

JoeSandbox Cloud BASIC



**ID:** 528196

**Sample Name:** exe.exe

**Cookbook:** default.jbs

**Time:** 20:50:07

**Date:** 24/11/2021

**Version:** 34.0.0 Boulder Opal

## Table of Contents

Table of Contents	2
Windows Analysis Report exe.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Memory Dumps	3
Sigma Overview	3
Jbx Signature Overview	3
AV Detection:	4
Networking:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Anti Debugging:	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
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	9
Static PE Info	9
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	10
Code Manipulations	10
Statistics	10
System Behavior	10
Analysis Process: exe.exe PID: 2632 Parent PID: 2680	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

# Windows Analysis Report exe.exe

## Overview

### General Information

Sample Name:

exe.exe

Analysis ID:

528196

MD5:

ccdf9de19a42d30..

SHA1:

413b2f4c1cc4f24...

SHA256:

0a2a2c18fa708a3.

Infos:

Most interesting Screenshot:

### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

76

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

### Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Yara detected GuLoader

Tries to detect virtualization through...

C2 URLs / IPs found in malware con...

Found potential dummy code loops (...)

Uses 32bit PE files

Sample file is different than original ...

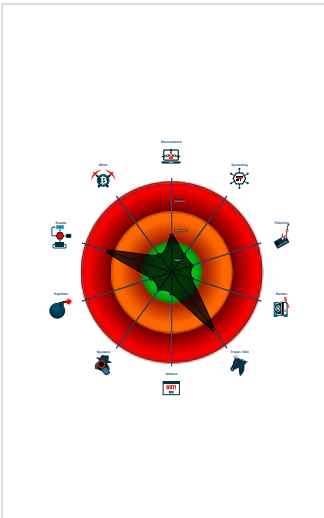
Tries to load missing DLLs

Contains functionality to read the PEB

Uses code obfuscation techniques (...)

Detected potential crypto function

### Classification



## Process Tree

System is w7x64

exe.exe (PID: 2632 cmdline: "C:\Users\user\Desktop\exe.exe" MD5: CCDF9DE19A42D303579DFCC11F846BCB)

cleanup

## Malware Configuration

### Threatname: GuLoader

```
{  "Payload URL ": "https://drive.google.com/uc?export=download"}
```

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.935818125.000000000002C0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

## Sigma Overview

No Sigma rule has matched

## Jbx Signature Overview

## AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

## Networking:



C2 URLs / IPs found in malware configuration

## Data Obfuscation:



Yara detected GuLoader

## Malware Analysis System Evasion:



Tries to detect virtualization through RDTSC time measurements

## Anti Debugging:

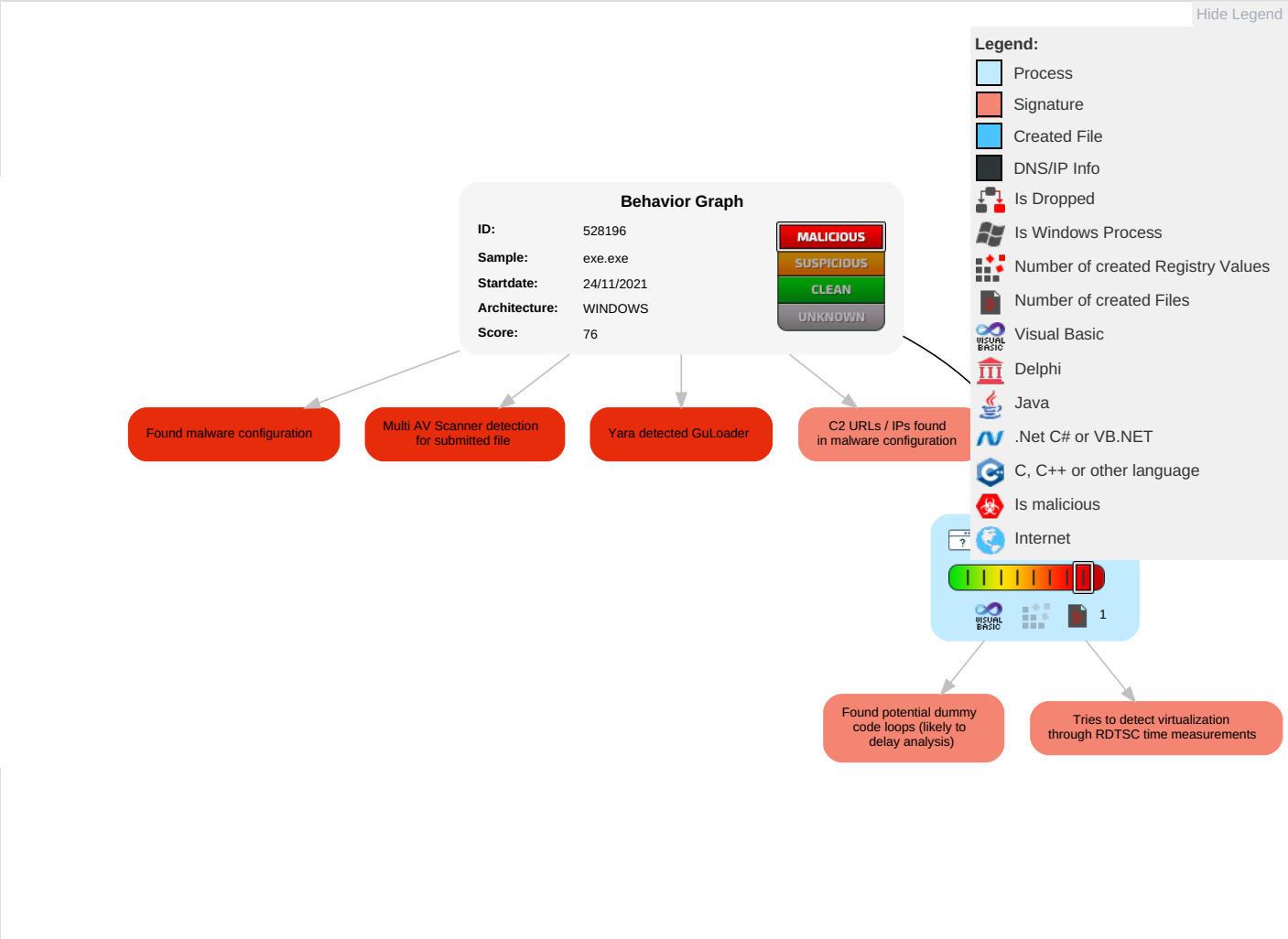


Found potential dummy code loops (likely to delay analysis)

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Recovery
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Oldest
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Information Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Be

## Behavior Graph





## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

Source	Detection	Scanner	Label	Link
exe.exe	21%	Virustotal		<a href="#">Browse</a>

### 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

### Contacted IPs

No contacted IP infos

## General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528196
Start date:	24.11.2021
Start time:	20:50:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	exe.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
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 style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.evad.winEXE@1/1@0/0
EGA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 100%</li></ul>
HDC Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 66.4% (good quality ratio 45%)</li><li>• Quality average: 31.7%</li><li>• Quality standard deviation: 27.8%</li></ul>
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found application associated with file extension: .exe</li><li>• Override analysis time to 240s for sample files taking high CPU consumption</li></ul>
Warnings:	Show All

## Simulations

### Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files


C:\Users\user\AppData\Local\Temp\~DF56168A067CC46460.TMP	
Process:	C:\Users\user\Desktop\exe.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	CE338FE6899778AACFC28414F2D9498B
SHA1:	897256B6709E1A4DA9DABA92B6BDE39CCFCCD8C1
SHA-256:	4FE7B59AF6DE3B665B67788CC2F99892AB827EFAE3A467342B3BB4E3BC8E5BFE
SHA-512:	6EB7F16CF7AFCABE9BDEA88BDAB0469A7937EB715ADA9DFD8F428D9D38D86133945F5F2F2688DDD96062223A39B5D47F07AFC3C48D9DB1D5EE3F41C8D274DCCF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	..... ..... ..... .....

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.802371954737389
TrID:	<ul style="list-style-type: none"><li>Win32 Executable (generic) a (10002005/4) 99.15%</li><li>Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%</li><li>Generic Win/DOS Executable (2004/3) 0.02%</li><li>DOS Executable Generic (2002/1) 0.02%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li></ul>
File name:	exe.exe
File size:	131072
MD5:	ccd9de19a42d303579dfcc11f846bcb
SHA1:	413b2f4c1cc4f242d50bd95faa7ca85bcbcbfdef



<b>General</b>	
SHA256:	0a2a2c18fa708a33573b788860a4911e6d6d6d3ddf8cacdddf4d9d100ca562d
SHA512:	3cac24c5db93f786247392af6c4425bc840fa7be314699b9d06f54b266cb8f326d9ab877270d7c70f7c445daf1f84cb8ec84802e0813ea00fc9d725c5a52dfd2
SSDEEP:	768:tyJDhaJ0vn7EZR5EjsXC1M+P7p/z8ol8e0JOCKIh3yOL1Z+lrNqVGPookwXB90JM:tkD00uzM7pAygkI5ZAk174OzyfD
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$......i..... .....*.....Rich.....PE..L...".AS..... ...0.....@.....

<b>File Icon</b>	
	
Icon Hash:	981dca909cee36b0

**Static PE Info**

<b>General</b>	
Entrypoint:	0x4013b4
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5341DD60 [Sun Apr 6 23:04:00 2014 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	d77040f4614bccfda7b8aa2e04863738

**Entrypoint Preview**

**Data Directories**

**Sections**

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1ce6c	0x1d000	False	0.35092268319	data	4.98845354205	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1e000	0x141c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x20000	0xf60	0x1000	False	0.3388671875	data	3.27120333743	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ


**Resources**

**Imports**

**Version Infos**

**Possible Origin**

Language of compilation system	Country where language is spoken	Map
--------------------------------	----------------------------------	-----

Language of compilation system	Country where language is spoken	Map
English	United States	
Turkmen	Turkmenistan	

## Network Behavior

No network behavior found

## Code Manipulations

## Statistics

## System Behavior

Analysis Process: exe.exe PID: 2632 Parent PID: 2680

### General

Start time:	20:50:19
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\exe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\exe.exe"
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	CCDF9DE19A42D303579DFCC11F846BCB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none"> <li>Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.935818125.00000000002C0000.00000040.00000001.sdmp, Author: Joe Security</li> </ul>
Reputation:	low

### File Activities

Show Windows behavior

## Disassembly

## Code Analysis

