




**ID:** 526365
**Sample Name:** 2GirCpksIO
**Cookbook:** default.jbs
**Time:** 15:16:43
**Date:** 22/11/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents


Table of Contents 2
Windows Analysis Report 2GirCpksIO 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
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
Entrypoint Preview 9
Data Directories 9
Sections 9
Resources 9
Imports 9
Version Infos 9
Possible Origin 9
Network Behavior 9
Code Manipulations 9
Statistics 10
System Behavior 10
Analysis Process: 2GirCpksIO.exe PID: 6604 Parent PID: 6136 10
General 10
Disassembly 10
Code Analysis 10


Copyright Joe Security LLC 2021

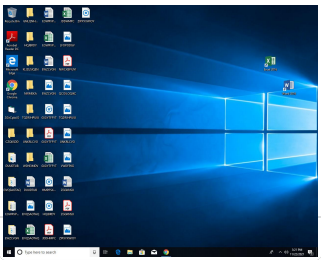
# Windows Analysis Report 2GirCpksIO

## Overview

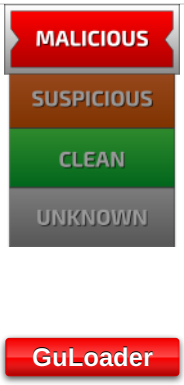
### General Information

| | |
|---|---|
| Sample Name: | 2GirCpksIO (renamed file extension from none to exe) |
| Analysis ID: | 526365 |
| MD5: | 5cc619f7dd365ec.. |
| SHA1: | 5b28cb97973da1.. |
| SHA256: | 7f5124088c09a92. |
| Infos: | |

Most interesting Screenshot:



### Detection

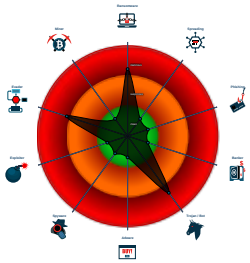



| | |
|---|---|
| Score: | 84 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Found potential dummy code loops (…
- 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 (…

### Classification



## Process Tree

- **System is w10x64**
- 2GirCpksIO.exe (PID: 6604 cmdline: "C:\Users\user\Desktop\2GirCpksIO.exe" MD5: 5CC619F7DD365EC061F1F385D25BEA30)
- **cleanup**

## Malware Configuration

### Threatname: GuLoader

```
{
  "Payload URL": "https://afrocompass.com/karinedocesesalgados_Hpi"
}
```

## Yara Overview

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.781020135.000000000293 0000.00000040.00000001.sdmp | JoeSecurity_GuLoader_2 | Yara detected GuLoader | Joe Security | |

## Sigma Overview

**No Sigma rule has matched**

## Jbx Signature Overview

Copyright Joe Security LLC 2021

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**

## System Summary:



**Potential malicious icon found**

## Data Obfuscation:



**Yara detected GuLoader**

## Anti Debugging:

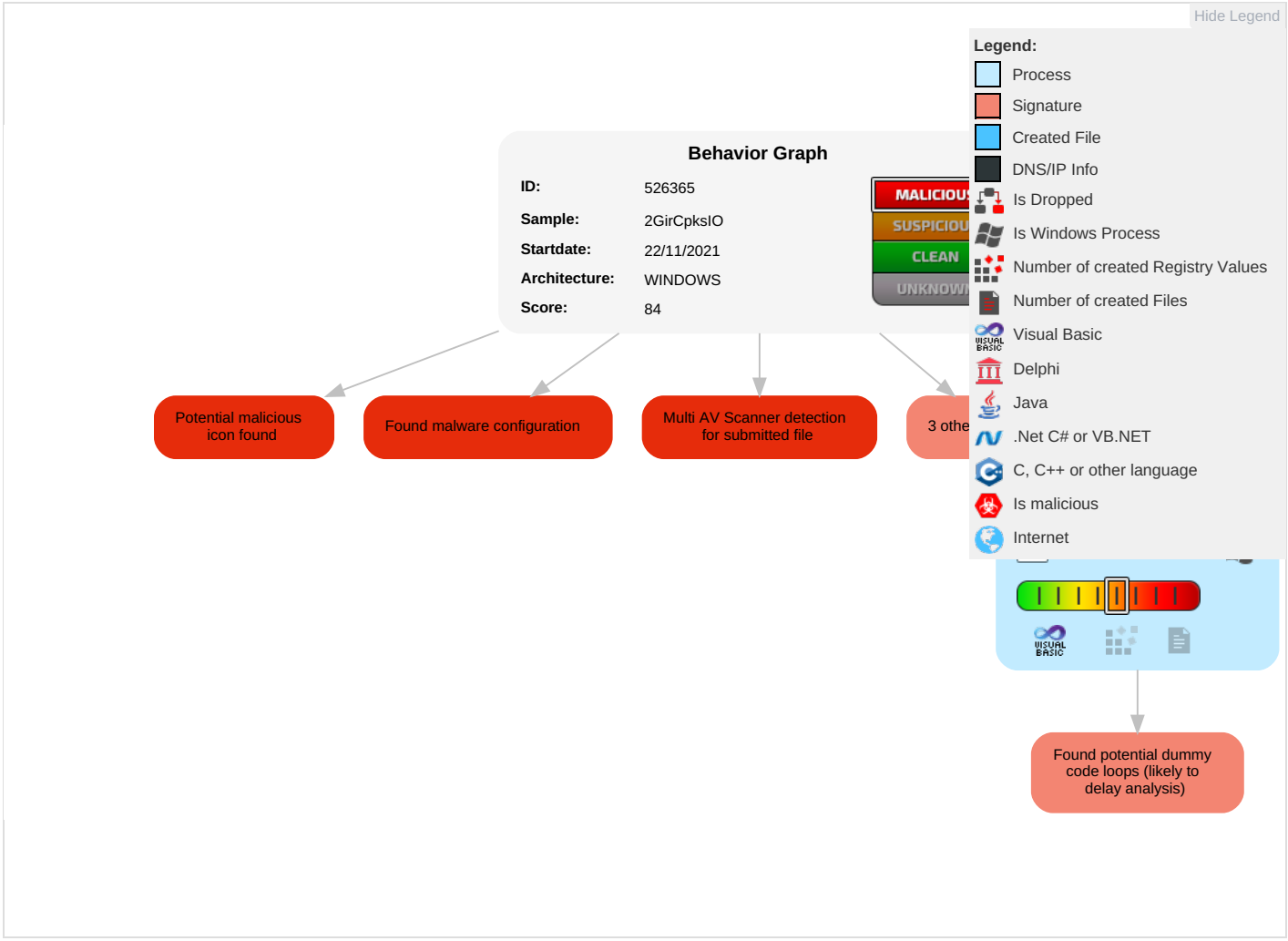


**Found potential dummy code loops (likely to delay analysis)**

## 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 Sc Ef |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Process Injection 1 | Virtualization/Sandbox Evasion 1 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 | R Tr W Au |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Software Packing 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 Au |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Process Injection 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 Cl Ba |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Obfuscated Files or Information 2 | NTDS | System Information Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | |

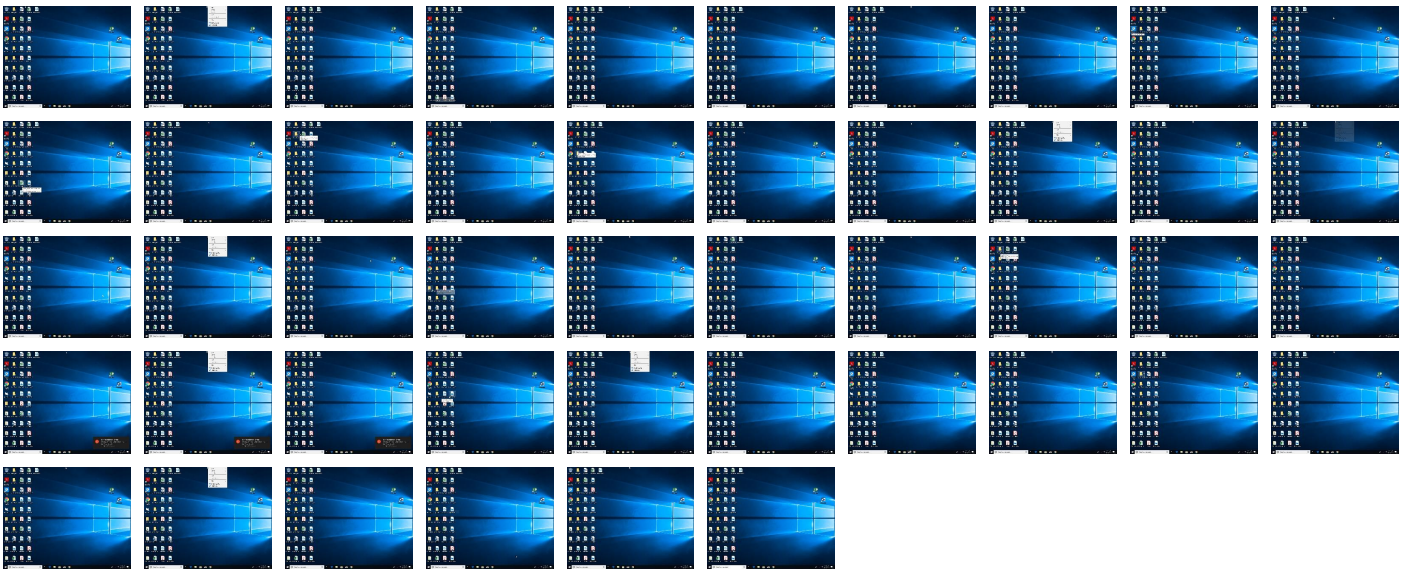
## Behavior Graph




## 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 |
|---|---|---|---|---|
| 2GirCpksIO.exe | 32% | Virustotal | | Browse |
| 2GirCpksIO.exe | 20% | ReversingLabs | | |
| 2GirCpksIO.exe | 100% | Joe Sandbox ML | | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://afrocompass.com/karinedocesesalgados_Hpi | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://afrocompass.com/karinedocesesalgados_Hpi | true | • Avira URL Cloud: safe | unknown |

## Contacted IPs

**No contacted IP infos**

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 526365 |
| Start date: | 22.11.2021 |
| Start time: | 15:16:43 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 7m 54s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 2GirCpksIO (renamed file extension from none to 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: | 25 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal84.rans.troj.evad.winEXE@1/0@0/0 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | • Successful, ratio: 17.9% (good quality ratio 12.1%)<br>• Quality average: 38.5%<br>• Quality standard deviation: 35.1% |
| HCA Information: | • Successful, ratio: 52%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• 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): | 6.550902828543532 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.15%<br>• Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | 2GirCpksIO.exe |
| File size: | 114688 |
| MD5: | 5cc619f7dd365ec061f1f385d25bea30 |
| SHA1: | 5b28cb97973da18953fb284648f13257f0aba2f3 |
| SHA256: | 7f5124088c09a925ad3a162b4e56391557dfc7d9950b9a5<br>5044036698d369d13 |
| SHA512: | bc3f1c85c20d22c7124ed93987f49d32cbe21639d7078ff<br>0cb11dc5f439342f9609ba78c92b097affd610ee878372e<br>8673a12829ba16ee70b73c1470f1124cd7 |
| SSDEEP: | 1536:SlQo1sxasghSzS9Qu2cRs/UVCNmETDFdnvr3Sy<br>jh3sMU+Wi04Mthlxxx:X51sxXiQu2cRss8mSFROyjh3s6<br>W2u |
| File Content Preview: | MZ.....@.....!..L.!Th<br>is program cannot be run in DOS mode....$.....O.....<br>.....D.....=.....Rich.....PE..L....5.a.....<br>@.....@..... |

## File Icon



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

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x401398 |
| 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: | 0x619B35E8 [Mon Nov 22 06:17:12 2021 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: | 6161f2da031dac68f8cae17819217d19 |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x17cac | 0x18000 | False | 0.631123860677 | data | 6.86127779315 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .data | 0x19000 | 0x11dc | 0x1000 | False | 0.00634765625 | data | 0.0 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x1b000 | 0x1ede | 0x2000 | False | 0.205200195312 | data | 4.84044222159 | 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: 2GirCpksIO.exe PID: 6604 Parent PID: 6136

### General

| | |
|---|---|
| Start time: | 15:17:46 |
| Start date: | 22/11/2021 |
| Path: | C:\Users\user\Desktop\2GirCpksIO.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\2GirCpksIO.exe" |
| Imagebase: | 0x400000 |
| File size: | 114688 bytes |
| MD5 hash: | 5CC619F7DD365EC061F1F385D25BEA30 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Yara matches: | • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.781020135.0000000002930000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

# Disassembly

## Code Analysis

Copyright Joe Security LLC


Copyright Joe Security LLC 2021