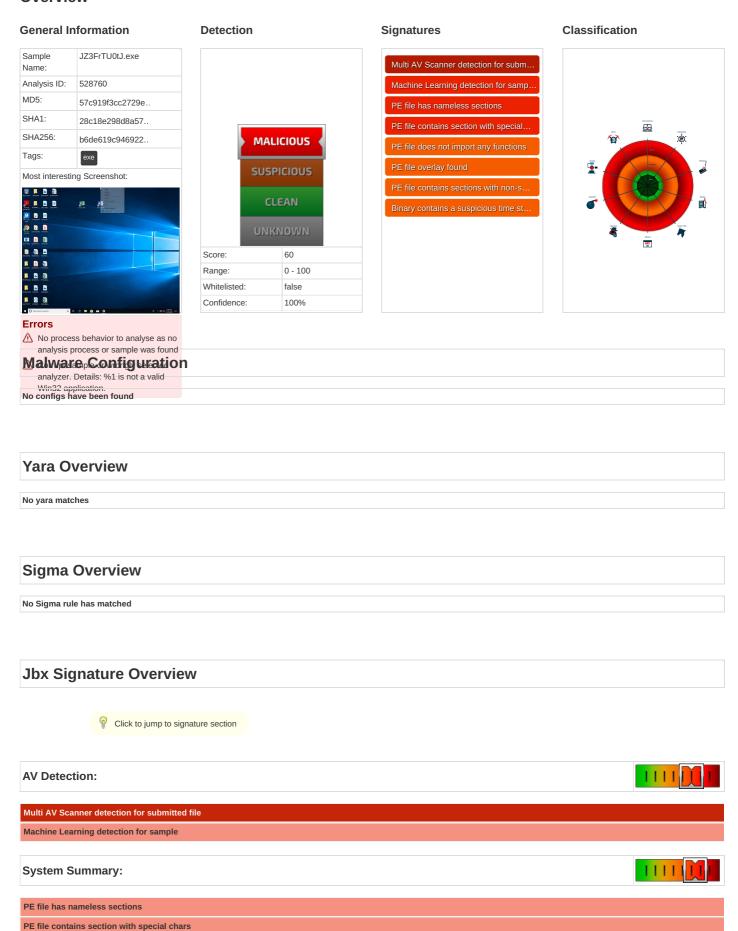
Version: 34.0.0 Boulder Opal

Table of Contents

Overview General Information Detection Signatures Classification Signatures Classification Signatures Classification Signatures Signa Overview Signa Overview Signa Overview Signa Overview Signa Overview Signa Overview Signature	Table of Contents	2
Overview General Information Detection Signatures Classification Malware Configuration Yara Overview Sigma Overview Jbx Signature Overview 4 AV Detection: System Summary: Mitre Attack Matrix 4 Behavior Graph 4 Screenshots 4 Thumbnails 4 Antivirus, Machine Learning and Genetic Malware Detection 5 Initial Sample 5 Dropped Files 9 Unpacked PE Files 9 Domains 0 URLs 0 Contacted of PE Files 6 Domains and IPS 6 Contacted IPS 6 General Information 6 Simulations 6 Behavior and APIs 6 Joe Sandbox View / Context 6 IPS 9 Domains 9 ASI Fingerprints 9 Domped Files 9 Static File Info <t< th=""><th>Windows Analysis Report JZ3FrTU0tJ.exe</th><th>3</th></t<>	Windows Analysis Report JZ3FrTU0tJ.exe	3
General Information Detection Signatures Classification Malware Configuration Yara Overview Sigma Overview Jbx Signature Overview AV Detection: System Summary: Mitre Att&ck Matrix Behavior Graph Screenshots Thumbnails Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Unpacked PE Files Unpacked PE Files Unpacked PE Files Contacted Domains URLs Contacted Domains Contacted Domains Contacted Domains Contacted PS General Information Simulations Behavior and APIS Joe Sandbox View / Context IPS Domains ASN JA3 Fingerprints Dropped Files Created / dropped Files Created / dropped Files Created / dropped Files Created / dropped Files Static File Info General File Icon Static File Info General Data Directories Socions Network Behavior Extensions Ex		3
Detection Signatures Classification Malware Configuration Signature Configuration Signature Configuration Signature Overview Signature O	General Information	3
Classification Malware Configuration Yara Overview Sigma Overview Jiby Signature Overview AV Detection: System Summary: Mitre Att&ck Matrix Behavior Graph Screenshots Thumbnais Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Domains URLs Domains and IPs Contacted Domains Contacted Domains Contacted Domains Contacted IPs General Information Simulations Behavior and APis Joe Sandbox View / Context IPs Domains ASN JA3 Fingerprints Dropped Files Created / dropped Files Static File Info General File Icon Static File Info General Data Directories Sections Network Behavior		3
Malware Configuration 9 Yara Overview 5 Sigma Overview 4 AV Detection: 5 System Summary: Mitre Att&ck Matrix Behavior Graph 2 Screenshots 4 Thumbonalis 4 Antivirus, Machine Learning and Genetic Malware Detection 8 Initial Sample 1 Dropped Files 1 Unpacked PE Files 1 Domains 1 URLs 1 Domains and IPs 6 Contacted Domains 6 Contacted IPs 6 General Information 6 Simulations 6 Behavior and APIs 6 Joe Sandbox View / Context 9 IPs 1 Domains 1 ASN 3AS Ingerprints Dropped Files 1 Created / dropped Files 1 Static File Info 6 General File Icon State PE Info 6 General File Icon		
Yara Overview Sigma Overview Jiby Signature Overview AV Detection: System Summary: Mitre Att&ck Matrix Behavior Graph Screenshots Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Unpacked PE Files Unpacked PE Files Obmains URLs Domains and IPS Contacted Domains Contacted IPS General Information Simulations Behavior and APIs Joe Sandbox View / Context IPS Domains ASN JA3 Fingerprints Dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General File Icon Static PE Info General Detail Details Deta		
Signa Overview JDS Signature Overview AV Detector: System Summary: Mitre Att&ck Matrix Behavior Graph Screenshots Thumbnails Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Domains URLs Domains and IPs Contacted Domains Contacted Domains Contacted IPs General Information Simulations Behavior and APIs Dos Sandbox View / Context IPs Domains ASN JDA Singerprints Dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General File Icon Sta		
Jbx Signature Overview AV Detection: System Summary: Mitre Att&ck Matrix Behavior Graph Screenshots Thumbnails Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Domains URLs Domains and IPs Contacted Domains Contacted IPs General Information Simulations Behavior and APis Joe Sandbox View / Context IPs Joanins ASN JA3 Fingerprints Dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General Dian Directories Sections Network Behavior Code Manipulations Statistics System Behavior		
AV Defection: System Summary: Mitre Att&ck Matrix Behavior Graph Screenshots Thumbnails Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Domains URLs Domains and IPs Contacted Domains Contacted IPs General Information Simulations Behavior and APIs Joe Sandbox View / Context IPs Domains ASN JAS Fingerprints Dropped Files Static File Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statistics System Behavior		
System Summary: Mitre Att&ck Matrix Behavior Graph Screenshots Thumbnails Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Domains URLs URLs Domains and IPS Contacted Domains Contacted IPS General Information Simulations Behavior and APIs Joe Sandbox View / Context IPS Domains ASN JA3 Fingerprints Dropped Files Static File Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statictics Statictics System Behavior Screenses Sections System Behavior Screenses System Behavior Screenses System Behavior Screenses System Behavior	Jbx Signature Overview	3
Mitre Att&ck Matrix Behavior Graph Screenshots Thumbnails Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Domains URLs Domains and IPS Contacted Domains Contacted IPs General Information Simulations Behavior and APIs JA3 Fingerprints Dropped Files Created / dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General Data Directories Sectors Network Behavior Network Behavior Ref System Behavior Statistics System Behavior		
Behavior Graph Screenshots Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Domains URLs Domains and IPS Contacted Domains Contacted IPS General Information Simulations Behavior and APIs Joe Sandbox View / Context IPS Domains ASN JAS Fingerprints Dropped Files Created / dropped Files Static File Info General File Loon Statu Dietories Sections Network Behavior Retwork Behavior Statistics System Behavior	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
Screenshots Thumbnails Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Domains URLs Domains and IPS Contacted Domains Contacted IPS General Information Gimulations Behavior and APIs Domains ASN JA3 Fingerprints Dropped Files Created / dropped Files Created / dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General Data Directories Sections Network Behavior Statistics System Behavior Statistics		
Thumbnails Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Unpacked PE Files Unpacked PE Files Domains URLs Domains and IPs Contacted Domains Contacted IPs General Information Gimulations Behavior and APIs Joe Sandbox View / Context IPs Domains ASN JA3 Fingerprints Dropped Files Created / dropped Files Static File Info General File Icon Static File Info General File Icon Static PE Info General Data Directories Sectors Network Behavior Code Manipulations Staticics System Behavior	Behavior Graph	
Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Domains URLs Domains and IPS Contacted Domains Contacted IPS General Information Gimulations Behavior and APIs Joe Sandbox View / Context IPS Domains JA3 Fingerprints Dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statics Statics Statics System Behavior		
Initial Sample Dropped Files Unpacked PE Files Domains URLs Domains and IPs Contacted Domains Contacted Domains Contacted IPs General Information Simulations Behavior and APIs Joe Sandbox View / Context IPs Domains ASN JA3 Fingerprints Dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statics System Behavior		
Dropped Files Inpacked PE Files Domains IDmains URLs IDmains and IPs Contacted Domains IDmains Contacted IPs IDmains General Information IDmains Simulations IDmains Behavior and APIs IDmains Joe Sandbox View / Context IPs Domains ASN JA3 Fingerprints IDmorped Files Created / dropped Files Image: Info General File Info General File Icon Static File Info General Data Directories Sections Image: Info General Sections Sections Network Behavior Image: Image		
Unpacked PE Files Domains URLs Domains and IPS Contacted Domains Contacted IPS General Information General IPS Domains ASN Joe Sandbox View / Context IPS Domains ASN JA3 Fingerprints Dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statics System Behavior		
Domains URLs Contacted Domains Contacted Domains Contacted IPs Contacted IPs Ceneral Information		
URLs Domains and IPs 6 Contacted Domains 6 Contacted IPs 6 General Information 6 Simulations 6 Behavior and APIs 6 Joe Sandbox View / Context 6 IPs 6 Domains 8 ASN 9 JA3 Fingerprints 9 Dropped Files 9 Created / dropped Files 9 Static File Info 9 General 9 File Icon 9 Static PE Info 9 General 9 Data Directories 9 Sections 9 Network Behavior 8 Code Manipulations 8 Statistics 8 System Behavior 8		
Domains and IPs		
Contacted Domains	Domains and IPs	6
General Information 6 Simulations 6 Behavior and APIs 6 Joe Sandbox View / Context 6 IPs 0 Domains 3 ASN JA3 Fingerprints JA3 Fingerprints 5 Toppped Files 5 Created / dropped Files 7 Static File Info 7 General 8 File Icon 9 Static PE Info 9 General 9 Data Directories 9 Sections 1 Network Behavior 8 Code Manipulations 8 Statistics 8 System Behavior 8	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
Simulations 6 Behavior and APIs 6 Joe Sandbox View / Context 6 IPs 6 Domains 5 ASN 3 JA3 Fingerprints 5 Dropped Files 6 Created / dropped Files 7 Static File Info 6 General 6 File Icon 5 Static PE Info 6 General 6 Data Directories 5 Sections 1 Network Behavior 2 Code Manipulations 2 Statistics 5 System Behavior 5	~	6
Behavior and APIs Joe Sandbox View / Context IPs Domains ASN JA3 Fingerprints Dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statistics System Behavior	General Information	6
Joe Sandbox View / Context IPs Domains ASN JA3 Fingerprints Dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statistics System Behavior	Simulations	6
IPS Domains ASN JA3 Fingerprints Dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statics System Behavior		(
Domains ASN JA3 Fingerprints Dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statistics System Behavior		
ASN JA3 Fingerprints Dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statistics System Behavior		
JA3 Fingerprints Dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations System Behavior	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
Dropped Files Created / dropped Files Static File Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statistics System Behavior		
Created / dropped Files Static File Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statistics System Behavior		
Static File Info General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statistics System Behavior		
General File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statistics System Behavior		7
File Icon Static PE Info General Data Directories Sections Network Behavior Code Manipulations Statistics System Behavior	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
General Data Directories 5 Sections 5 Network Behavior 8 Code Manipulations 8 Statistics 8 System Behavior 8		
Data Directories Sections Network Behavior Code Manipulations Statistics System Behavior		
Sections Network Behavior Code Manipulations Statistics System Behavior		
Network Behavior Code Manipulations Statistics System Behavior		
Statistics System Behavior Statistics	Network Behavior	8
Statistics System Behavior Statistics	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	3
System Behavior 8		3
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	3
DISASSETTIBLY	Disassembly	

# Windows Analysis Report JZ3FrTU0tJ.exe

#### **Overview**

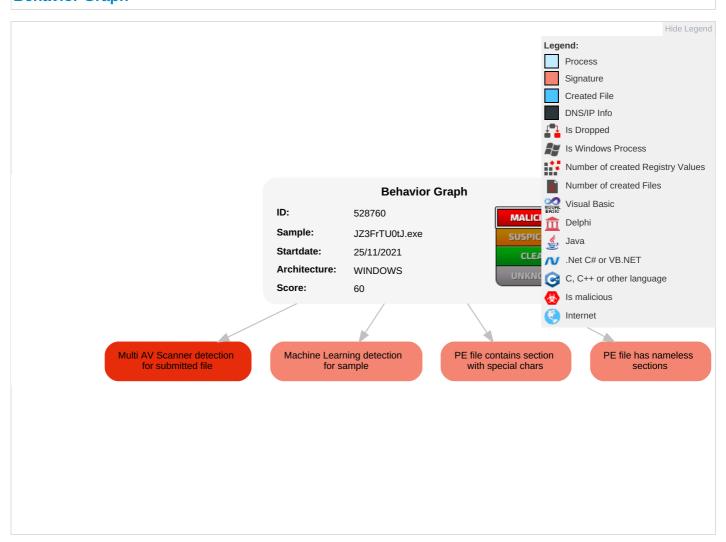


Copyright Joe Security LLC 2021 Page 3 of 9

### Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Software Packing 2	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Partitio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Timestomp 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockou
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares		Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

# **Behavior Graph**



### **Screenshots**

#### **Thumbnails**

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Copyright Joe Security LLC 2021 Page 4 of 9





Antivirus, macrime Learning and Seriede Maiware Detection							
Initial Sample							
Source	Detection	Scanner	Label	Link			
JZ3FrTU0tJ.exe	20%	Virustotal		Browse			
JZ3FrTU0tJ.exe	100%	Joe Sandbox ML					
Dropped Files							
No Antivirus matches							
Unpacked PE Files							
No Antivirus matches							
Domains							
No Antivirus matches							
URLs							
No Antivirus matches							

Copyright Joe Security LLC 2021 Page 5 of 9

## **Domains and IPs**

#### **Contacted Domains**

No contacted domains info

#### **Contacted IPs**

No contacted IP infos

## **General Information**

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528760
Start date:	25.11.2021
Start time:	18:39:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JZ3FrTU0tJ.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	3
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><li>EGA enabled</li><li>HDC enabled</li><li>AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.winEXE@0/0@0/0
Cookbook Comments:	<ul> <li>Adjust boot time</li> <li>Enable AMSI</li> <li>Found application associated with file extension: .exe</li> <li>Unable to launch sample, stop analysis</li> </ul>
Warnings:	Show All
Errors:	<ul> <li>No process behavior to analyse as no analysis process or sample was found</li> <li>Corrupt sample or wrongly selected analyzer. Details: %1 is not a valid Win32 application.</li> </ul>

## **Simulations**

#### **Behavior and APIs**

No simulations

## Joe Sandbox View / Context

IPs

Copyright Joe Security LLC 2021 Page 6 of 9

No context	
D	
Domains	
No context	
ASN	
AON	
No context	
JA3 Fingerprints	
3.1	
No context	
Dropped Files	
No context	
Created / dropped Files	
No created / dropped files found	
Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assemb ly, for MS Windows
Entrany (9hit):	6.062702964006129

#### TrID: • Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) • Generic Win/DOS Executable (2004/3) 0.01% DOS Executable Generic (2002/1) 0.01% JZ3FrTU0tJ.exe File name: File size: 183635 MD5: 57c919f3cc2729eef0f8cbf72aa712a9 SHA1: 28c18e298d8a579db4cbfa459c35bdde29de58ac b6de619c9469226aef6d9af08b03d51e7d200d53a9acffc SHA256: 6adcd975e0d48e3d9 SHA512: 92833ac52b646cb0c79f1e87e5e54996a446f46442bcffd 321857fc8190374d57acc74e25a53d2371be0ae2af34998 0182fa785b5e930003aa95e22398df1468 SSDEEP: 3072:yVaok+snqUvu3m7xAddxcrmGHlrNHjEalqIU+onE ksKSm20DMxQQtYscKgoN60eZ:yVa3+sqU4/Kx6aPIU+ onEksKSm20DMxG File Content Preview: MZ......@..... is program cannot be run in DOS mode....\$......PE..L...q

# File Icon

Icon Hash: 00828e8e8686b000

### Static PE Info

General	
Entrypoint:	0x44200a
Entrypoint Section:	

Copyright Joe Security LLC 2021 Page 7 of 9

General	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0xD261EA71 [Thu Nov 6 05:26:09 2081 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	

#### **Data Directories**

#### Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
[`MOak	0x2000	0xe564	0xe600	False	1.00044157609	data	7.99738998665	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_D ATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0x12000	0x2c908	0x2ca00	False	0.29661927892	data	4.34882960737	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x40000	0x5d6	0x600	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_D ATA, IMAGE_SCN_MEM_READ
	0x42000	0x10	0x200	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x44000	Охс	0x200	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_D ATA, IMAGE_SCN_MEM_DISCARDABLE , IMAGE_SCN_MEM_READ

## **Network Behavior**

No network behavior found

# **Code Manipulations**

## **Statistics**

# **System Behavior**

# Disassembly

Copyright Joe Security LLC

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal

Copyright Joe Security LLC 2021 Page 8 of 9

Copyright Joe Security LLC 2021 Page 9 of 9