ID: 526293
Sample Name: justificante de la transfer.exe
Cookbook: default.jbs
Time: 13:42:12
Date: 22/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

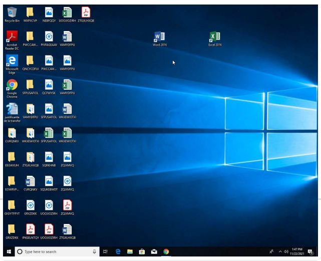
Windows Analysis Report justificante de la transfer.exe

Overview

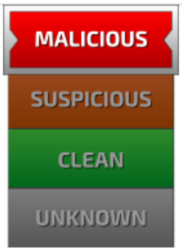
General Information

Sample Name:	justificante de la transfer.exe
Analysis ID:	526293
MD5:	e565201ac69a8a..
SHA1:	fed196aeff9aca5…
SHA256:	b6fad861abae70b.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



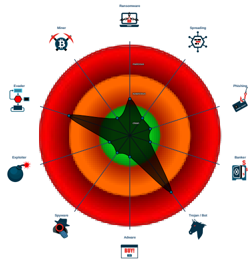
GuLoader

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Found potential dummy code loops (…
- Uses 32bit PE files
- Found a high number of Window / Us…
- 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
- Contains functionality to call native f…

Classification



Process Tree

- System is w10x64
- justificante de la transfer.exe (PID: 6224 cmdline: "C:\Users\user\Desktop\justificante de la transfer.exe" MD5: E565201AC69A8A2FA7EE22E0809F7B3C)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?exporto"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.870508386.000000000228 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

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

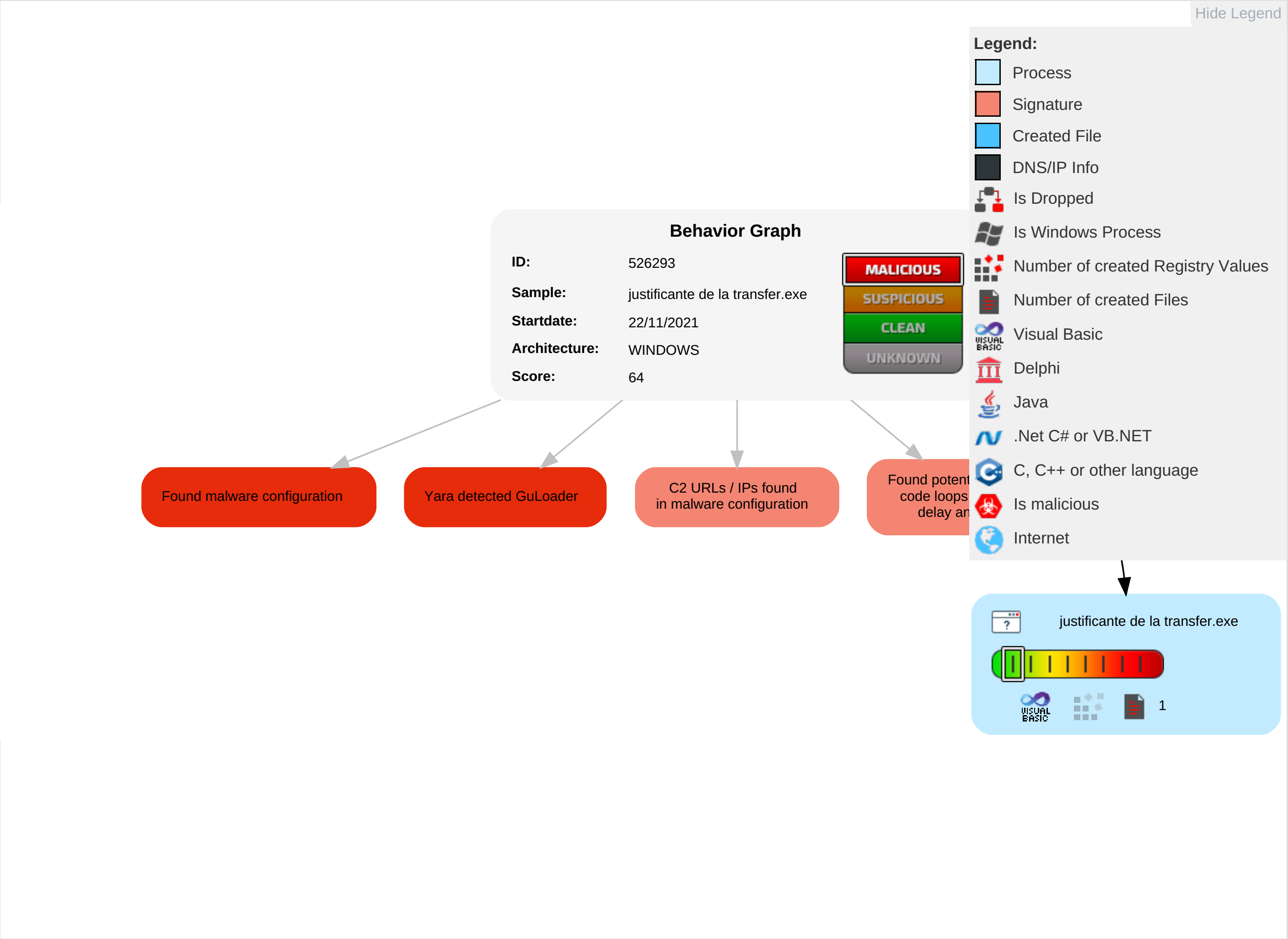
Anti Debugging:

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	R S E
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	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 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	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

Behavior Graph



Behavior Graph

ID: 526293

Sample: justificante de la transfer.exe

Startdate: 22/11/2021

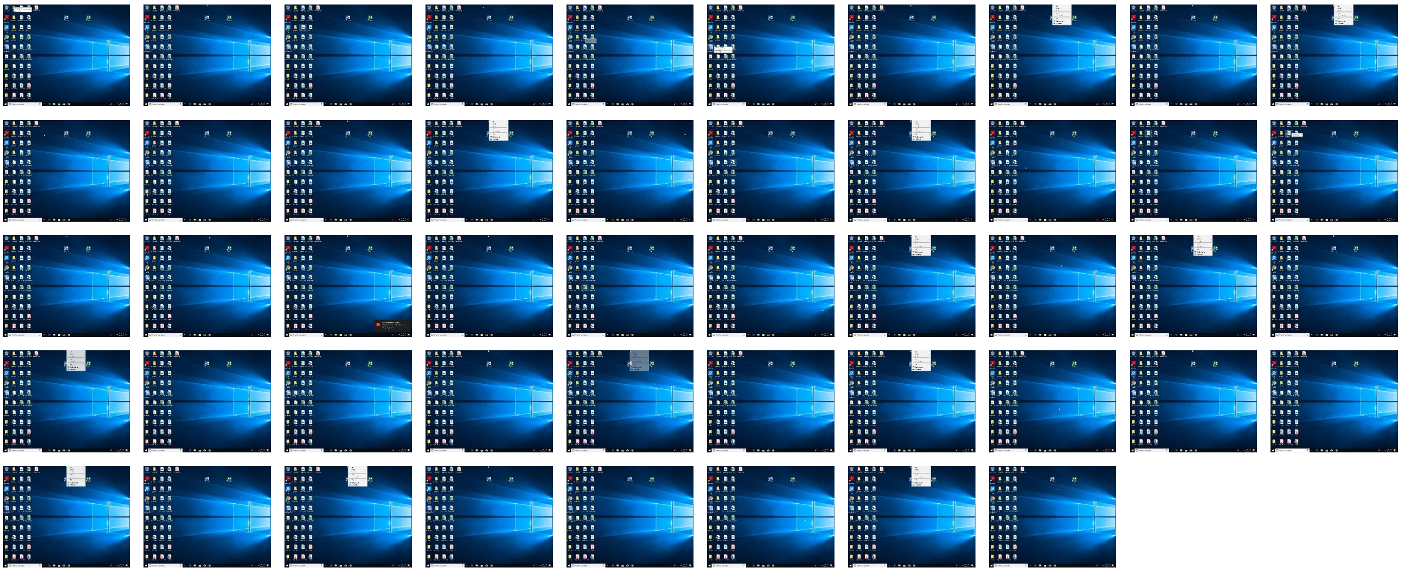
Architecture: WINDOWS

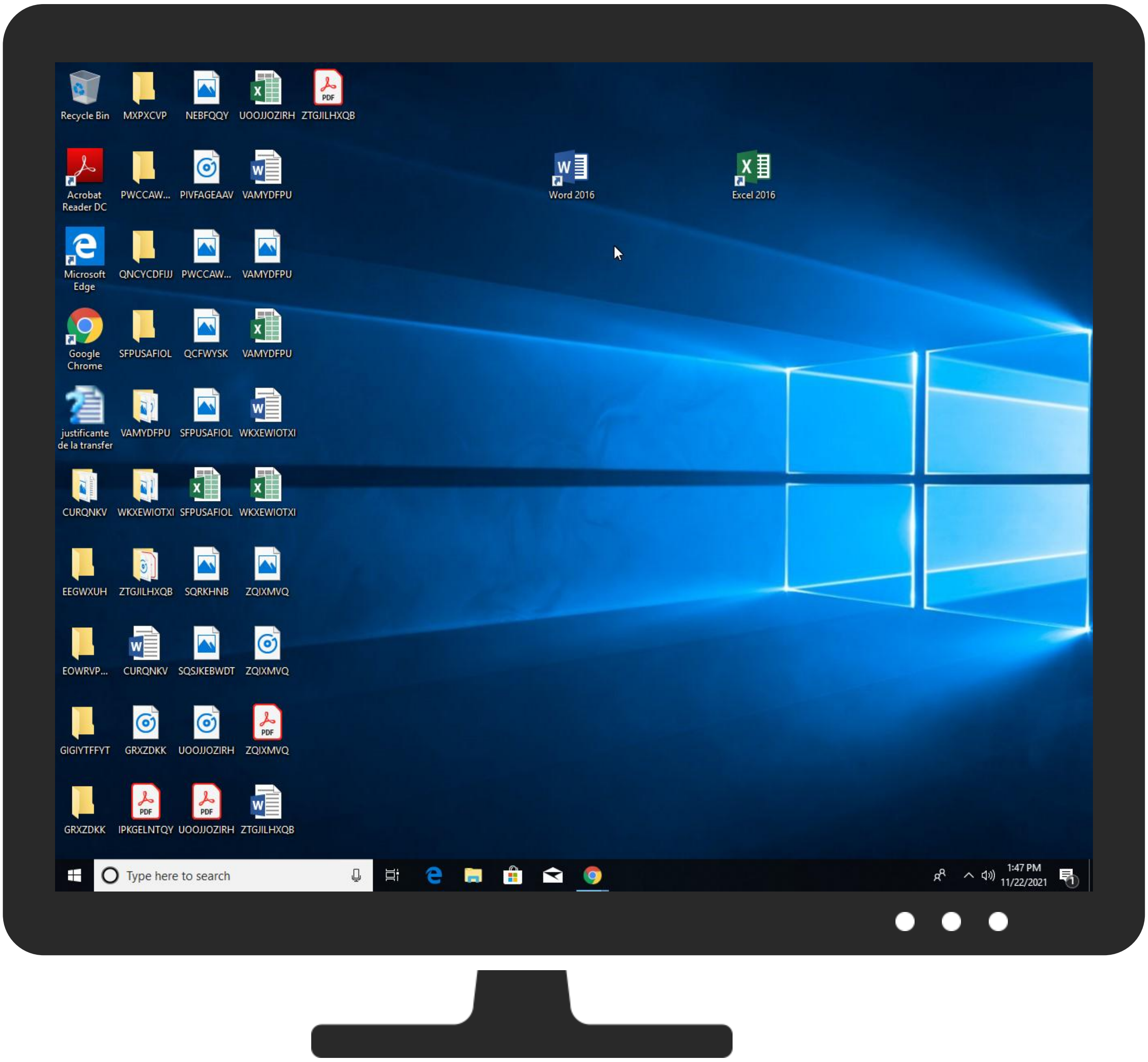
Score: 64

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

No Antivirus matches

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:	526293
Start date:	22.11.2021
Start time:	13:42:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	justificante de la transfer.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:	mal64.troj.evad.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 29.8% (good quality ratio 16.4%) • Quality average: 30.6% • Quality standard deviation: 31.9%
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

C:\Users\user\AppData\Local\Temp\~DFEB935E0BE46A145A.TMP	
Process:	C:\Users\user\Desktop\justificante de la transfer.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.351590352286438
Encrypted:	false
SSDEEP:	48:rSTIhbzrJeuFpbB5KivFyAEcSRRfPD9PPba:7bzrJFFVB5KityAEcSLL9La
MD5:	D3984E0D0AAA56BBDF17314D4CFF0945
SHA1:	C0C7838BB49133CAD3B9DD5DE562DDE05463D379
SHA-256:	2EE69010A71F26BFCFB8DDA0379733605F5A7EE0C91ABB012F766E32C3D94D24
SHA-512:	C81FA9FCCAB4DD2984E1BD27C76D253EB667115A65475FAD5A7D2EBB726376BB048E4795EB2F79FEF386B06547EF976D762899CA1EAB0026656254E3A506294
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......................>.. ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.187050367832804
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:	justificante de la transfer.exe
File size:	286720
MD5:	e565201ac69a8a2fa7ee22e0809f7b3c
SHA1:	fed196aeff9aca57c198b0b99a9c9bc6e01d31b9
SHA256:	b6fad861abae70b69d7f0ef4e51756b181149e165ada09aee47e3d2bd5f9a0c6
SHA512:	b40afaa6d2f831ef3ec0f8170cc0fa2d8cb8be978861613f0f1149451ad06c4e75e6cb9341ce7ee2173f0bff87c92d1eab6cc0b0584c03174860cc47825d6e24
SSDEEP:	3072:KUDFBR3qusY6Ric7RnqRNiY61rsS1IHK2looQkoW2nLEHHDSG:H5B1R6Riyci4GUFf2noH

General

File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........6...W...W...W...K...W...u...W...q...W..Rich.W..........................PE..L.....OS.................0... ....@....@

File Icon

Icon Hash:	f89ea9acb4b0b092

Static PE Info

General

Entrypoint:	0x4013fc
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:	0x534FFE1F [Thu Apr 17 16:15:27 2014 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:	d7d4adb5e5d083da305ede89b87ddf22

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x42204	0x43000	False	0.333820399953	data	6.29830429337	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x44000	0xd78	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x45000	0xdbe	0x1000	False	0.4873046875	data	4.27786524894	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: justificante de la transfer.exe PID: 6224 Parent PID: 3628

General

Start time:	13:43:11
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\justificante de la transfer.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\justificante de la transfer.exe"
Imagebase:	0x400000
File size:	286720 bytes
MD5 hash:	E565201AC69A8A2FA7EE22E0809F7B3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.870508386.0000000002280000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal