JOE Sandbox Cloud BASIC

ID: 432966
Sample Name: FACTURA Y
ALBARANES (2).exe
Cookbook: default.jbs
Time: 01:43:23
Date: 11/06/2021
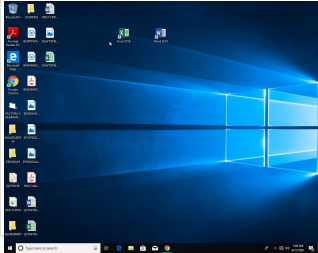**Version:** 32.0.0 Black Diamond

Table of Contents

Analysis Report FACTURA Y ALBARANES (2).exe

Overview

General Information

Sample Name:	FACTURA Y ALBARANES (2).exe
Analysis ID:	432966
MD5:	0a2ce5a915bf643.
SHA1:	21a26264df4f615..
SHA256:	5a5428877719d2..
Infos:	🔍 ⚙️ HCA

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…

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 call native f…

Classification
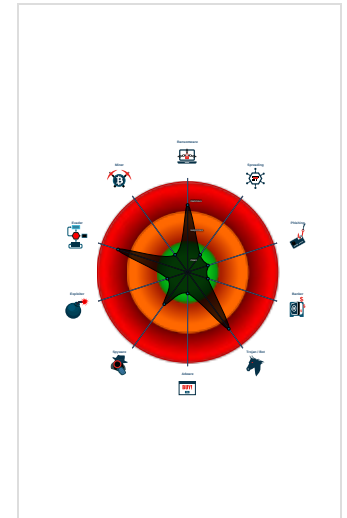
Process Tree

- **System is w10x64**
- 📁 FACTURA Y ALBARANES (2).exe (PID: 6036 cmdline: 'C:\Users\user\Desktop\FACTURA Y ALBARANES (2).exe' MD5: 0A2CE5A915BF643953BAF2FCF3B25A5E)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
    "Payload URL": "https://drive.google.com/uc?export=download&id=10cWvVkUqjSi-M-x6hHokSklVF3h_YX3c"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
FACTURA Y ALBARANES (2).exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

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

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	Re Se Ef
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 4 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
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	Re W Au
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	Ob De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph

Behavior Graph

ID: 432966

Sample: FACTURA Y ALBARANES (2).exe

Startdate: 11/06/2021

Architecture: WINDOWS

Score: 92

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

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

Hide Legend

Potential malicious icon found

Found malware configuration

Multi AV Scanner detection for submitted file

6 other sig

FACTURA Y ALBARANES (2).exe

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.
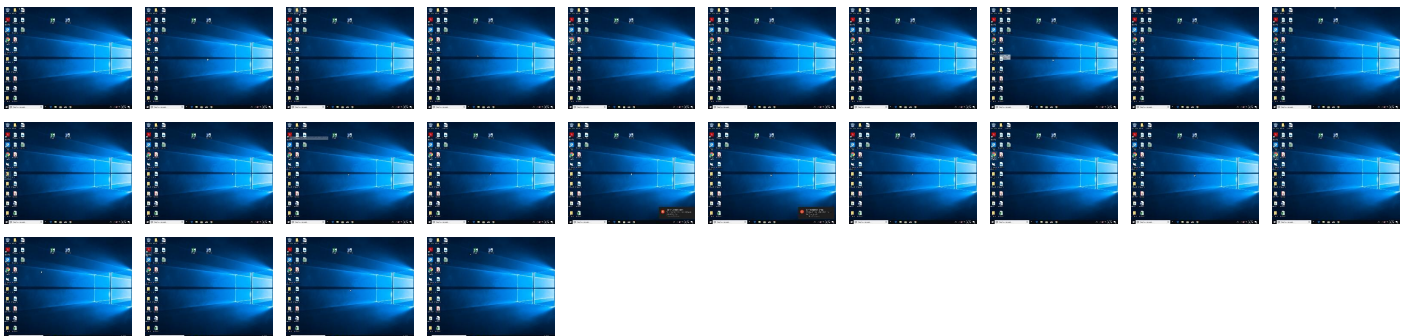
Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
FACTURA Y ALBARANES (2).exe	59%	Virustotal		Browse
FACTURA Y ALBARANES (2).exe	40%	Metadefender		Browse
FACTURA Y ALBARANES (2).exe	86%	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:	32.0.0 Black Diamond
Analysis ID:	432966
Start date:	11.06.2021
Start time:	01:43:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FACTURA Y ALBARANES (2).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:	32
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:	mal92.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Successful, ratio: 100%
HDC Information:	- Successful, ratio: 3.9% (good quality ratio 0.4%) - Quality average: 4% - Quality standard deviation: 6.3%
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):	4.640178061841888
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 Y ALBARANES (2).exe
File size:	143360
MD5:	0a2ce5a915bf643953baf2fcf3b25a5e
SHA1:	21a26264df4f615da898b38ef9332ff66d24b505
SHA256:	5a5428877719d24368bc14761dee49adf676fd883abd3a8 c30b84c0b0c7e13f5
SHA512:	9f79397ffdef767bd1d7ae12395be4b9172b556e6626b08 11a22670acc645d7367f5dadeb5b1b4007e4c0f1829494d ea55e2d3a28cddc16aa43f43bbab820574
SSDEEP:	3072:CBWkR/6N08mSDea0rRzkaNTBW1NieJHz:CBW kR/E3Tia0RzkaNTBW1NieJ
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......`............. ....0...................@................

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4014b8
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:	0x60BE0213 [Mon Jun 7 11:25:07 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:	b1d5215cf0ff1abab4dacdc311d642d4

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1f70c	0x20000	False	0.333885192871	data	4.89089028239	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x21000	0x1234	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x23000	0xa04	0x1000	False	0.181396484375	data	2.20390073464	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: FACTURA Y ALBARANES (2).exe PID: 6036 Parent PID: 5604

General

Start time:	01:44:08
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\FACTURA Y ALBARANES (2).exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\FACTURA Y ALBARANES (2).exe'
Imagebase:	0x400000
File size:	143360 bytes
MD5 hash:	0A2CE5A915BF643953BAF2FCF3B25A5E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities
Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 32.0.0 Black Diamond