ID: 491983
Sample Name: FACTURA.exe
Cookbook: default.jbs
Time: 08:46:57
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report FACTURA.exe

Overview

General Information

Sample Name:	FACTURA.exe
Analysis ID:	491983
MD5:	dbe61cfd43c9575..
SHA1:	71b7f9ea7778a67.
SHA256:	7194eca2c497f9e..
Tags:	exe GuLoader
Infos:	🔍 ⬇️ ⚙️ HCA
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 …

PE file contains strange resources

Contains functionality to read the PEB

Uses code obfuscation techniques (…

Detected potential crypto function

Classification
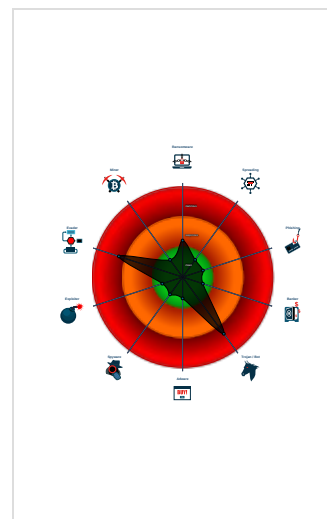
Process Tree

- **System is w10x64**
  - 🖼️ FACTURA.exe (PID: 3092 cmdline: 'C:\Users\user\Desktop\FACTURA.exe' MD5: DBE61CFD43C95752F6DFBDE236558782)
- **cleanup**

Malware Configuration

Threatname: GuLoader

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.825566947.0000000002AD 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

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements
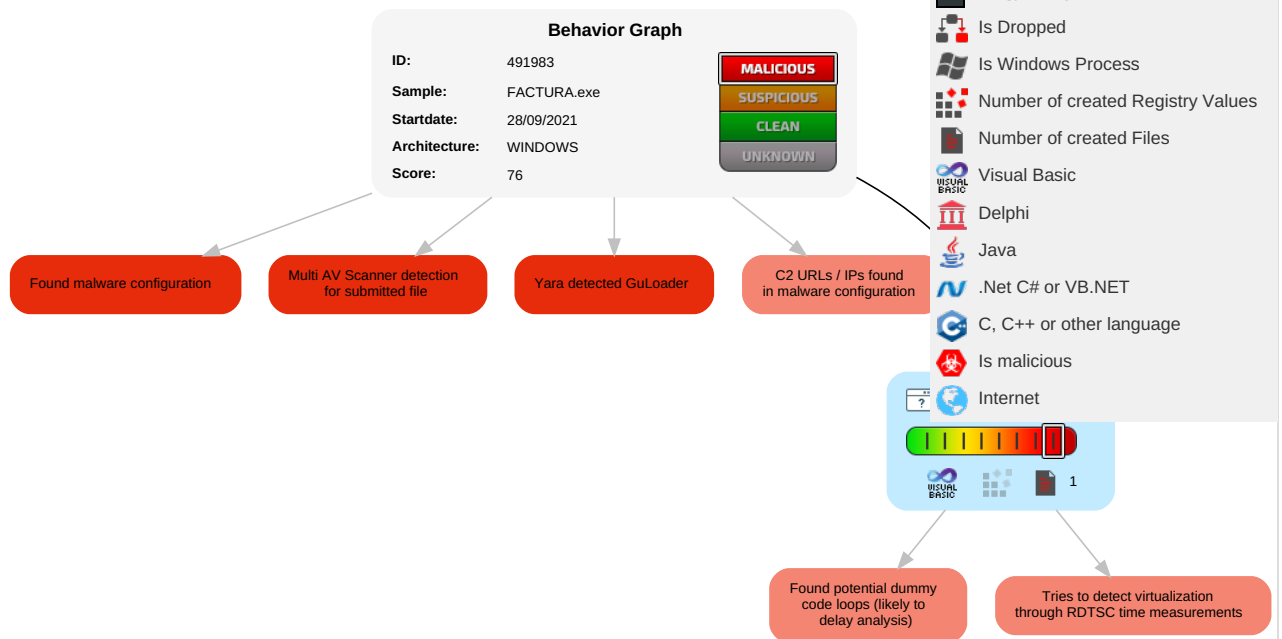
Anti Debugging:

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	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	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	R T W A
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	R W A
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	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph

Behavior Graph

ID: 491983
Sample: FACTURA.exe
Startdate: 28/09/2021
Architecture: WINDOWS
Score: 76

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected GuLoader

C2 URLs / IPs found in malware configuration

Found potential dummy code loops (likely to delay analysis)

Tries to detect virtualization through RDTSC time measurements

Legend:

- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet
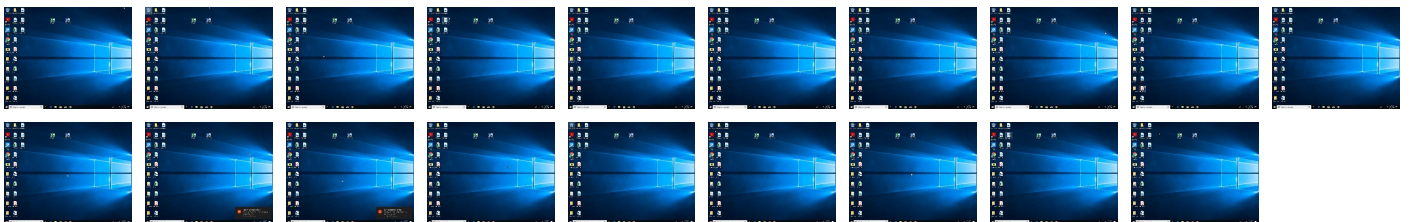
1

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
FACTURA.exe	25%	Virustotal		Browse
FACTURA.exe	27%	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:	491983
Start date:	28.09.2021
Start time:	08:46:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FACTURA.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:	18
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:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	- Successful, ratio: 28.4% (good quality ratio 14.8%) - Quality average: 29.2% - Quality standard deviation: 33.4%
HCA Information:	Failed
Cookbook Comments:	- Adjust boot time - Enable AMSI - Found application associated with file extension: .exe - Override analysis time to 240s for sample files taking high CPU consumption
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):	5.825848109421746
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	FACTURA.exe
File size:	90112
MD5:	dbe61cfd43c95752f6dfbde236558782
SHA1:	71b7f9ea7778a67ffc75fa0f7d8a74dc243aae22
SHA256:	7194eca2c497f9ea9c3bb989fb7f328d9740b6d396af39ec66ec730c0db61044
SHA512:	080df78e19db66f774e4924875da9301fdfb164563b32e3bbf3e32ef720de2d146e2e67f7752eea5ac1d30c64f81209a9b52a1d3a48009402e9f5b91b41226c7
SSDEEP:	768:t2FgA8P1DadQOyLO/j5RhgmDSXlqhZLkVYC5OEn7m7j1Oavx6aG7Cj7nFytQ:t2AP1msO7ZgmDSVq7VUIIj1jJ6nm7/
File Content Preview:	MZ.....................@...................................!..L.!This program cannot be run in DOS mode....$.........i..................*.............Rich....................PE..L....l.Y.................0... ....@....@........

File Icon

Icon Hash:	821ca88c8e8c8c00

Static PE Info

General

Entrypoint:	0x4012c8

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:	0x59A36C05 [Mon Aug 28 01:04:05 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:	e73b8c032c82c64991ebe487a7ffcd43

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x12e4c	0x13000	False	0.52587890625	data	6.31843765659	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x14000	0xcf4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x15000	0x548	0x1000	False	0.132080078125	data	1.43485201544	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

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: FACTURA.exe PID: 3092 Parent PID: 3248

General

Start time:	08:47:58
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\FACTURA.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\FACTURA.exe'
Imagebase:	0x400000
File size:	90112 bytes
MD5 hash:	DBE61CFD43C95752F6DFBDE236558782
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.825566947.0000000002AD0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 33.0.0 White Diamond