ID: 531838
Sample Name: FACTURAS.exe
Cookbook: default.jbs
Time: 13:16:12
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report FACTURAS.exe

Overview

General Information

Sample Name:	FACTURAS.exe
Analysis ID:	531838
MD5:	ab82f374210a08b.
SHA1:	6a56b815491850..
SHA256:	ab41887e471ac8..
Tags:	exe signed
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

GuLoader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration

Potential malicious icon found

Multi AV Scanner detection for subm…

Yara detected GuLoader

C2 URLs / IPs found in malware con…

Uses 32bit PE files

PE / OLE file has an invalid certificate

Sample file is different than original …

PE file contains strange resources

Contains functionality to read the PEB

Uses code obfuscation techniques (…

Contains functionality for execution …

Classification
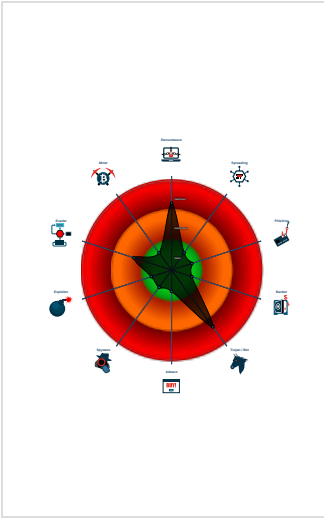
Process Tree

- **System is w10x64**
  - FACTURAS.exe (PID: 6088 cmdline: "C:\Users\user\Desktop\FACTURAS.exe" MD5: AB82F374210A08B2221D5E1807400A32)
  - **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
   "Payload URL": "https://drive.google.com/uc?export=download&id=11UpsPasq_HHoJ"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.822667479.0000000002A8 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

System Summary:

Potential malicious icon found

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	In
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pi
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	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Di L(
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	Di Di Di

Behavior Graph

Behavior Graph

ID: 531838

Sample: FACTURAS.exe

Startdate: 01/12/2021

Architecture: WINDOWS

Score: 76

MALICIO
SUSPICIO
CLEAN
UNKNO

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

Potential malicious icon found

Found malware configuration

Multi AV Scanner detection for submitted file

2 ot

FACTURAS.exe

VISUAL BASIC   1   2
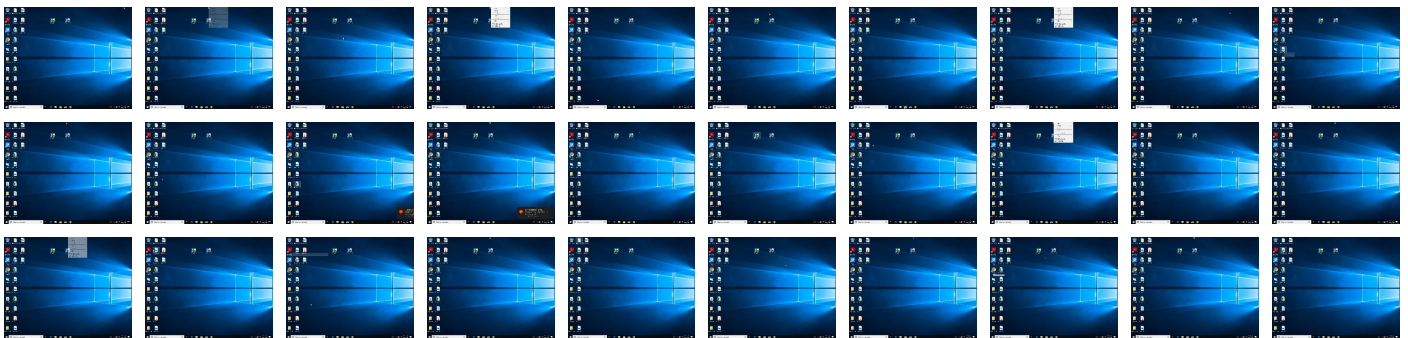
Screenshots

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	13%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.FACTURAS.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140082		Download File
0.0.FACTURAS.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140082		Download File

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:	531838
Start date:	01.12.2021
Start time:	13:16:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 9s
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:	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.rans.troj.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	- Successful, ratio: 8.3% (good quality ratio 4.8%) - Quality average: 37.4% - Quality standard deviation: 34.9%
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):	5.1786714462714025
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:	152720
MD5:	ab82f374210a08b2221d5e1807400a32
SHA1:	6a56b81549185015743deaa196996f73787c5c7d
SHA256:	ab41887e471ac822f1240bf554098fa042910f1c7ac2f9e3 90081829515bc2fa
SHA512:	8844aca394f38a59a63b1984a00b16861a0f7e0fdc04ba2 0aba264da79fc6e54eeb73c6814f0745ab37ba12ba306e6 371561e64f23deac22ba555d75aa3b2019
SSDEEP:	1536:gZEG7DecysKvlp4erYY77BLm321zb2aKQhbHdE s5obasAJepPNp8:6EG7Dpy9nYYn2EzBKYpdOSoNp8
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......O.............. ....D.......=.......Rich............PE..L.....4U..................... 0............... ....@................

File Icon

Icon Hash:		20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401888
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5534C2F5 [Mon Apr 20 09:12:21 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:	b209c8634733456633136bfedc71877a

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=parteringens@Shiremen3.slu, CN=SELSKABSLOKALET, OU=Interimskvitteringerne, O=JUSTITSEN, L=Rutiners, S=honkytonks, C=ML
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 12/1/2021 2:36:44 AM 12/1/2022 2:36:44 AM
Subject Chain	• E=parteringens@Shiremen3.slu, CN=SELSKABSLOKALET, OU=Interimskvitteringerne, O=JUSTITSEN, L=Rutiners, S=honkytonks, C=ML
Version:	3
Thumbprint MD5:	CDDFD4747563B21AE94964F7C6F9EB7A
Thumbprint SHA-1:	1CFBE705D5055A36D357E2EF5F5FE20BC6959CA9
Thumbprint SHA-256:	176B1E7918EE21C3FEADE8CC2C9D049B7DFDE73ECFE288C07CF37C692D0011A0
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20cc4	0x21000	False	0.367520419034	data	5.25414504645	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x122c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x970	0x1000	False	0.173828125	data	2.0476168209	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: FACTURAS.exe PID: 6088 Parent PID: 3324

General

Start time:	13:17:09
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\FACTURAS.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\FACTURAS.exe"
Imagebase:	0x400000
File size:	152720 bytes
MD5 hash:	AB82F374210A08B2221D5E1807400A32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.822667479.0000000002A80000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities   Show Windows behavior

File Created

Registry Activities   Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis