

JoeSandbox Cloud BASIC



**ID:** 450786

**Sample Name:** PREVENTIVO  
RICHIESTO (2).exe

**Cookbook:** default.jbs

**Time:** 18:12:29

**Date:** 19/07/2021

**Version:** 33.0.0 White Diamond



## Table of Contents


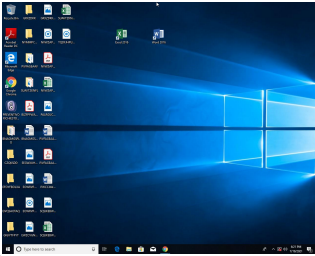
Table of Contents	2
Windows Analysis Report PREVENTIVO RICHIESTO (2).exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Initial Sample	3
Memory Dumps	3
Unpacked PEs	3
Sigma Overview	4
Jbx Signature Overview	4
AV Detection:	4
Networking:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Anti Debugging:	4
Mitre Att&ck Matrix	4
Behavior Graph	5
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: PREVENTIVO RICHIESTO (2).exe PID: 5716 Parent PID: 5644	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10



# Windows Analysis Report PREVENTIVO RICHIESTO (2)....

## Overview

### General Information

Sample Name:	PREVENTIVO RICHIESTO (2).exe
Analysis ID:	450786
MD5:	72d9c62e448351..
SHA1:	12093edc01bcf89..
SHA256:	42c8ded976a7c9..
Tags:	exe
Infos:	
Most interesting Screenshot:	
	

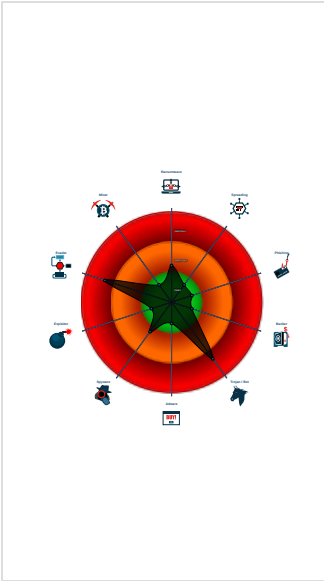
### Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div> <div>GuLoader</div>	
Score:	80
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...
Detected RDTSC dummy instruction...
Found potential dummy code loops (...)
Tries to detect virtualization through...
Abnormal high CPU Usage
Contains functionality for execution ...
Contains functionality to query CPU ...
Detected potential crypto function
PE file contains strange resources
Program does not show much activi...
Sample file is different than original ...

### Classification



## Process Tree

- System is w10x64
-  PREVENTIVO RICHIESTO (2).exe (PID: 5716 cmdline: 'C:\Users\user\Desktop\PREVENTIVO RICHIESTO (2).exe' MD5: 72D9C62E4483519DF1303FE0C46D16AA)
- cleanup

## Malware Configuration

### Threatname: GuLoader

```
{
  "Payload URL": "https://banontarquitectura.com.mx/IRANSAT_kowbB4.bin"
}
```

## Yara Overview

### Initial Sample

Source	Rule	Description	Author	Strings
PREVENTIVO RICHIESTO (2).exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

### Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1236460953.00000000004 01000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
00000000.00000000.208215258.000000000040 1000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

### Unpacked PEs



Source	Rule	Description	Author	Strings
0.0.PREVENTIVO RICHIESTO (2).exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
0.2.PREVENTIVO RICHIESTO (2).exe.400000.0.unpack	JoeSecurity_GuLoader_1	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

### Malware Analysis System Evasion:



Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect virtualization through RDTSC time measurements

### Anti Debugging:



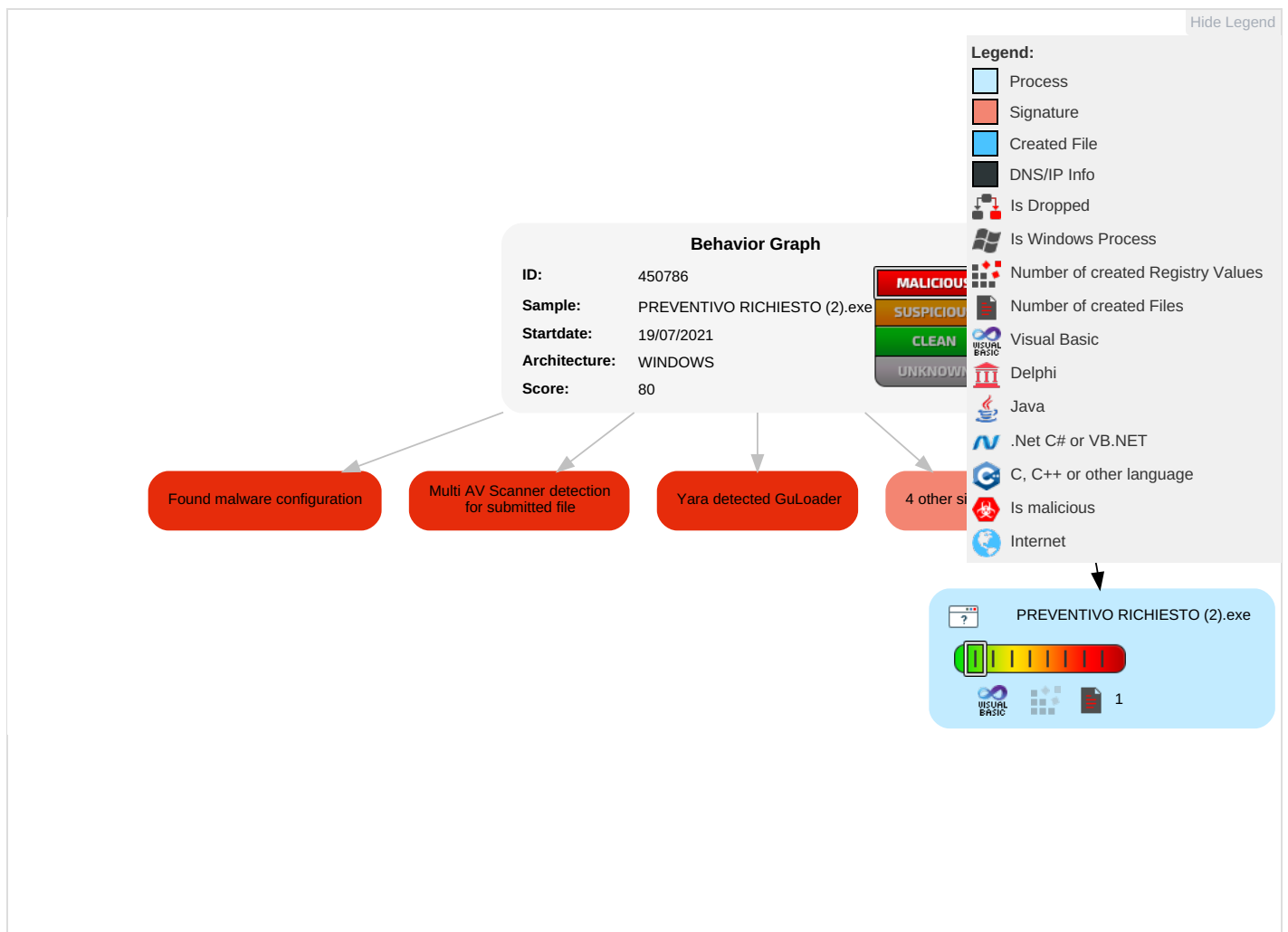
Found potential dummy code loops (likely to delay analysis)

## 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	Path Interception	Virtualization/Sandbox Evasion <b>1</b> <b>1</b>	OS Credential Dumping	Security Software Discovery <b>3</b> <b>1</b>	Remote Services	Archive Collected Data <b>1</b>	Exfiltration Over Other Network Medium	Encrypted Channel <b>1</b>	Eavesdrop on Insecure Network Communication	Recovery Techniques Windows Administrative
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information <b>1</b>	LSASS Memory	Virtualization/Sandbox Evasion <b>1</b> <b>1</b>	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol <b>1</b>	Exploit SS7 to Redirect Phone Calls/SMS	Recovery Techniques Windows Administrative
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery <b>2</b> <b>1</b> <b>1</b>	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Operational Techniques Windows Administrative



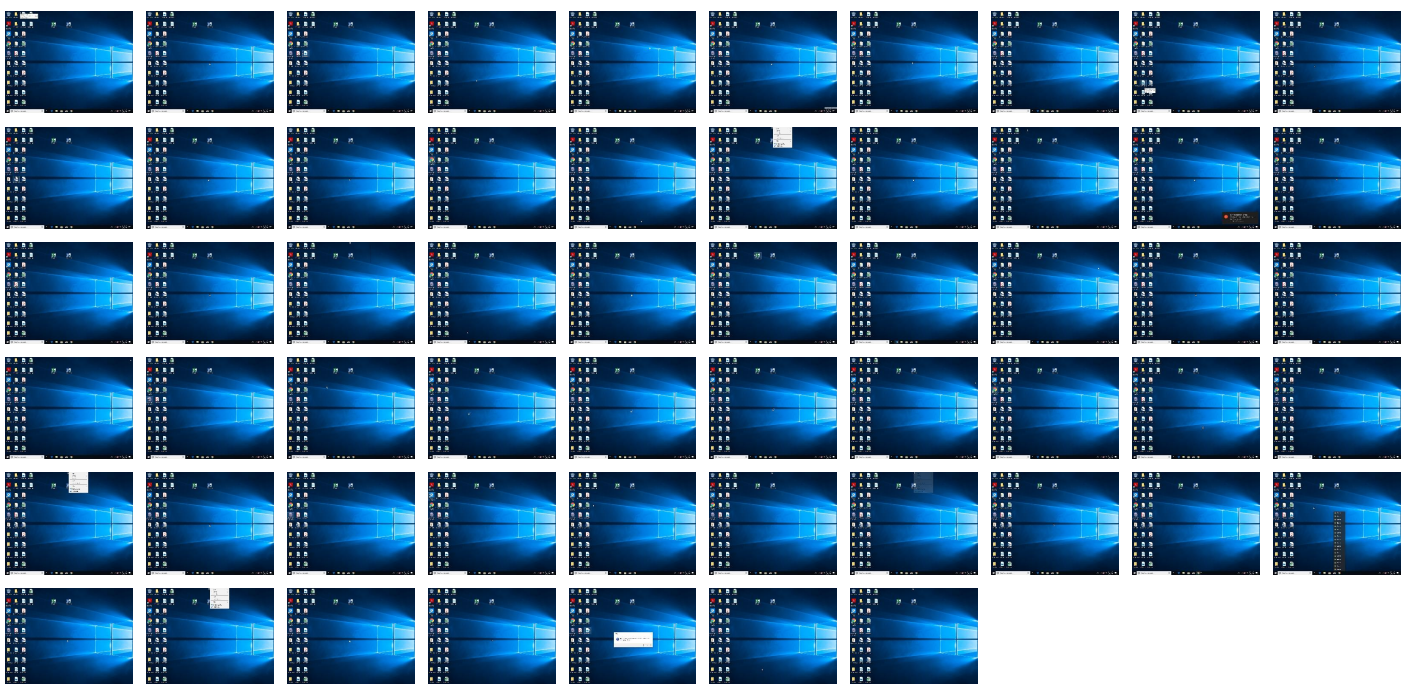
## Behavior Graph



## Screenshots

### Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.









## Domains and IPs

### Contacted Domains

No contacted domains info

### Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bamontarquitectura.com.mx/IRANSAT_kowbB4.bin	true	<ul style="list-style-type: none"><li>Avira URL Cloud: safe</li></ul>	unknown

### Contacted IPs

No contacted IP infos

## General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	450786
Start date:	19.07.2021
Start time:	18:12:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PREVENTIVO RICHIESTO (2).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
Run name:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	41
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:	mal80.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>Successful, ratio: 51.6% (good quality ratio 23%)</li><li>Quality average: 24.6%</li><li>Quality standard deviation: 33.1%</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></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

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.24355762284074
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:	PREVENTIVO RICHIESTO (2).exe
File size:	241664
MD5:	72d9c62e4483519df1303fe0c46d16aa
SHA1:	12093edc01bcf89eb7a9758d1392592fb273de35
SHA256:	42c8ded976a7c9f295888220d4d2fc273535f1fa15e6e25cfceaf454188f7895
SHA512:	cf6d6c1a6072c022ab4d19f098715cba02f8dcc74f01ce7ad735d5cdb5c7505aeb9c98fb9ff3faac7932ffbdb7cdf581c583fa846cc76b71dee3f2a71b7b30a0
SSDEEP:	3072:c3BepJlZa/E5cv3MRwqmVqY+9uiwBDa1Gh7HJlZapGBR:eiUEUMyqmVrTjDc4HP
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode...\$.....#...B...B ...B..L^...B...`...B...d...B..Rich.B.....PE..L.....W..... .....0....@.....

File Icon





Icon Hash:	f8fcd4ccf4e4e8d0
------------	------------------

## Static PE Info

### General

Entrypoint:	0x4019b0
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:	0x5783B9FD [Mon Jul 11 15:23:41 2016 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:	e9f7dd0da1a2a1266893e1ae4ef42b67

### Entrypoint Preview

### Data Directories

### Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x31d44	0x32000	False	0.390419921875	data	6.39904472476	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x33000	0x1290	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x35000	0x6d0e	0x7000	False	0.48193359375	data	5.46083184817	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



## Code Manipulations

## Statistics

## System Behavior

Analysis Process: PREVENTIVO RICHIESTO (2).exe PID: 5716 Parent PID: 5644

### General

Start time:	18:13:20
Start date:	19/07/2021
Path:	C:\Users\user\Desktop\PREVENTIVO RICHIESTO (2).exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PREVENTIVO RICHIESTO (2).exe'
Imagebase:	0x400000
File size:	241664 bytes
MD5 hash:	72D9C62E4483519DF1303FE0C46D16AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none"><li>Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000002.1236460953.0000000000401000.00000020.00020000.sdmp, Author: Joe Security</li><li>Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000000.208215258.0000000000401000.00000020.00020000.sdmp, Author: Joe Security</li></ul>
Reputation:	low

### File Activities

Show Windows behavior

## Disassembly

## Code Analysis