

JOeSandbox Cloud BASIC



**ID:** 528676

**Sample Name:**

RFQ\_TZDQP2110257921.exe

**Cookbook:** default.jbs

**Time:** 16:22:09

**Date:** 25/11/2021




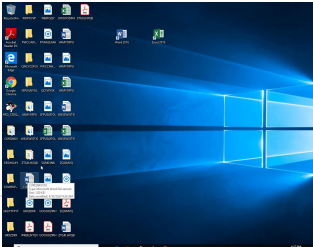
**Version:** 34.0.0 Boulder Opal

## Table of Contents

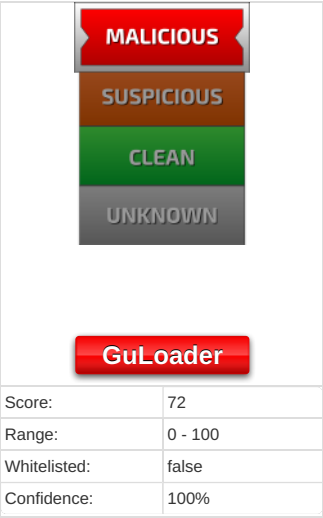
Table of Contents	2
Windows Analysis Report RFQ_TZDQP2110257921.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Memory Dumps	3
Sigma Overview	3
Jbx Signature Overview	3
AV Detection:	4
Networking:	4
Data Obfuscation:	4
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 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	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: RFQ_TZDQP2110257921.exe PID: 5908 Parent PID: 2944	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

## Overview

## General Information

Sample Name:	exe_TZDQP2110257921.exe
Analysis ID:	528676
MD5:	de5e1ca79f9bc16..
SHA1:	c688c1b2ea205a..
SHA256:	9f1956145a9bdc6..
Tags:	exe
Infos:	  
Most interesting Screenshot:	
	

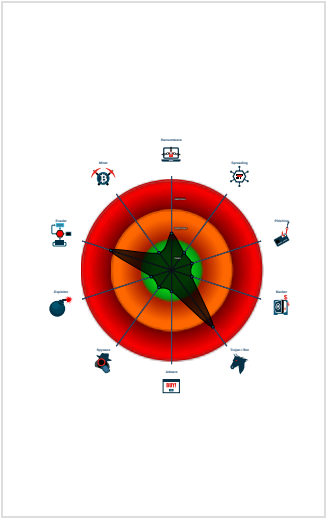
## Detection



## Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected GuLoader
- Found potential dummy code loops (...)
- C2 URLs / IPs found in malware con...
- Uses 32bit PE files
- Contains functionality to call native f...
- Sample file is different than original ...
- Contains functionality to read the PEB
- Program does not show much activi...
- Uses code obfuscation techniques (...)
- Contains functionality for execution ...

## Classification



## Process Tree

- System is w10x64
-  **RFQ\_TZDQP2110257921.exe** (PID: 5908 cmdline: "C:\Users\user\Desktop\RFQ\_TZDQP2110257921.exe" MD5: DE5E1CA79F9BC16726E87F9E04529A33)
- cleanup

## Malware Configuration

## Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=d_"
}
```

## Yara Overview

## Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1180599647.0000000002B50000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

## Sigma Overview

No Sigma rule has matched

## Jbx Signature Overview

## 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

## Anti Debugging:

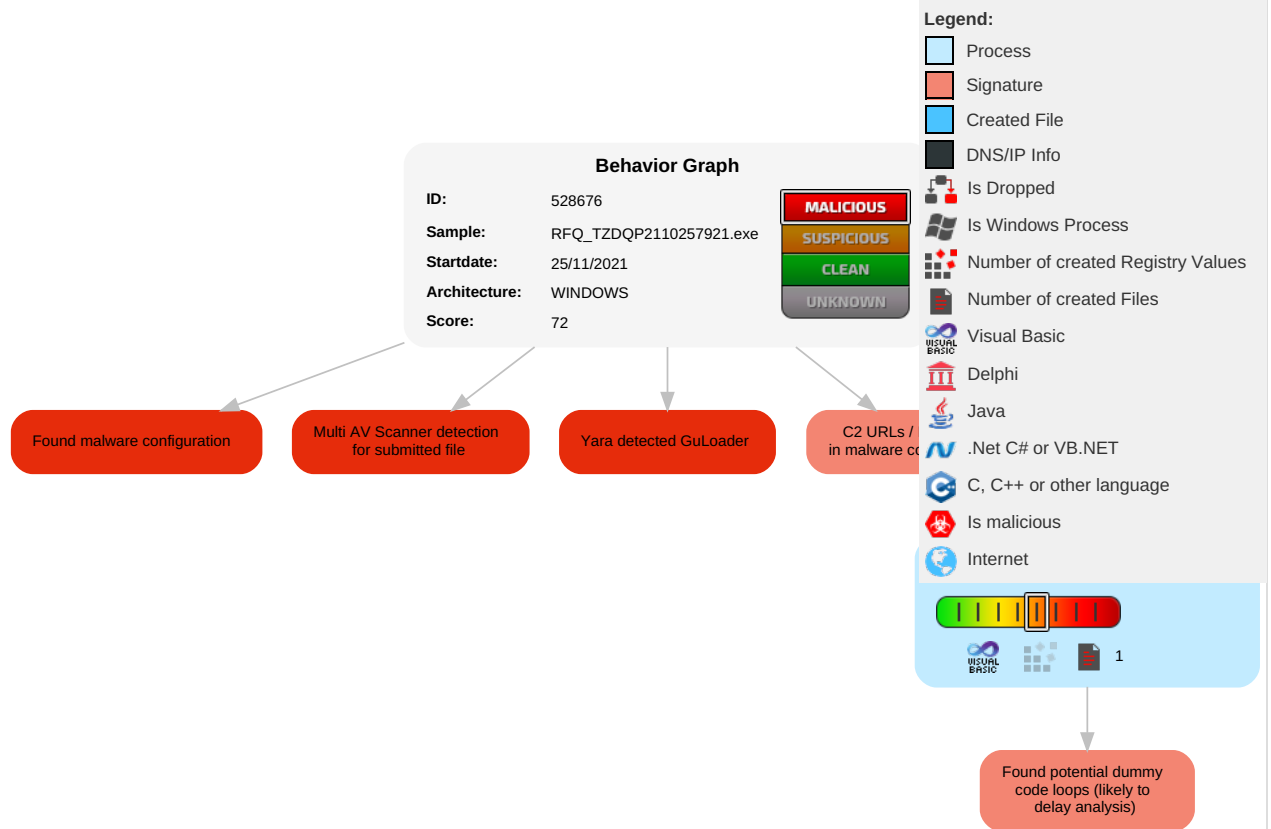


Found potential dummy code loops (likely to delay analysis)

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
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	Recovery
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	Recovery
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	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

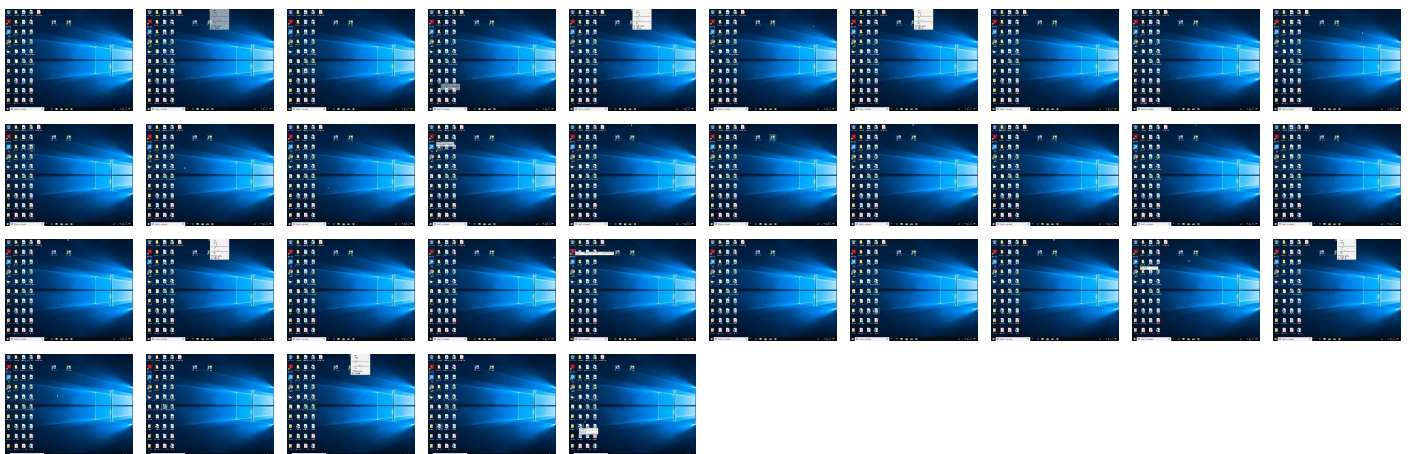
## Behavior Graph



## 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
RFQ_TZDQP2110257921.exe	14%	ReversingLabs	Win32.Downloader.GuLoad er	

### 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:	528676
Start date:	25.11.2021
Start time:	16:22:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ_TZDQP2110257921.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:	15
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:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.evad.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 2.2% (good quality ratio 1.2%)</li><li>• Quality average: 29.8%</li><li>• Quality standard deviation: 31.7%</li></ul>
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found application associated with file extension: .exe</li><li>• Override analysis time to 240s for sample files taking high CPU consumption</li></ul>
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\~DF87EDA8D7970694A0.TMP	
Process:	C:\Users\user\Desktop\RFQ_TZDQP2110257921.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9277305547216628
Encrypted:	false
SSDEEP:	48:rJSq2Upu8metqPriXHimU7zdvP1vncU7pCr8P:VSKUpACLFcUVCrG
MD5:	19809EDD1FF00A1D7C105BC58A97CD02
SHA1:	26FB6D339CF2A7474DE6F785166163FA9B2ADBB1
SHA-256:	4745D04A4BB99D70866D722394D9E71F3FAE597AA84E229A1E3B40F31521594C
SHA-512:	434722936006B56B042FB5C72CAB98D8B7615A5A0E48EE6746DD6839BE029029E3BCECF7EFA49DDC8A9DB016FA472FB9EE1CE75126C13E06D66EAA12166A387
Malicious:	false
Reputation:	low
Preview:	.....>..... ..... ..... .....

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.800736460840025
TrID:	<ul style="list-style-type: none"><li>Win32 Executable (generic) a (10002005/4) 99.15%</li><li>Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%</li><li>Generic Win/DOS Executable (2004/3) 0.02%</li><li>DOS Executable Generic (2002/1) 0.02%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li></ul>
File name:	RFQ_TZDQP2110257921.exe
File size:	135168
MD5:	de5e1ca79f9bc16726e87f9e04529a33
SHA1:	c688c1b2ea205aa37f7fe4a511d18f1bdead62a1

General

SHA256:	9f1956145a9bdc606ad1463721f38ea1c31c6aeabfb028a0b134c0f3e881db47
SHA512:	c474e84731b9d0428d9bdac8df5b56f30e8738e709871c7a25e0fdb0eff304a095cbbc8a1602be113ffce0e4239ae69c7cde7442abbc9c437d6312930087b57
SSDEEP:	1536:thDtliZk5GmFDOQbC91Ugi+yDWkzjHOredD:th25B7CfrEWWjMed
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......i..... .....*.....Rich.....PE..L.....J..... ..0.....@.....

File Icon



Icon Hash:	981dca909cee36b0
------------	------------------

Static PE Info

General

Entrypoint:	0x4013b4
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:	0x4AC47F1B [Thu Oct 1 10:06:19 2009 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:	d77040f4614bccfda7b8aa2e04863738

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1d45c	0x1e000	False	0.353116861979	data	4.98754225046	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1f000	0x141c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x21000	0xf50	0x1000	False	0.339111328125	data	3.26324381728	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
--------------------------------	----------------------------------	-----

Language of compilation system	Country where language is spoken	Map
English	United States	
Turkmen	Turkmenistan	

## Network Behavior

No network behavior found

## Code Manipulations

## Statistics

## System Behavior

Analysis Process: RFQ\_TZDQP2110257921.exe PID: 5908 Parent PID: 2944

### General

Start time:	16:23:00
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\RFQ_TZDQP2110257921.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\RFQ_TZDQP2110257921.exe"
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	DE5E1CA79F9BC16726E87F9E04529A33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none"> <li>Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1180599647.0000000002B50000.00000040.00000001.sdmp, Author: Joe Security</li> </ul>
Reputation:	low

### File Activities

Show Windows behavior

## Disassembly

### Code Analysis

