


**ID:** 395265
**Sample Name:** cotizacion.exe
**Cookbook:** default.jbs
**Time:** 11:16:18
**Date:** 22/04/2021
**Version:** 31.0.0 Emerald

# Table of Contents

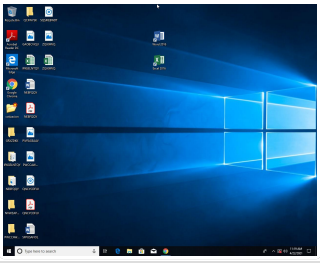
# Analysis Report cotizacion.exe

## Overview

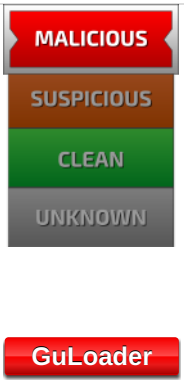
### General Information

| | |
|---|---|
| Sample Name: | cotizacion.exe |
| Analysis ID: | 395265 |
| MD5: | 35f5d83dbc44b90. |
| SHA1: | 745ba0ab77e726.. |
| SHA256: | daf8d6de50e27c4. |
| Infos: | |

Most interesting Screenshot:



### Detection



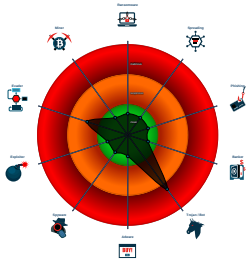

GuLoader

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

### Signatures

- Icon mismatch, binary includes an ic…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Machine Learning detection for samp…
- Found a high number of Window / Us…
- PE file contains an invalid checksum
- PE file contains strange resources
- Program does not show much activi…
- Sample execution stops while proce…
- Sample file is different than original …
- Uses 32bit PE files
- Uses code obfuscation techniques (…

### Classification



## Startup

- **System is w10x64**
- cotizacion.exe (PID: 1976 cmdline: 'C:\Users\user\Desktop\cotizacion.exe' MD5: 35F5D83DBC44B907D379C5AB35F725F8)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

### Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| cotizacion.exe | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.493125170.000000000401000.00000020.00020000.sdmp | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |
| 00000000.00000000.229099820.000000000401000.00000020.00020000.sdmp | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |

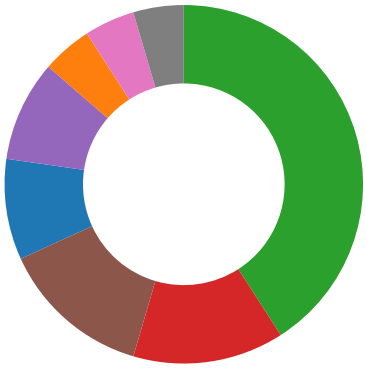
### Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0.0.cotizacion.exe.400000.0.unpack | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |
| 0.2.cotizacion.exe.400000.0.unpack | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |

## Sigma Overview

**No Sigma rule has matched**

## Signature Overview



- AV Detection
- Compliance
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

### AV Detection:

**Multi AV Scanner detection for submitted file**

**Machine Learning detection for sample**

### Data Obfuscation:

**Yara detected GuLoader**

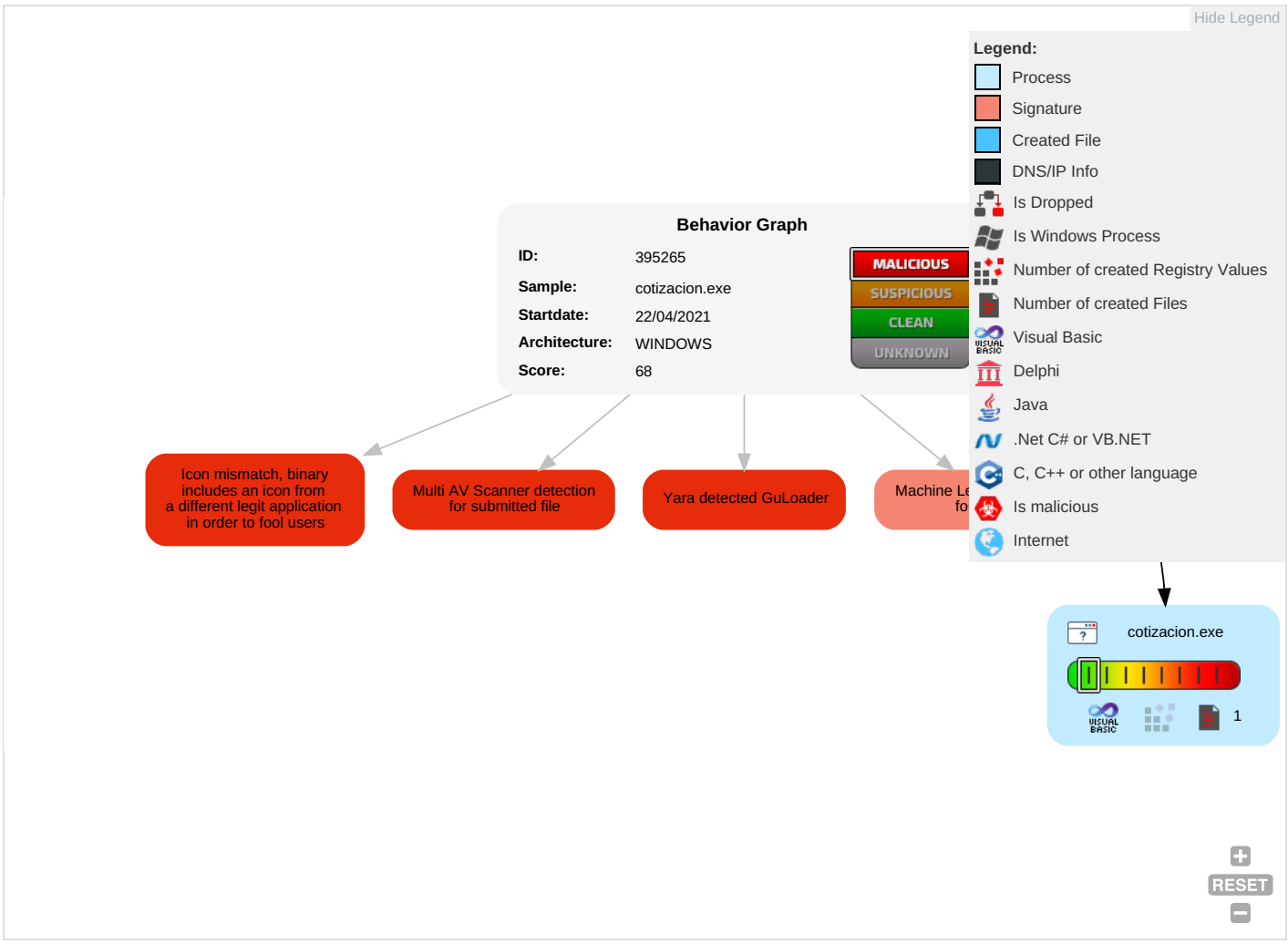
### Hooking and other Techniques for Hiding and Protection:

**Icon mismatch, binary includes an icon from a different legit application in order to fool users**

## 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 | Masquerading 1 | OS Credential Dumping | Process Discovery 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Data Obfuscation | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | M Sy Pa |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Process Injection 1 | LSASS Memory | Application Window Discovery 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | D Lo |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Obfuscated Files or Information 1 | 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 | D D D |

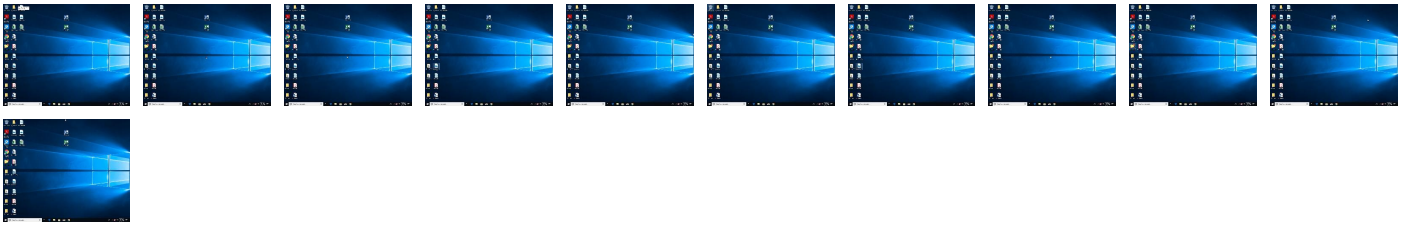
# Behavior Graph




# 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 |
|---|---|---|---|---|
| cotizacion.exe | 63% | Virustotal | | Browse |
| cotizacion.exe | 32% | Metadefender | | Browse |
| cotizacion.exe | 70% | ReversingLabs | Win32.Trojan.VBObfuse | |
| cotizacion.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: | 31.0.0 Emerald |
| Analysis ID: | 395265 |
| Start date: | 22.04.2021 |
| Start time: | 11:16:18 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 4m 52s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | cotizacion.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: | 12 |
| 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: | mal68.troj.winEXE@1/0@0/0 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | • Successful, ratio: 95.3% (good quality ratio 56.3%)<br>• Quality average: 28.7%<br>• Quality standard deviation: 26.6% |
| HCA Information: | Failed |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe |
| Warnings: | Show All<br>• Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe |

# 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): | 5.714049017467046 |
| 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: | cotizacion.exe |
| File size: | 118784 |
| MD5: | 35f5d83dbc44b907d379c5ab35f725f8 |
| SHA1: | 745ba0ab77e726e01d3f2fca4506383948906e24 |
| SHA256: | daf8d6de50e27c49b372d6cb0a7c6b7cd7a0946f959d13d3d3eb8d5d892c9eb7 |
| SHA512: | 76404764d6eb8d7392207ced43ba52b39702bdcff84e0b3842af2fa35105000abdf8d1e8c34a778fceab651ae4f52369d6e85645e0452db49c53ade5cd37e775 |
| SSDEEP: | 1536:PA1ybwSbXGgN79EiSJ99mLUaYugzYxrm19Ko2o/1hQr5UOaM0tmxswXpuqltL:P0KbVN7VSDXUxrh0G |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....).M.....p...`.....h.....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | c0c6f2e0e4fefe3f |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x401968 |
| 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: | 0x4DAB29E3 [Sun Apr 17 17:56:51 2011 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: | 7677b40f5f8927412a58af017314f1ed |

### Entrypoint Preview

| Instruction |
|---|
| push 0040F0A8h |
| call 00007FC704574F23h |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| xor byte ptr [eax], al |
| add byte ptr [eax], al |
| inc eax |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [esi], dh |
| loopne 00007FC704574F21h |
| mov edx, 4F5D2BC2h |
| mov es, ax |
| dec ebp |
| dec ecx |
| push 00000037h |
| hlt |
| and dword ptr [eax], eax |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [ecx], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [ebp+45h], cl |
| push esp |
| inc ecx |
| dec esp |
| dec edi |
| inc edi |
| dec ecx |
| inc ebx |
| inc ecx |
| dec esp |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |

| Instruction |
|---|
| add bh, bh |
| int3 |
| xor dword ptr [eax], eax |
| or al, ACh |
| sbb eax, dword ptr [esi] |
| push ebx |
| aaa |
| loop 00007FC704574ED9h |
| inc ebp |
| xchg eax, esi |
| and byte ptr [eax+4Fh], bl |
| lea ecx, dword ptr [esp+esi] |
| je 00007FC704574F4Ch |
| in al, dx |
| or al, D1h |
| and cl, bl |
| call far 69DBh : CB71A849h |
| xchg eax, edi |
| wait |

## Data Directories

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x17324 | 0x28 | .text |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x1a000 | 0x383a | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x228 | 0x20 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x1000 | 0x1a8 | .text |
| IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_RESERVED | 0x0 | 0x0 | |

## Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x16908 | 0x17000 | False | 0.442064368207 | data | 6.09226152403 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .data | 0x18000 | 0x1260 | 0x1000 | False | 0.00634765625 | data | 0.0 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x1a000 | 0x383a | 0x4000 | False | 0.462524414062 | data | 5.1445020687 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

## Resources

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_ICON | 0x1cf92 | 0x8a8 | data | | |
| RT_ICON | 0x1c8ca | 0x6c8 | data | | |
| RT_ICON | 0x1c362 | 0x568 | GLS_BINARY_LSB_FIRST | | |
| RT_ICON | 0x1b2ba | 0x10a8 | data | | |
| RT_ICON | 0x1a932 | 0x988 | data | | |
| RT_ICON | 0x1a4ca | 0x468 | GLS_BINARY_LSB_FIRST | | |
| RT_GROUP_ICON | 0x1a470 | 0x5a | data | | |
| RT_VERSION | 0x1a1e0 | 0x290 | MS Windows COFF PA-RISC object file | English | United States |

## Imports

| DLL | Import |
|---|---|
| MSVBVM60.DLL | _CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaLenBstr, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, __vbaLenBstrB, _adj_fdiv_m32, __vbaAryDestruct, __vbaOnError, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaObjVar, DllFunctionCall, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaLateMemCall, __vbaVarAdd, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, __vbaLateIdSt, _CItan, __vbaFPInt, _CIexp, __vbaFreeStr, __vbaFreeObj |

### Version Infos

| Description | Data |
|---|---|
| Translation | 0x0409 0x04b0 |
| InternalName | Forkvakledes |
| FileVersion | 1.00 |
| CompanyName | Cluster-C |
| Comments | Cluster-C |
| ProductName | Cluster-C |
| ProductVersion | 1.00 |
| FileDescription | Cluster-C |
| OriginalFilename | Forkvakledes.exe |

### 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: cotizacion.exe PID: 1976 Parent PID: 5576

### General

| | |
|---|---|
| Start time: | 11:17:10 |
| Start date: | 22/04/2021 |
| Path: | C:\Users\user\Desktop\cotizacion.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\cotizacion.exe' |
| Imagebase: | 0x400000 |
| File size: | 118784 bytes |
| MD5 hash: | 35F5D83DBC44B907D379C5AB35F725F8 |

| | |
|---|---|
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Yara matches: | • Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000002.493125170.0000000000401000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000000.229099820.0000000000401000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | low |

**File Activities**

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

# Disassembly

## Code Analysis