

JOeSandbox Cloud BASIC



**ID:** 433003

**Sample Name:** Facturas  
Pagadas al Vencimiento 6.exe

**Cookbook:** default.jbs

**Time:** 04:49:17

**Date:** 11/06/2021

**Version:** 32.0.0 Black Diamond



## Table of Contents

Table of Contents	2
Analysis Report Facturas Pagadas al Vencimiento 6.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
Initial Sample	3
Sigma Overview	3
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	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	8
Static PE Info	8
General	9
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	10
System Behavior	10
Analysis Process: Facturas Pagadas al Vencimiento 6.exe PID: 4628 Parent PID: 5696	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

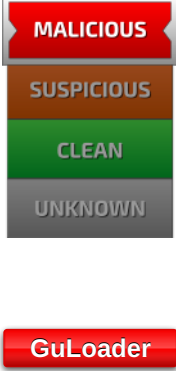
# Analysis Report Facturas Pagadas al Vencimiento 6.exe

## Overview

### General Information

Sample Name:	Facturas Pagadas al Vencimiento 6.exe
Analysis ID:	433003
MD5:	78c3e32a156e44..
SHA1:	02f175cb27dcf85..
SHA256:	4d1b07efb6e87b7.
Infos:	
Most interesting Screenshot:	

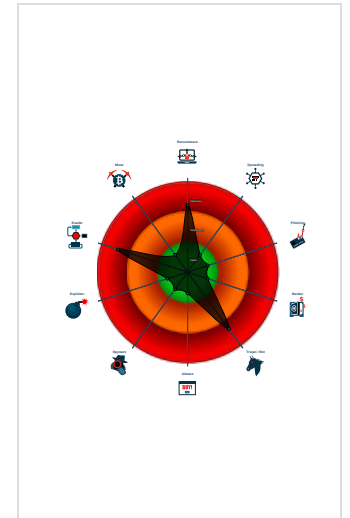
### Detection

	
Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

### Signatures

Found malware configuration
Multi AV Scanner detection for subm...
Potential malicious icon found
Yara detected GuLoader
C2 URLs / IPs found in malware con...
Contains functionality to detect hard...
Detected RDTSC dummy instruction...
Found potential dummy code loops (...)
Tries to detect virtualization through...
Abnormal high CPU Usage
Contains functionality for execution ...
Contains functionality to read the PEB

### Classification



## Process Tree

- System is w10x64
-  Facturas Pagadas al Vencimiento 6.exe (PID: 4628 cmdline: 'C:\Users\user\Desktop\Facturas Pagadas al Vencimiento 6.exe' MD5: 78C3E32A156E44865FCDF53B4783265B)
- cleanup

## Malware Configuration

### Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1ZXsoOW_y-1MUyiIhdh0WNmzZqI-by8yY"
}
```

## Yara Overview

### Initial Sample

Source	Rule	Description	Author	Strings
Facturas Pagadas al Vencimiento 6.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

## Sigma Overview

No Sigma rule has matched

## Signature Overview

## AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

## Networking:



C2 URLs / IPs found in malware configuration

## System Summary:



Potential malicious icon found

## 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:

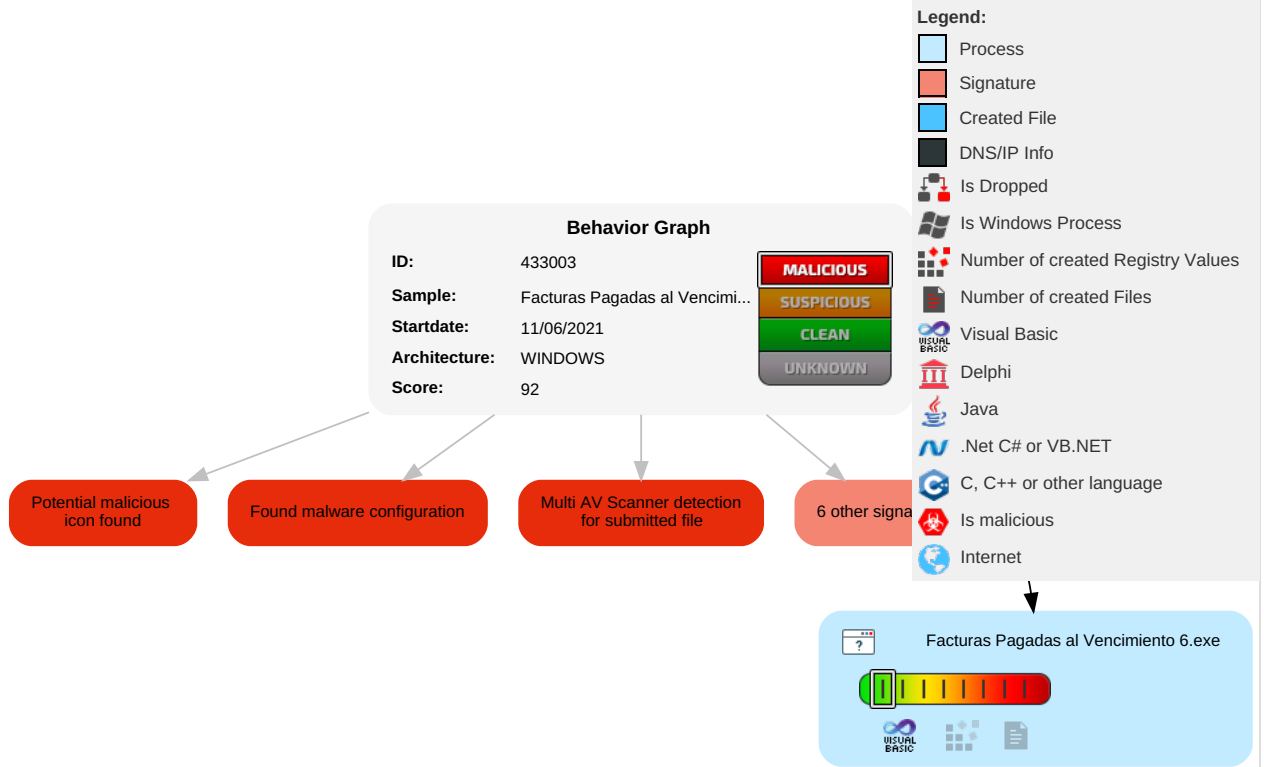


Found potential dummy code loops (likely to delay analysis)

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 4 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	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	Recovery
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	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

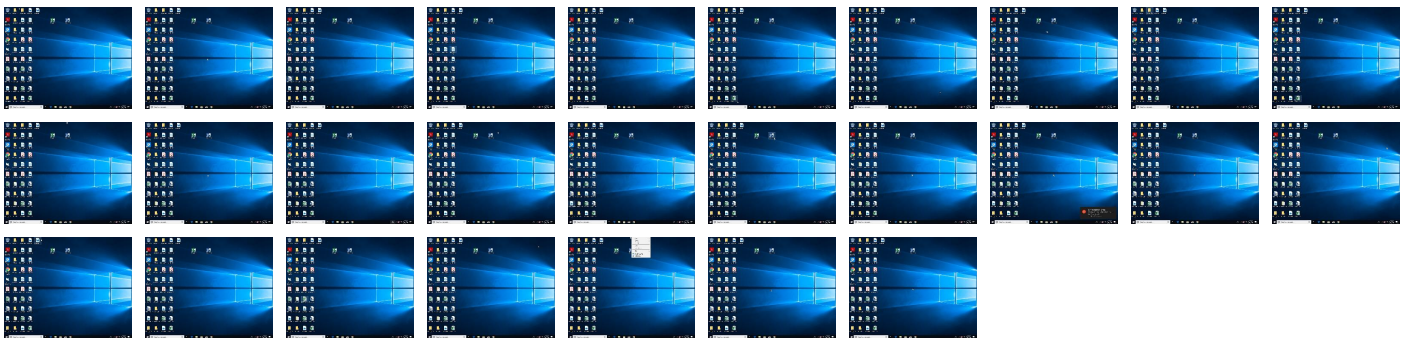
## Behavior Graph



## 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
Facturas Pagadas al Vencimiento 6.exe	51%	Virustotal		<a href="#">Browse</a>
Facturas Pagadas al Vencimiento 6.exe	43%	Metadefender		<a href="#">Browse</a>
Facturas Pagadas al Vencimiento 6.exe	79%	ReversingLabs	Win32.Trojan.Graftor	

### 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:	32.0.0 Black Diamond
Analysis ID:	433003
Start date:	11.06.2021
Start time:	04:49:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Facturas Pagadas al Vencimiento 6.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:	31
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.rans.troj.evad.winEXE@1/0@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: 6% (good quality ratio 0%)</li><li>• Quality average: 1.8%</li><li>• Quality standard deviation: 4.2%</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):	4.463177731670157
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:	Facturas Pagadas al Vencimiento 6.exe
File size:	135168
MD5:	78c3e32a156e44865cdf53b4783265b
SHA1:	02f175cb27dcf85b810f40d3c0adc66de1467ca0
SHA256:	4d1b07efb6e87b7c1379cf8f9eacef7443c54a57ab8e9d50c98053193316fd91
SHA512:	18fa858551003d425d3dc71e80fee12c6eb77bef6bcb1961212457e0b85c335ce757c6ae13c07ad90b14d337d009b648c71254f5610953ca2897ed56d4e2bfe9
SSDEEP:	1536:v9J+koly03uySeJTFsn9FQsZ57DuAPxEISnEtG8z:vP+ko3ytF2nQa5Nzs
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..._Q.`..... .....0.....@.....

### File Icon

	
Icon Hash:	20047c7c70f0e004

### Static PE Info



<b>General</b>	
Entrypoint:	0x4014bc
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:	0x60BD515F [Sun Jun 6 22:51:11 2021 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:	54ea68151857c1f30c42224007018bf1

Entrypoint Preview

Data Directories

Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1dcf8	0x1e000	False	0.334098307292	data	4.72155519745	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1f000	0x1230	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x21000	0x9b8	0x1000	False	0.17822265625	data	2.11732977417	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
Sesotho (Sutu)	South Africa	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Facturas Pagadas al Vencimiento 6.exe PID: 4628 Parent PID: 5696

General

Start time:	04:50:01
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\Facturas Pagadas al Vencimiento 6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Facturas Pagadas al Vencimiento 6.exe'
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	78C3E32A156E44865FCDF53B4783265B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis