

JoeSandbox Cloud BASIC



**ID:** 457991

**Sample Name:** Documentos de  
env#U00edo.exe

**Cookbook:** default.jbs

**Time:** 16:48:15

**Date:** 02/08/2021

**Version:** 33.0.0 White Diamond

## Table of Contents

Table of Contents	2
Windows Analysis Report Documentos de env#U00edo.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
System Summary:	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	7
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static PE Info	8
General	8
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Code Manipulations	9
Statistics	9
System Behavior	10
Analysis Process: Documentos de env#U00edo.exe PID: 5064 Parent PID: 5556	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

# Windows Analysis Report Documentos de env#U00edo....

## Overview

### General Information

Sample Name:

Documentos de env#U00edo.exe

Analysis ID:

457991

MD5:

a60166d50572ee..

SHA1:

0b5c5afd46ab950.


SHA256:

8a714868cf6bea9.

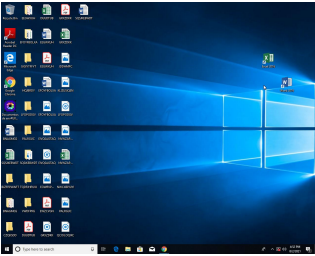
Tags:

exe

Infos:



Most interesting Screenshot:



### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

92

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

### Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Yara detected GuLoader

C2 URLs / IPs found in malware con...

Contains functionality to detect hard...

Detected RDTSC dummy instruction...

Executable has a suspicious name (...)

Found potential dummy code loops (...)

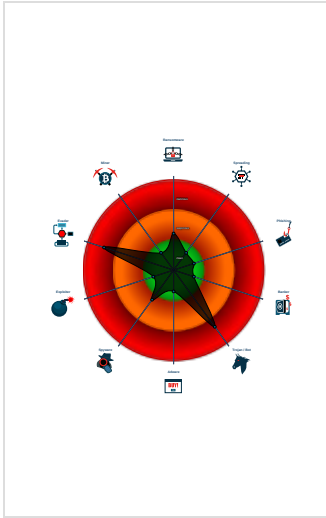
Initial sample is a PE file and has a ...

Tries to detect virtualization through...

Abnormal high CPU Usage


Contains functionality for execution ...

### Classification



## Process Tree

System is w10x64

 Documentos de env#U00edo.exe (PID: 5064 cmdline: 'C:\Users\user\Desktop\Documentos de env#U00edo.exe' MD5: A60166D50572EEDC2E44B327E4928324)

cleanup

## Malware Configuration

Threatname: GuLoader

{

"Payload URL": "https://drive.google.com/uc?exportC"

}

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.748823935.0000000002B6 0000.00000040.00000001.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

## System Summary:



Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

## Data Obfuscation:



Yara detected GuLoader

## Malware Analysis System Evasion:



Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect virtualization through RDTSC time measurements

## Anti Debugging:

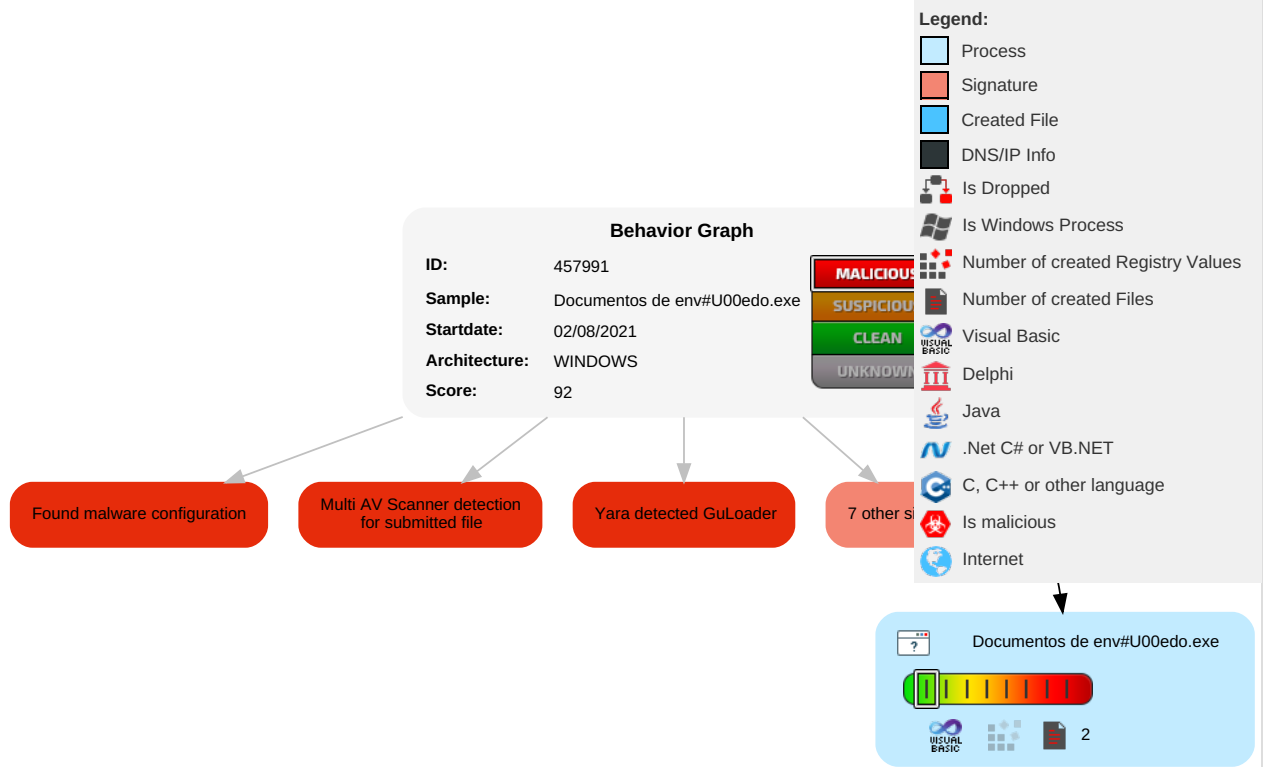


Found potential dummy code loops (likely to delay analysis)

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1 1	Security Software Discovery 4 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
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	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

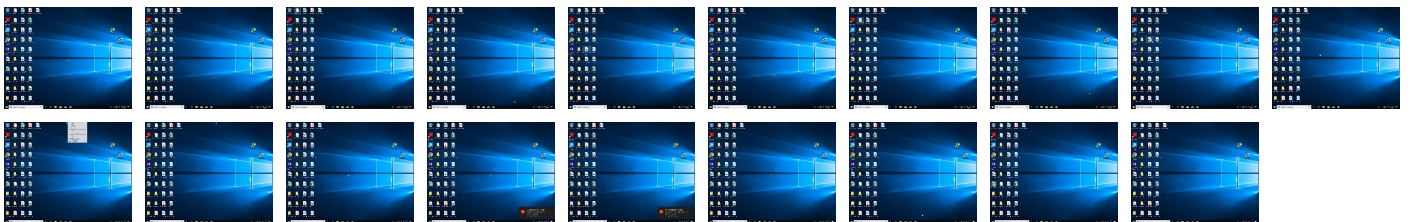
## Behavior Graph



## 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
Documentos de env#U00edo.exe	21%	Virustotal		<a href="#">Browse</a>
Documentos de env#U00edo.exe	7%	ReversingLabs	Win32.Trojan.Mucc	

### 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:	33.0.0 White Diamond
Analysis ID:	457991
Start date:	02.08.2021
Start time:	16:48:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Documentos de env#U00edo.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:	28
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:	mal92.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 5.1% (good quality ratio 2.3%)</li><li>• Quality average: 25%</li><li>• Quality standard deviation: 30.8%</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

No created / dropped files found

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.37444232902198
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:	Documentos de env#U00edo.exe
File size:	143360
MD5:	a60166d50572eedc2e44b327e4928324
SHA1:	0b5c5afd46ab950959dc1e5fda5520ddae0c51a4
SHA256:	8a714868cf6bea9d1a01154cc98fa33abbe75350f06cf26d31538ed0aba6a808
SHA512:	b3ff28a846c6f0c7f7d54ea3c485be76b76f1d49b497ea79c145b4d2e0b53806d6a254e2b7e6931612fc688874ec85b03e7c50f405f638a18b94394ad111d81c
SSDEEP:	3072:W5CFYJr2EF82w1+AG+TeMn5+oXdFv1x9:PHEbLEzhNFv
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode...\$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...u..NY.....0.....@.....

File Icon

	
Icon Hash:	c4e8c8ccce0e8e8

Static PE Info

General	
Entrypoint:	0x4014b4



General

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:	0x594EF175 [Sat Jun 24 23:10:45 2017 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:	fef384fc3a66a559dff455f07d497ca0

Entrypoint Preview

Data Directories

Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1facc	0x20000	False	0.381553649902	data	6.66782218684	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x21000	0x11bc	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x23000	0xc1c	0x1000	False	0.313720703125	data	3.27540208335	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
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

## System Behavior

Analysis Process: Documentos de env#U00edo.exe PID: 5064 Parent PID: 5556

### General

Start time:	16:49:04
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\Documentos de env#U00edo.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Documentos de env#U00edo.exe'
Imagebase:	0x400000
File size:	143360 bytes
MD5 hash:	A60166D50572EEDC2E44B327E4928324
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: 00000001.00000002.748823935.0000000002B60000.00000040.00000001.sdmp, Author: Joe Security</li></ul>
Reputation:	low

### File Activities

Show Windows behavior

## Disassembly

### Code Analysis