

JOESandbox Cloud BASIC



**ID:** 526313

**Sample Name:**

n#U00ba410000512664.exe

**Cookbook:** default.jbs

**Time:** 14:04:11

**Date:** 22/11/2021

**Version:** 34.0.0 Boulder Opal

# Table of Contents

Table of Contents	2
Windows Analysis Report n#U00ba410000512664.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
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
URLs from Memory and Binaries	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: n#U00ba410000512664.exe PID: 3232 Parent PID: 5476	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

# Windows Analysis Report n#U00ba410000512664.exe

## Overview

### General Information

Sample Name:	n#U00ba410000512664.exe
Analysis ID:	526313
MD5:	7c91db57c98a1f0..
SHA1:	28cb0d40a73c1a..
SHA256:	12992fe3f998693..
Tags:	exe
Infos:	
Most interesting Screenshot:	

### Detection

**MALICIOUS**

SUSPICIOUS

CLEAN

UNKNOWN

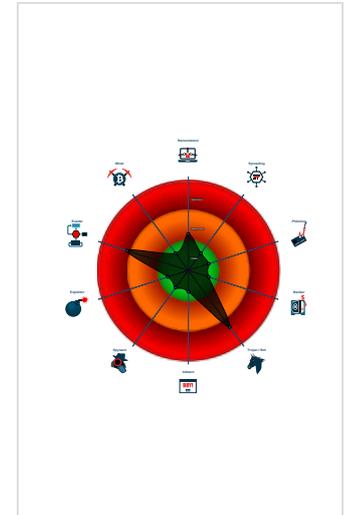
**GuLoader**

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

### Signatures

- Found malware configuration
- Yara detected GuLoader
- Found potential dummy code loops (...)
- Machine Learning detection for samp...
- C2 URLs / IPs found in malware con...
- Uses 32bit PE files
- Sample file is different than original ...
- PE file contains strange resources
- Contains functionality to read the PEB
- Program does not show much activi...
- Uses code obfuscation techniques (...)
- Contains functionality for execution ...

### Classification



## Process Tree

- System is w10x64
-  n#U00ba410000512664.exe (PID: 3232 cmdline: "C:\Users\user\Desktop\n#U00ba410000512664.exe" MD5: 7C91DB57C98A1F0E38BA65ED651B4779)
- cleanup

## Malware Configuration

Threatname: GuLoader

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

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.781957449.00000000021F0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

## Sigma Overview

No Sigma rule has matched

## Jbx Signature Overview

Click to jump to signature section

### AV Detection:



Found malware configuration

Machine Learning detection for sample

### Networking:



C2 URLs / IPs found in malware configuration

### Data Obfuscation:



Yara detected GuLoader

### Anti Debugging:

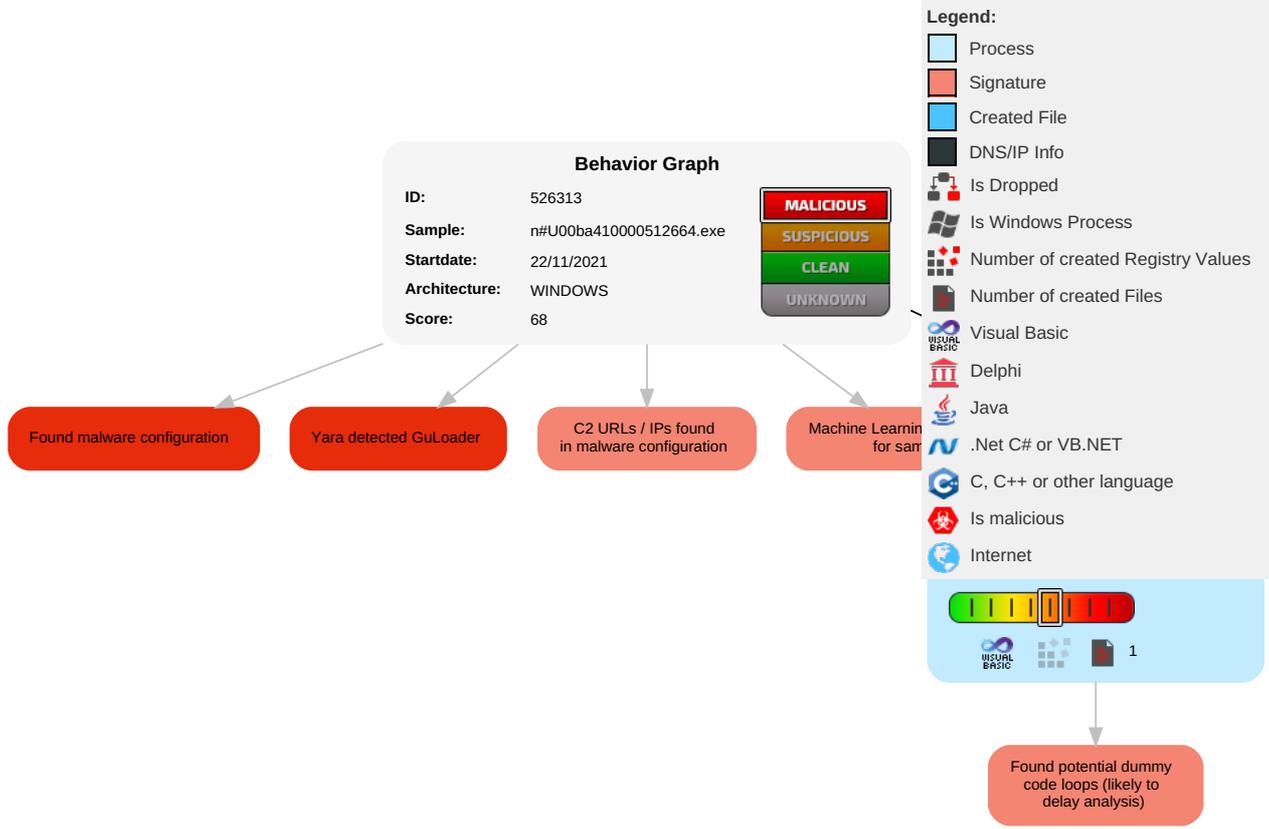


Found potential dummy code loops (likely to delay analysis)

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Risk Score
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	High
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	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	High
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 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	Medium
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Low

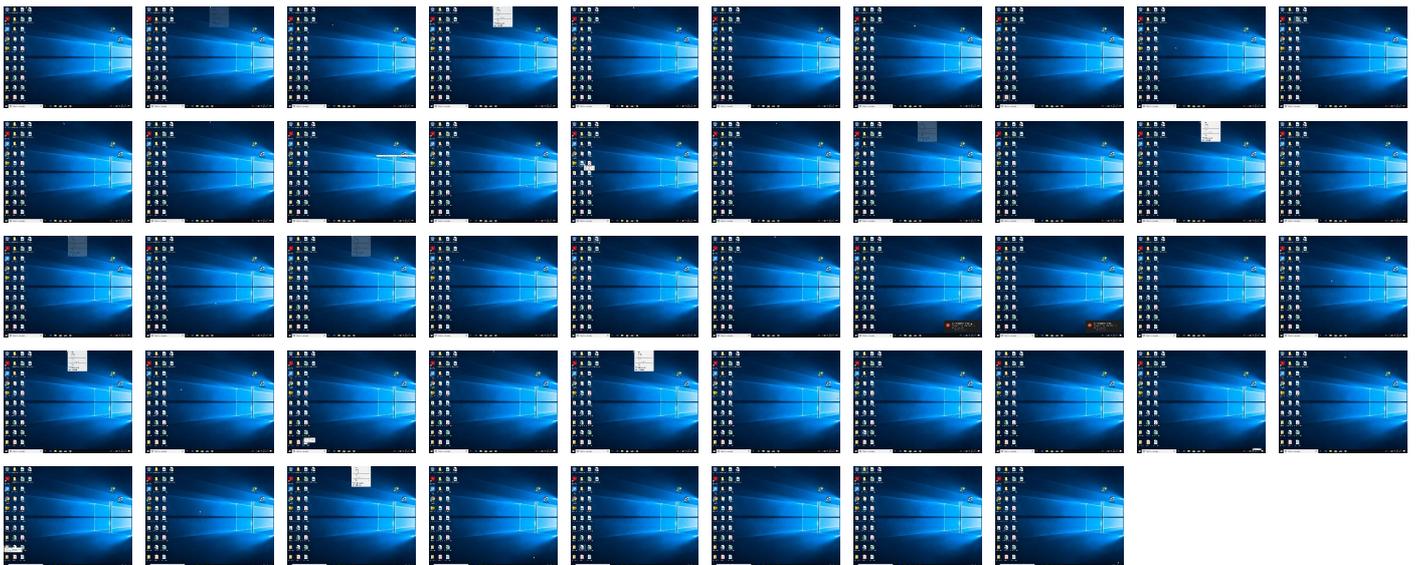
## Behavior Graph



## 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

Source	Detection	Scanner	Label	Link
n#U00ba410000512664.exe	100%	Joe Sandbox ML		

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

Source	Detection	Scanner	Label	Link
http://topqualityfreeware.com	0%	Virustotal		<a href="#">Browse</a>
http://topqualityfreeware.com	0%	Avira URL Cloud	safe	
http://www.topqualityfreeware.com/	0%	Virustotal		<a href="#">Browse</a>
http://www.topqualityfreeware.com/	0%	Avira URL Cloud	safe	

## Domains and IPs

### Contacted Domains

No contacted domains info

### URLs from Memory and Binaries

### Contacted IPs

No contacted IP infos

## General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526313
Start date:	22.11.2021
Start time:	14:04:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	n#U00ba410000512664.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:	27
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:	mal68.troj.evad.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 54.1% (good quality ratio 41%)</li><li>• Quality average: 47.9%</li><li>• Quality standard deviation: 35%</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\~DFE27628A3FBE5D858.TMP	
Process:	C:\Users\user\Desktop\n#U00ba410000512664.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	4.01191323271951
Encrypted:	false
SSDEEP:	384:wcZ0tADSVIx6JQhynrV7Vr9wrCIM/ZUYVPzBAPN:wcZeADSV/6qhynrV7VxwrrMvqPN
MD5:	6C4C01A4316CD9338DE51EC175EBF11D
SHA1:	8C5D5B07E0ED6AAC72705F516E25BEA891EFA0
SHA-256:	95876F7C1242672418DB201C02D70276EE9CC4345394DEAD3500619A39DA28F0
SHA-512:	9F60729E865B0414DB4792F76465EDCE1595D22E884D01C07389A312474D1CE916E4CF73275D5AA0CB411D8EBB0617EF661CD10467AD838FD1B0B388C44823D
Malicious:	false
Reputation:	low
Preview:	.....>..... ..... ..... .....

## Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.926810109816392
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:	n#U00ba410000512664.exe
File size:	192512
MD5:	7c91db57c98a1f0e38ba65ed651b4779

General	
SHA1:	28cb0d40a73c1a421a9720808d49da010f9ff4ef
SHA256:	12992fe3f998693d92625c53bf5aa6723e87c8c3fb7057dbba4b334742cab376
SHA512:	2ca3ac7de708b85262bd7e9d42b0cd78cd0af4f92c1da9c7be9d2e473bcc238a5935030eff688049d8c75fd3c3fd8fd80a5703eca4ab112e3a0997e74d6ac58a
SSDEEP:	3072:tdejCYyLGrRDAfor5hINZI71PAMrc0yvhXeJ:tdeiGrRDAfA5XXMrbbeJ
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$......i..... .....*.....Rich.....PE..L...&T..... 0.....L.....@...@.....

## File Icon

	
Icon Hash:	0ceefedec6f67c0c

## Static PE Info

General	
Entrypoint:	0x40134c
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:	0x54260EAF [Sat Sep 27 01:11:11 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:	f27a613fda76c14f4eab7dc0085d799e

## Entrypoint Preview

## Data Directories

## Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x229ac	0x23000	False	0.354959542411	data	5.0849300681	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x24000	0x13f0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x26000	0x90d5	0xa000	False	0.346411132813	data	4.35437576998	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: n#U00ba410000512664.exe PID: 3232 Parent PID: 5476**

### General

Start time:	14:05:13
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\n#U00ba410000512664.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\n#U00ba410000512664.exe"
Imagebase:	0x400000
File size:	192512 bytes
MD5 hash:	7C91DB57C98A1F0E38BA65ED651B4779
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: 00000000.00000002.781957449.0000000021F0000.00000040.00000001.sdmp, Author: Joe Security</li> </ul>
Reputation:	low

[File Activities](#) Show Windows behavior

## Disassembly

## Code Analysis

