ID: 539419
Sample Name: FACTURAS.exe
Cookbook: default.jbs
Time: 09:38:19
Date: 14/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

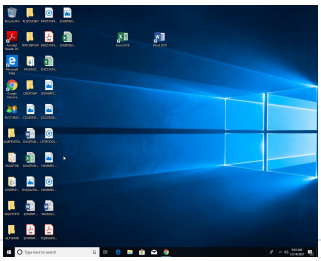
Windows Analysis Report FACTURAS.exe

Overview

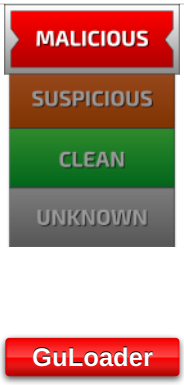
General Information

Sample Name:	FACTURAS.exe
Analysis ID:	539419
MD5:	2332fdde9344114.
SHA1:	303c40dd112294..
SHA256:	0e693b9dcb4ccb…
Infos:	

Most interesting Screenshot:



Detection

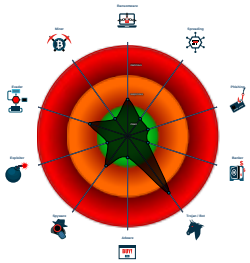


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- Contains functionality to call native f…
- Sample file is different than original …
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…
- Contains functionality for execution …
- Abnormal high CPU Usage

Classification



Process Tree

- **System is w10x64**
- FACTURAS.exe (PID: 6492 cmdline: "C:\Users\user\Desktop\FACTURAS.exe" MD5: 2332FDDE9344114749DB5496EEF5F5F9)
- **cleanup**

Malware Configuration

Threatname: GuLoader

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.862055491.000000000306 0000.00000040.00000001.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

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

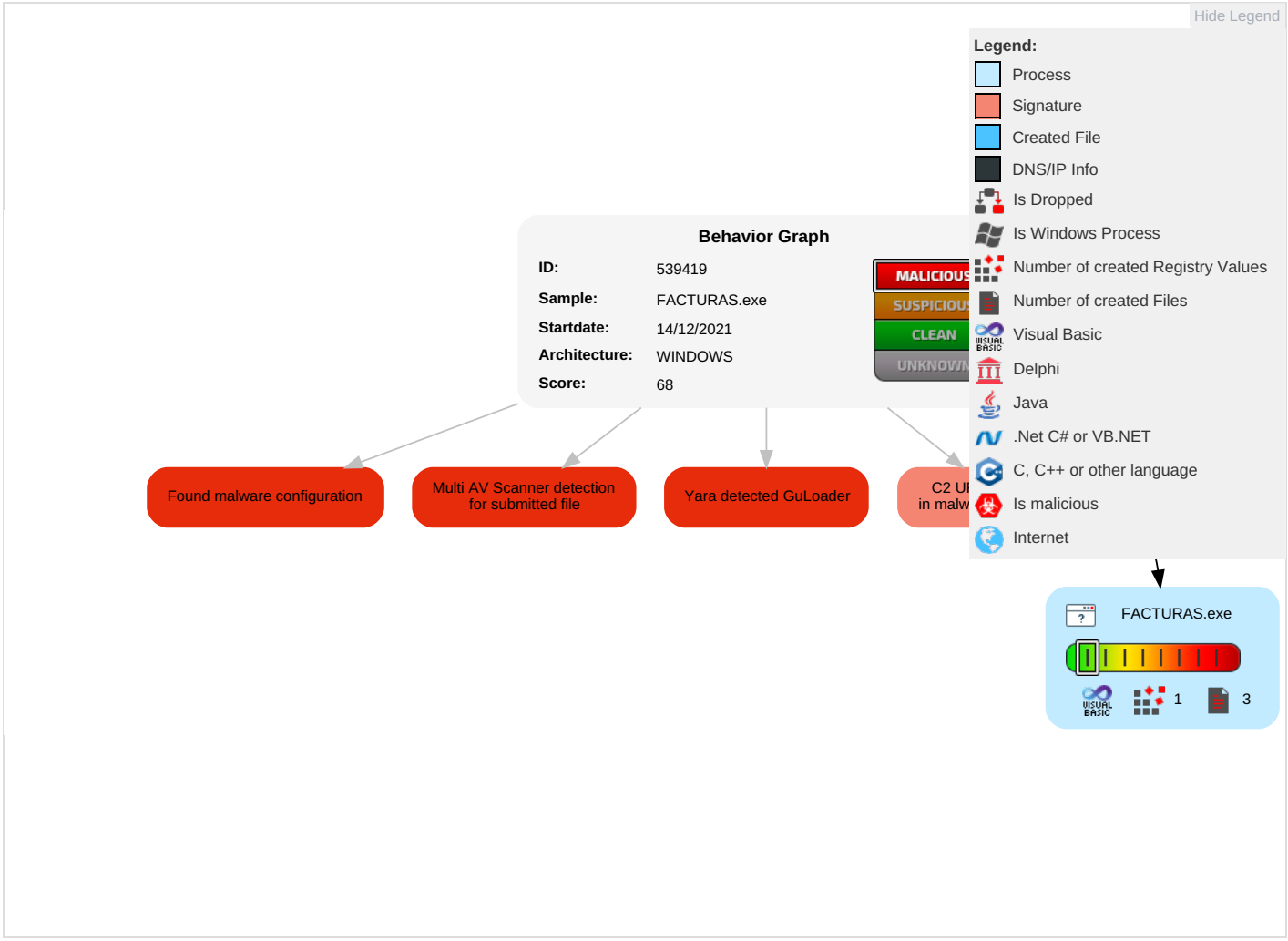
Data Obfuscation:

Yara detected GuLoader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Im
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	Input Capture 1	Security Software Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

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.exe	41%	Virustotal		Browse
FACTURAS.exe	38%	Metadefender		Browse
FACTURAS.exe	58%	ReversingLabs	Win32.Trojan.GuLoader	

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:	539419
Start date:	14.12.2021
Start time:	09:38:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FACTURAS.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:	16
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:	mal68.troj.winEXE@1/2@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 4.1% (good quality ratio 1.6%) • Quality average: 18.8% • Quality standard deviation: 26.4%
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

C:\Users\user\AppData\Local\Temp\M9XgMRXaN30mgEl56ja236	
Process:	C:\Users\user\Desktop\FACTURAS.exe
File Type:	data
Category:	dropped
Size (bytes):	4
Entropy (8bit):	0.8112781244591328
Encrypted:	false
SSDEEP:	3:1ln:v
MD5:	34F45818F16D1BBB62BA5874B8814CC7
SHA1:	A454CA483B4A66B83826D061BE2859DD79FF0D6C
SHA-256:	DC765660B06EE03DD16FD7CA5B957E8C805161AC2C4AF28C5A100AB2AB432CA1
SHA-512:	65711C8D556639DDFC14CE292B2415F3A2824D003AF1A530093B8E0B70B695E6C639694B7B90C6750B1129566D9A3784ED274667988D4B227DB2AC9B6CF7548B
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF6CBEB2FF77188695.TMP	
Process:	C:\Users\user\Desktop\FACTURAS.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.365570111635911
Encrypted:	false
SSDEEP:	48:rCXH5P26XpZKfAujEnkmHE+dJ+//iaBnF6UmkM:EHrZedAnjHrMyaL61
MD5:	E5AAF1474D5E7489F86A267B928DE425
SHA1:	8DAC741F82956D6111A5B442442E095DC4FC3299
SHA-256:	DBBEF5EC504CF458770890AF07448ABF835345029D078D4BA36CBF431F86314E
SHA-512:	B9AE66432026ADF7FE691F6E95292C6299CFE37FDC27760AD8DB5464386663A0398E53A770B0C8CCFDD734A8162064FF2D01093197A3BEC7356E9933EC344961
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.04128986675064
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:	FACTURAS.exe
File size:	147456
MD5:	2332fdde9344114749db5496eef5f5f9
SHA1:	303c40dd112294dc012836be48eb38e8af056432
SHA256:	0e693b9dcb4ccb3e64cb61396447dd4e3871234b4af80c2d57e4fbc9b6268a61
SHA512:	7b3d94fb5e12a09f1b417e8042cbb0abe394a1d577a466cd2394e9aa0068ab276d5da25edf742660edb8bd01611f480c982d6f14373d80e2896d34a887379c1
SSDEEP:	1536:nVas/8YOk4FOHBbmpBpQr9nV43XExeM0Jw52P3u1D6CqljbW:Is/8YJ4kRmpBpqVC090JS63hN
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L....e`V.....0..... ....@.....

File Icon

Icon Hash:	0cceececceece400

Static PE Info

General

Entrypoint:	0x401698
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:	0x566065B6 [Thu Dec 3 15:54:30 2015 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:	98b6dd560a57b8960045d82e7d77c431

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20638	0x21000	False	0.363976680871	data	5.21775436592	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1238	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x24000	0xc6c	0x1000	False	0.484130859375	data	4.2105621782	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
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: FACTURAS.exe PID: 6492 Parent PID: 5852

General

Start time:	09:39:39
Start date:	14/12/2021
Path:	C:\Users\user\Desktop\FACTURAS.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\FACTURAS.exe"
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	2332FDDE9344114749DB5496EEF5F5F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.862055491.0000000003060000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis