ID: 539535
Sample Name:
pago12_14299038859.exe
Cookbook: default.jbs
Time: 13:59:26
Date: 14/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report pago12_14299038859.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 3
AV Detection: 4
Networking: 4
Data Obfuscation: 4
Malware Analysis System Evasion: 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 IPs 7
General Information 7
Simulations 7
Behavior and APIs 7
Joe Sandbox View / Context 7
IPs 8
Domains 8
ASN 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
Static File Info 8
General 8
File Icon 9
Static PE Info 9
General 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: pago12_14299038859.exe PID: 4680 Parent PID: 3716 10
General 10
File Activities 10
Registry Activities 10
Key Created 10
Key Value Created 10
Disassembly 10
Code Analysis 10

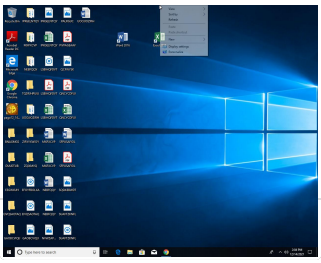
Windows Analysis Report pago12_14299038859.exe

Overview

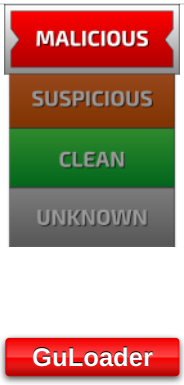
General Information

Sample Name:	pago12_14299038859.exe
Analysis ID:	539535
MD5:	9a1518ed709f916.
SHA1:	7c85312d66edf5b.
SHA256:	2a0878c1962783..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



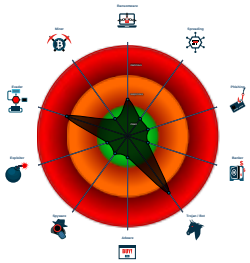
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- 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

Classification



Process Tree

- **System is w10x64**
- pago12_14299038859.exe (PID: 4680 cmdline: "C:\Users\user\Desktop\pago12_14299038859.exe" MD5: 9A1518ED709F916360E56B5AC7D76995)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1rvzmbX5uh5o/"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1196997646.0000000004D20000.00000040.00000001.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

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

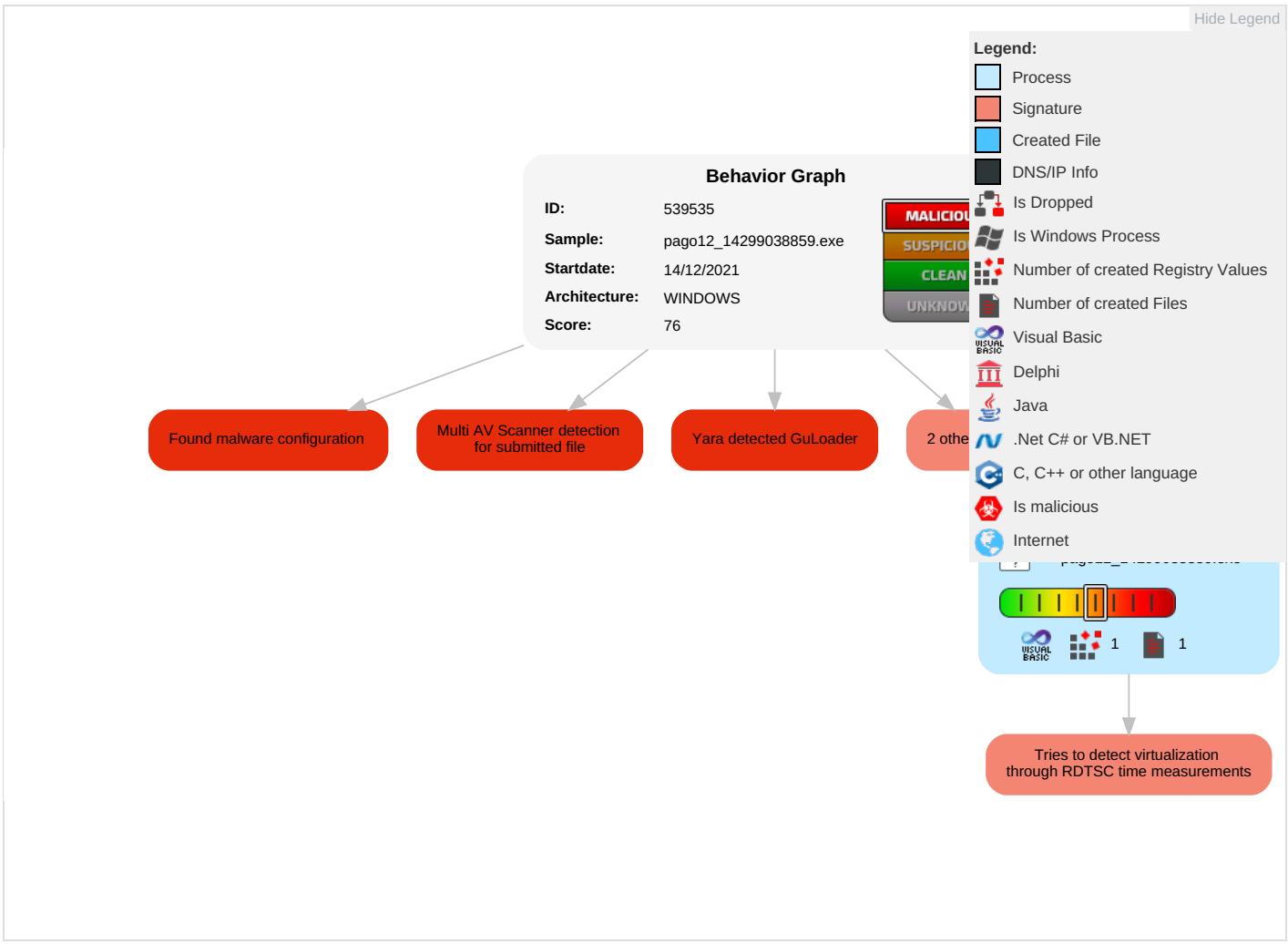
Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

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	Software Packing 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	Remotely Track Device Without Authorization	M S P
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	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D

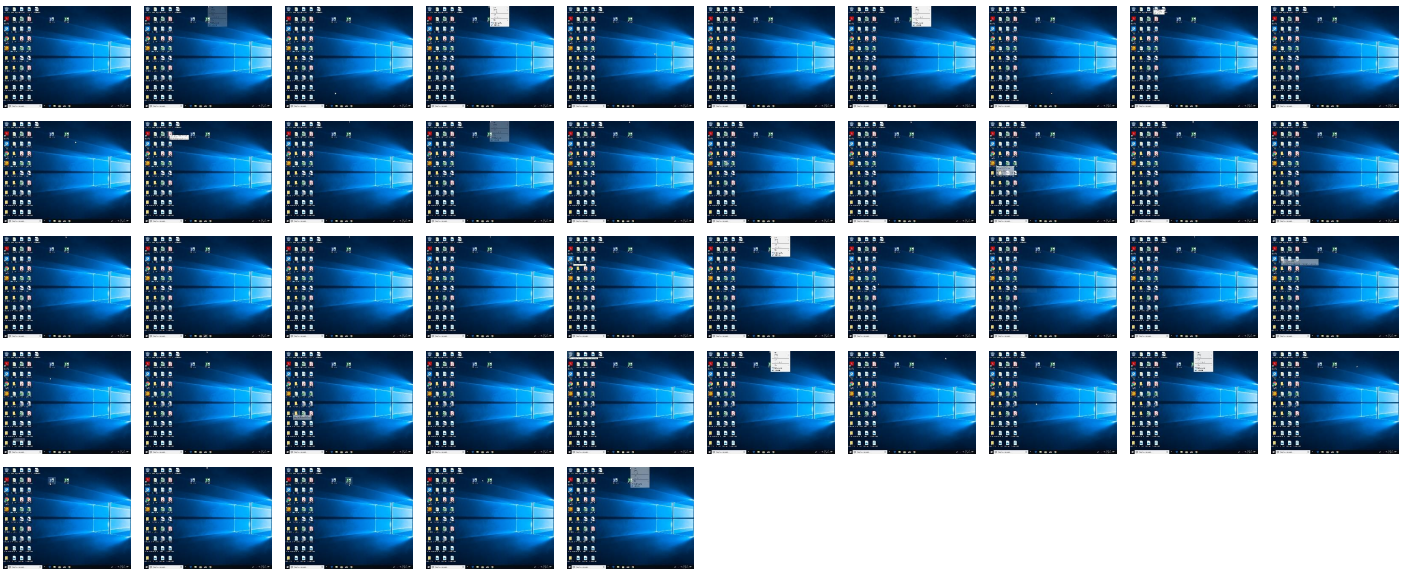
Behavior Graph



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
pago12_14299038859.exe	16%	ReversingLabs		
pago12_14299038859.exe	100%	Joe Sandbox ML		

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:	539535
Start date:	14.12.2021
Start time:	13:59:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pago12_14299038859.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:	mal76.troj.evad.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 7.8% (good quality ratio 5%) • Quality average: 37.9% • Quality standard deviation: 33.2%
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\~DF56158A8C389C0AF7.TMP	
Process:	C:\Users\user\Desktop\pago12_14299038859.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9730200708513237
Encrypted:	false
SSDEEP:	24:r/hDKifA3RuOH/3+aVR4J5lBefVYyDnKoKgQBX2:rJKifAhx5853weyDKoKgQB
MD5:	E8C98D07896778A7A68D9895386FC8A0
SHA1:	734F506C412CAFA5BF6680E7C1EBBE939CE63773
SHA-256:	DCEDB0D3B75126360C0556DC3310ACBBB97ADAD114F518DF8C65E84C0E6BED51
SHA-512:	A48737384CACB83CDB77F1CD5CCD89EB50E5CB48C7F6A41E2EC91093A4B4E6A634B0CCF85C39B4DC49D6C0B4D3D2DEF69FF002FCD96D0CC9EA8AFADF47E F14F
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.9046699069840765
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:	pago12_14299038859.exe
File size:	167936
MD5:	9a1518ed709f916360e56b5ac7d76995
SHA1:	7c85312d66edf5b02ebd6c25cfe9c036a3471263
SHA256:	2a0878c196278384aab473c92977d236680c788b4e5ae0 cc1f415a075a6fa9e2

General

SHA512:	8f99b5b19d72548340c8bfc3ce6460d73c055b556daa956 739cdeb67c2d0db56688e9f017deb2a94f29a298da959d4 79f3c8dc20123eac6762c69103cd004b13
SSDEEP:	1536:FrdvP8OOzT80mFxgs0HtyWPK0xljCwioDoWjJNa +I37KTqPRzV5pkNXuUAnq:ddvP81zTGUjKWMoDhjJN S7hPHUAnq
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....W.x..... .....\.....%.....Rich.....PE..L.....pV.... .....`...P.....\.....p....@

File Icon

Icon Hash:	937160c0d2e4f9fb

Static PE Info

General

Entrypoint:	0x40195c
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:	0x567083E4 [Tue Dec 15 21:19:32 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:	e7597de960f525af7c9e8aa5873fcec3

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x25ba0	0x26000	False	0.558850740132	data	7.15645216813	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x27000	0x36e4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DA TA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2b000	0x850	0x1000	False	0.322265625	data	3.08403187378	IMAGE_SCN_CNT_INITIALIZED_DA TA, 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: pago12_14299038859.exe PID: 4680 Parent PID: 3716

General

Start time:	14:00:24
Start date:	14/12/2021
Path:	C:\Users\user\Desktop\pago12_14299038859.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\pago12_14299038859.exe"
Imagebase:	0x400000
File size:	167936 bytes
MD5 hash:	9A1518ED709F916360E56B5AC7D76995
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1196997646.0000000004D20000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis