

JoeSandbox Cloud BASIC



ID: 528616

Sample Name: Justificante de
Pago 25112021.pdf_.exe

Cookbook: default.jbs

Time: 15:07:14

Date: 25/11/2021

Version: 34.0.0 Boulder Opal


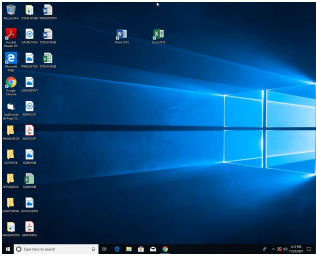
Table of Contents

Table of Contents	2
Windows Analysis Report Justificante de Pago 25112021.pdf _.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
Memory Dumps	3
Sigma Overview	3
Jbx Signature Overview	4
AV Detection:	4
Networking:	4
System Summary:	4
Data Obfuscation:	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 URLs	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	9
General	9
Authenticode Signature	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	10
Code Manipulations	10
Statistics	10
System Behavior	10
Analysis Process: Justificante de Pago 25112021.pdf _.exe PID: 6016 Parent PID: 5364	10
General	10
File Activities	10
Disassembly	10
Code Analysis	11

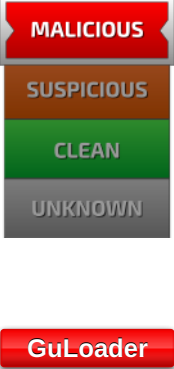
Windows Analysis Report Justificante de Pago 2511202...

Overview

General Information

Sample Name:	Justificante de Pago 25112021.pdf __.exe
Analysis ID:	528616
MD5:	494cd8be1913f9d.
SHA1:	ff74b67fa7c03d4...
SHA256:	75934da02313e0..
Tags:	exe guloader
Infos:	
Most interesting Screenshot:	
	

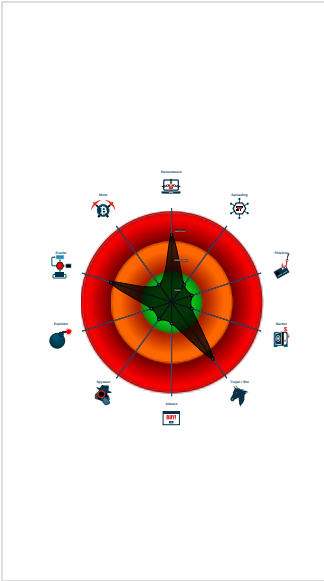
Detection

	
Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%


Signatures

Found malware configuration
Potential malicious icon found
Multi AV Scanner detection for subm...
Yara detected GuLoader
Initial sample is a PE file and has a ...
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
PE / OLE file has an invalid certificate

Classification



Process Tree

- System is w10x64
-  Justificante de Pago 25112021.pdf __.exe (PID: 6016 cmdline: "C:\Users\user\Desktop\Justificante de Pago 25112021.pdf __.exe" MD5: 494CD8BE1913F9DEF79B10031587AA8A)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://onedrive.live.com/download?c"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1185369693.00000000029 80000.00000040.00000001.sdm	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

Initial sample is a PE file and has a suspicious name

Data Obfuscation:



Yara detected GuLoader

Anti Debugging:

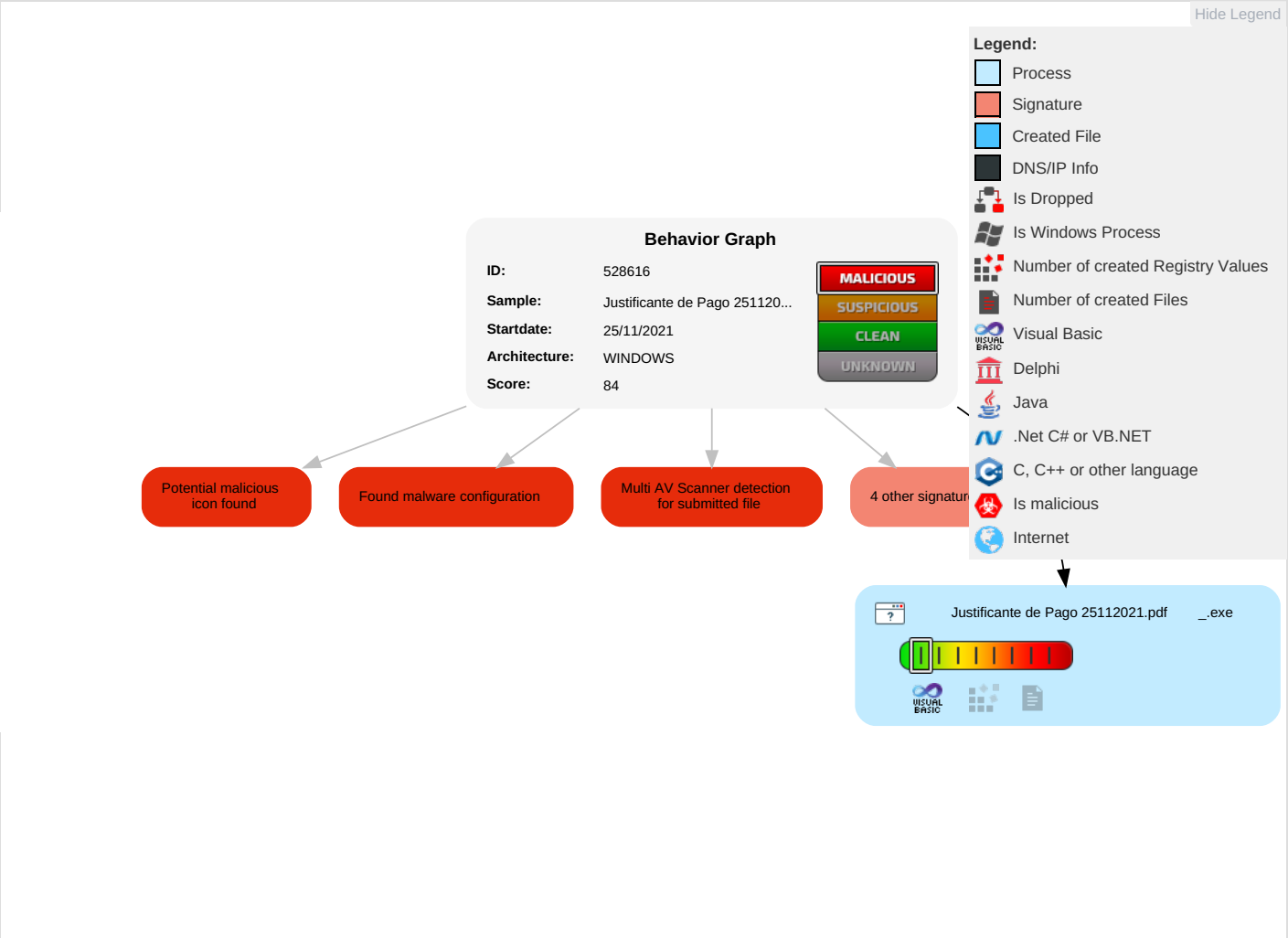


Found potential dummy code loops (likely to delay analysis)

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 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery Time Window Analysis
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 Time Window Analysis
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	Operational Continuity Breach
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Justificante de Pago 25112021.pdf .exe	18%	ReversingLabs	Win32.Trojan.Lazy	

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 URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?c	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528616
Start date:	25.11.2021
Start time:	15:07:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Justificante de Pago 25112021.pdf __.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:	15
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">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 26.5% (good quality ratio 11.6%)• Quality average: 23.1%• Quality standard deviation: 30.7%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">• 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):	6.141971298184264
TrID:	<ul style="list-style-type: none">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:	Justificante de Pago 25112021.pdf __.exe
File size:	148800
MD5:	494cd8be1913f9def79b10031587aa8a
SHA1:	ff74b67fa7c03d4fb388f49289ff14639656b3d3
SHA256:	75934da02313e0d772b4703bfaa3331311fc5a2b981f8ff0e455795bc3448ddb
SHA512:	620ac0b14cfac47728cc1761d6cb9a50d45e1c050c96e8cf069cfb2729fdac8e257fcd07db97c71c536b63646a548d956e9ec4614f703bd7f8b8a6803dea4e4
SSDEEP:	1536:q9aYr5MjHE4q7c4BMoDh9t4ooodRRK7bgNmGT4JVom8D/Qy5gy9LE+YJi3hbh:JYCjH7mc4BMtZ742JV4/Qa4J6h
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode...\$.....,SM..S M..SM...Q..RM...o..UM..ek..RM..RichSM.....PE.. L..._XW.....0.....X.....@.....

File Icon



Icon Hash:	20047c7c70f0e004
------------	------------------

Static PE Info

General

Entrypoint:	0x401578
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:	0x57589F5F [Wed Jun 8 22:42:39 2016 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:	e6bbebdc7c1418bc1bcd0dc8a54e696

Authenticode Signature

Signature Valid:	false
Signature Issuer:	E=Beske7@Udtoemtlif6.opm, CN=Srvvgtere, OU=faringsa, O=Hepa6, L=MODGAAS, S=Dann4, C=NE
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	<ul style="list-style-type: none">11/24/2021 3:02:10 AM 11/24/2022 3:02:10 AM
Subject Chain	<ul style="list-style-type: none">E=Beske7@Udtoemtlif6.opm, CN=Srvvgtere, OU=faringsa, O=Hepa6, L=MODGAAS, S=Dann4, C=NE
Version:	3
Thumbprint MD5:	38CEFA178A560F005C02C0AB1CCD5B2C
Thumbprint SHA-1:	6831094E8AE768575C155840ECA02AE1798897CF
Thumbprint SHA-256:	0577BE6AC49E2682236F51DB9FD872B71506301CDBE61148CA0A74BB6E8C4A4
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1ee24	0x1f000	False	0.46585969002	data	6.32767470182	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x20000	0xc24	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x21000	0x11ce	0x2000	False	0.18798828125	data	2.35454948934	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
--------------------------------	----------------------------------	-----

Language of compilation system	Country where language is spoken	Map
English	United States	
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Justificante de Pago 25112021.pdf _exe PID: 6016 Parent PID: 5364

General

Start time:	15:08:08
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\Justificante de Pago 25112021.pdf _exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Justificante de Pago 25112021.pdf _exe"
Imagebase:	0x400000
File size:	148800 bytes
MD5 hash:	494CD8BE1913F9DEF79B10031587AA8A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none"> Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1185369693.0000000002980000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

