ID: 491606
Sample Name: GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe
Cookbook: default.jbs
Time: 18:35:52
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

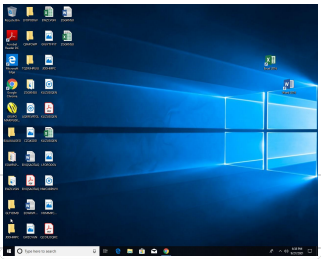
Windows Analysis Report GRUPO MARI#U00d1O OBRA…

Overview

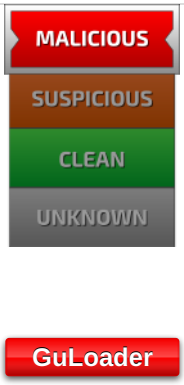
General Information

Sample Name:	GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe
Analysis ID:	491606
MD5:	917a78f3605abfd..
SHA1:	c753e171b3ef5b9.
SHA256:	03e08e44d9df2a0.
Tags:	exe guloader
Infos:	

Most interesting Screenshot:



Detection

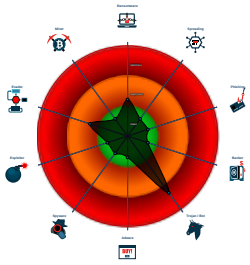


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to read the PEB
- Program does not show much activi…
- Uses code obfuscation techniques (…
- Contains functionality for execution …
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe (PID: 5148 cmdline: 'C:\Users\user\Desktop\GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe' MD5: 917A78F3605ABFDA3674FE5264A721E9)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1qlA"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.514140065.00000000021F0000.00000040.00000001.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

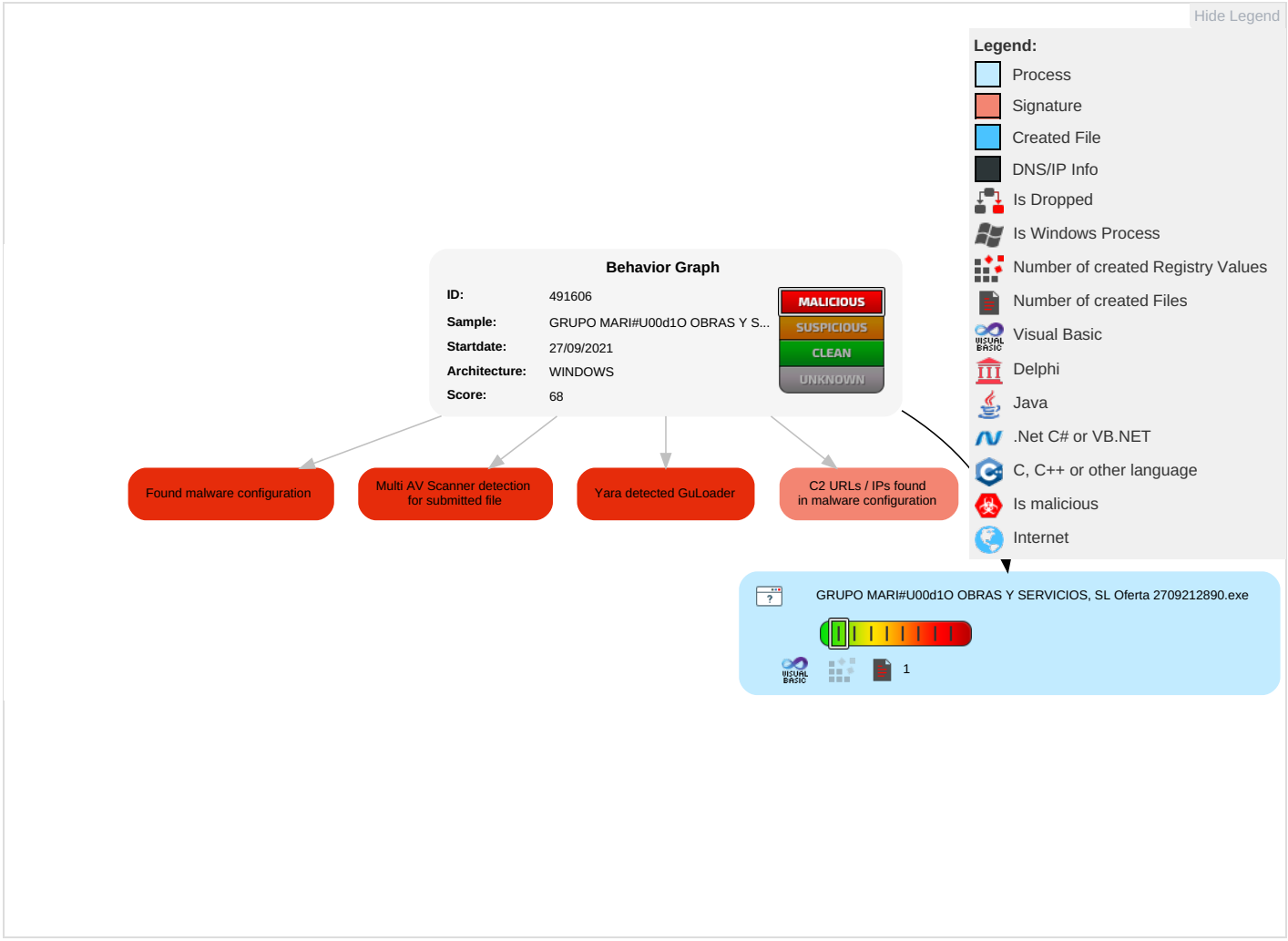
Data Obfuscation:

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	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Process Injection 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	Modi Syst Parti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 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	Devi Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	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	Dele Devi Data

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
GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe	25%	Virustotal		Browse
GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe	14%	ReversingLabs		

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:	33.0.0 White Diamond
Analysis ID:	491606
Start date:	27.09.2021
Start time:	18:35:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.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:	24
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@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 28.6% (good quality ratio 12.6%) • Quality average: 26.4% • Quality standard deviation: 34.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
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):	6.27152818261402
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:	GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe
File size:	102400
MD5:	917a78f3605abfda3674fe5264a721e9
SHA1:	c753e171b3ef5b974d70de7247734e3008841fd2
SHA256:	03e08e44d9df2a0ecc7824cc1b8f41e200cee531be111ee21d56ae1a5e05821a
SHA512:	b47adccf86fe1998de864d46a71a7b40efa8846b969ffc175fa2a345000f7f9b472c223c040b58fbda1511bfb5b0c58bb3b309ad276c3ad41e05234107eba67f
SSDEEP:	3072:ybQFnVb1t7zwaWVXpDMDeUtulrRMMBSy7gSNYS:WMnh1twaWh2DeUtulrRMuSy7gg
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L.....xY.....P...0.....`....@.....

File Icon

Icon Hash:	78f8d6d4ac88d0e2

Static PE Info

General

Entrypoint:	0x4012d4

General

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:	0x597805FC [Wed Jul 26 03:01:16 2017 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:	1eb0aaa4f15bbd841e91215ce68e26d2

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x14308	0x15000	False	0.561941964286	data	6.66841189519	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x16000	0x9f4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x1cb0	0x2000	False	0.263427734375	data	3.45335815554	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

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe PID: 5148 Parent PID: 5312

General

Start time:	18:36:49
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe'
Imagebase:	0x400000
File size:	102400 bytes
MD5 hash:	917A78F3605ABFDA3674FE5264A721E9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.514140065.00000000021F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis