# JOeSandbox Cloud BASIC

**ID:** 450724
**Sample Name:** RICHIESTA DI OFFERTA.exe
**Cookbook:** default.jbs
**Time:** 16:34:49
**Date:** 19/07/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

# Windows Analysis Report RICHIESTA DI OFFERTA.exe

## Overview

### General Information

| | |
|---|---|
| Sample Name: | RICHIESTA DI OFFERTA.exe |
| Analysis ID: | 450724 |
| MD5: | 73bb5c4b690b8d.. |
| SHA1: | 60adddd91b6038.. |
| SHA256: | a3feb5265e6d027. |
| Infos: | |

Most interesting Screenshot:

### Detection

**MALICIOUS**

SUSPICIOUS

CLEAN

UNKNOWN

**GuLoader**

| | |
|---|---|
| Score: | 84 |
| 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…

Contains functionality to detect hard…

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 …

Contains functionality to read the PEB

### Classification
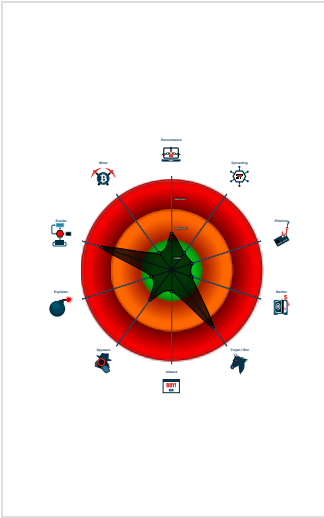
## Process Tree

- **System is w10x64**
- RICHIESTA DI OFFERTA.exe (PID: 3448 cmdline: 'C:\Users\user\Desktop\RICHIESTA DI OFFERTA.exe' MD5: 73BB5C4B690B8D6DF88D6BC18FB3A553)
- **cleanup**

## Malware Configuration

### Threatname: GuLoader

```
{
    "Payload URL": "https://bamontarquitectura.com.mx/IRANSAT_kowbB4.bi}"
}
```

## Yara Overview

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.856112688.00000000029B 0000.00000040.00000001.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 |

## Networking:

| C2 URLs / IPs found in malware configuration |

## Data Obfuscation:

| Yara detected GuLoader |

## Malware Analysis System Evasion:

| Contains functionality to detect hardware virtualization (CPUID execution measurement) |
| 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 | R... S... E... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Process Injection 1 | Virtualization/Sandbox Evasion 1 1 | OS Credential Dumping | Security Software Discovery 4 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communication | R... Tr... W... A... |
| 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 | R... W... A... |
| 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 | O... D... C... B... |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Binary Padding | NTDS | System Information Discovery 3 1 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | |

## Behavior Graph

**Behavior Graph**

| | |
|---|---|
| **ID:** | 450724 |
| **Sample:** | RICHIESTA DI OFFERTA.exe |
| **Startdate:** | 19/07/2021 |
| **Architecture:** | WINDOWS |
| **Score:** | 84 |

MALICIOU
SUSPICIOU
CLEAN
UNKNOWN

**Legend:**

- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected GuLoader

5 other

RICHIESTA DI OFFERTA.exe

1

# Screenshots

**Thumbnails**

This section contains all screenshots as thumbnails, including those not shown in the slideshow.
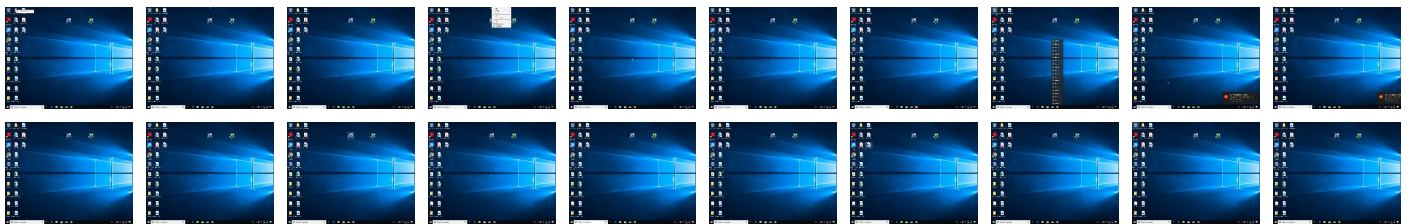
## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| RICHIESTA DI OFFERTA.exe | 21% | Virustotal | | Browse |
| RICHIESTA DI OFFERTA.exe | 9% | ReversingLabs | Win32.Backdoor.Remcos | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://bamontarquitectura.com.mx/IRANSAT_kowbB4.bi} | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|------|-----------|---------------------|------------|
| http://https://bamontarquitectura.com.mx/IRANSAT_kowbB4.bi} | true | • Avira URL Cloud: safe | unknown |

## Contacted IPs

**No contacted IP infos**

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 450724 |
| Start date: | 19.07.2021 |
| Start time: | 16:34:49 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 7m 31s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | RICHIESTA DI OFFERTA.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: | Potential for more IOCs and behavior |
| Number of analysed new started processes analysed: | 21 |
| 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.troj.evad.winEXE@1/0@0/0 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | • Successful, ratio: 42.2% (good quality ratio 15.2%)<br>• Quality average: 20.9%<br>• Quality standard deviation: 31.4% |
| HCA Information: | Failed |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe<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): | 6.2221702126738 |
| TrID: | <ul><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: | RICHIESTA DI OFFERTA.exe |
| File size: | 241664 |
| MD5: | 73bb5c4b690b8d6df88d6bc18fb3a553 |
| SHA1: | 60adddd91b6038fc9d819cf6d647ce3be0b11d38 |
| SHA256: | a3feb5265e6d02710f04ff618e966e9da9ba8fc8dc5692d6 f7633fe0a3037b66 |
| SHA512: | 9c023dc66d9bcfb2f5bc0274001d92948ac058fc8765d21 78907dfd8fb9885ede57acc3836d583ad97516dce1a97c5 0f081800b41a1f42ea938efb8b23e87567 |
| SSDEEP: | 3072:+3BepJlZa/xao5JKwI7V4R4iUW/qcijw2HJlZapGB R:EiUIo5JKPgU99vHP |
| 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...WS.N......... ........ ...................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: | 0x4EA15357 [Fri Oct 21 11:11:19 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: | e9f7dd0da1a2a1266893e1ae4ef42b67 |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x318a4 | 0x32000 | False | 0.39177734375 | data | 6.3764832494 | 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 | 0x6d0a | 0x7000 | False | 0.481689453125 | data | 5.46300019784 | 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: RICHIESTA DI OFFERTA.exe PID: 3448 Parent PID: 5876

### General

| | |
|---|---|
| Start time: | 16:35:41 |
| Start date: | 19/07/2021 |
| Path: | C:\Users\user\Desktop\RICHIESTA DI OFFERTA.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\RICHIESTA DI OFFERTA.exe' |
| Imagebase: | 0x400000 |
| File size: | 241664 bytes |
| MD5 hash: | 73BB5C4B690B8D6DF88D6BC18FB3A553 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Yara matches: | • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.856112688.00000000029B0000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities                                    Show Windows behavior

# Disassembly

## Code Analysis

Joe Sandbox Cloud Basic 33.0.0 White Diamond