JoeSandbox Cloud BASIC

**ID:** 433075
**Sample Name:** eCooEFZfZJ.exe
**Cookbook:** default.jbs
**Time:** 08:53:11
**Date:** 11/06/2021
**Version:** 32.0.0 Black Diamond

# Table of Contents

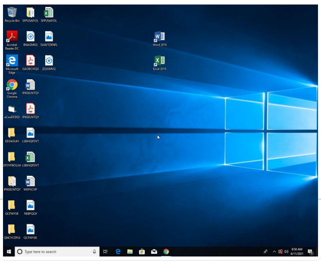
# Analysis Report eCooEFZfZJ.exe

## Overview

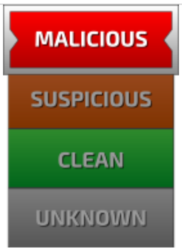
### General Information

| | |
|---|---|
| Sample Name: | eCooEFZfZJ.exe |
| Analysis ID: | 433075 |
| MD5: | 2db978e7cd2512.. |
| SHA1: | 22736d8d3ffe0e7.. |
| SHA256: | 9ec05fd611c2df6.. |
| Tags: | exe GuLoader |
| Infos: | |

Most interesting Screenshot:



### Detection



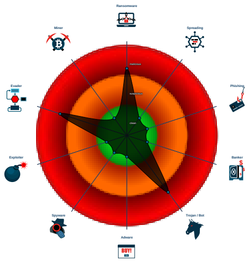
GuLoader

| | |
|---|---|
| Score: | 88 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Found potential dummy code loops (…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to call native f…
- Contains functionality to read the PEB

### Classification



## Process Tree

- **System is w10x64**
- eCooEFZfZJ.exe (PID: 5600 cmdline: 'C:\Users\user\Desktop\eCooEFZfZJ.exe'  MD5: 2DB978E7CD2512C358518B1981FEE079)
- **cleanup**

## Malware Configuration

### Threatname: GuLoader

```
{
  "Payload URL": "https://bara-seck.com/bin_sLFaSDyCig163.bin, http://benvenuti.rs/wp-content/bin_s"
}
```

## Yara Overview

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.755211123.00000000021B 0000.00000040.00000001.sdmp | JoeSecurity_GuLoader_2 | Yara detected GuLoader | Joe Security | |

## Sigma Overview

**No Sigma rule has matched**

## 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**

## System Summary:

**Potential malicious icon found**

## Data Obfuscation:

**Yara detected GuLoader**

## Malware Analysis System Evasion:

**Contains functionality to detect hardware virtualization (CPUID execution measurement)**

**Tries to detect virtualization through RDTSC time measurements**

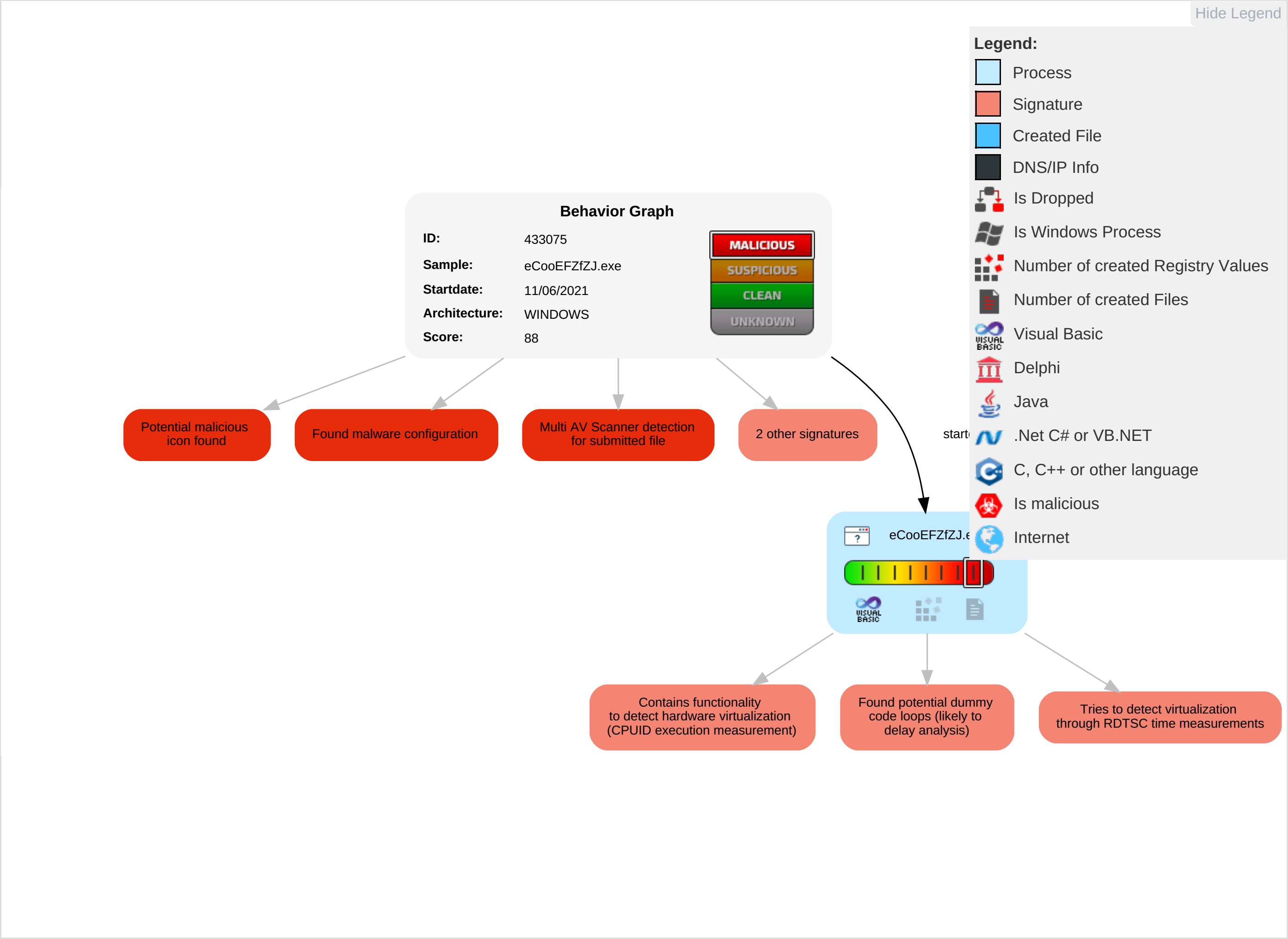
## Anti Debugging:

**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 | System Time Discovery 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communication | R T W A |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Process Injection 1 | LSASS Memory | Security Software Discovery 3 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 A |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Obfuscated Files or Information 1 | Security Account Manager | Virtualization/Sandbox Evasion 1 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 | Process Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Software Packing | LSA Secrets | System Information Discovery 2 2 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | |

## Behavior Graph



Hide Legend

**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

**Behavior Graph**

| | |
|---|---|
| **ID:** | 433075 |
| **Sample:** | eCooEFZfZJ.exe |
| **Startdate:** | 11/06/2021 |
| **Architecture:** | WINDOWS |
| **Score:** | 88 |

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Potential malicious icon found

Found malware configuration

Multi AV Scanner detection for submitted file

2 other signatures

start

eCooEFZfZJ.e

Contains functionality to detect hardware virtualization (CPUID execution measurement)

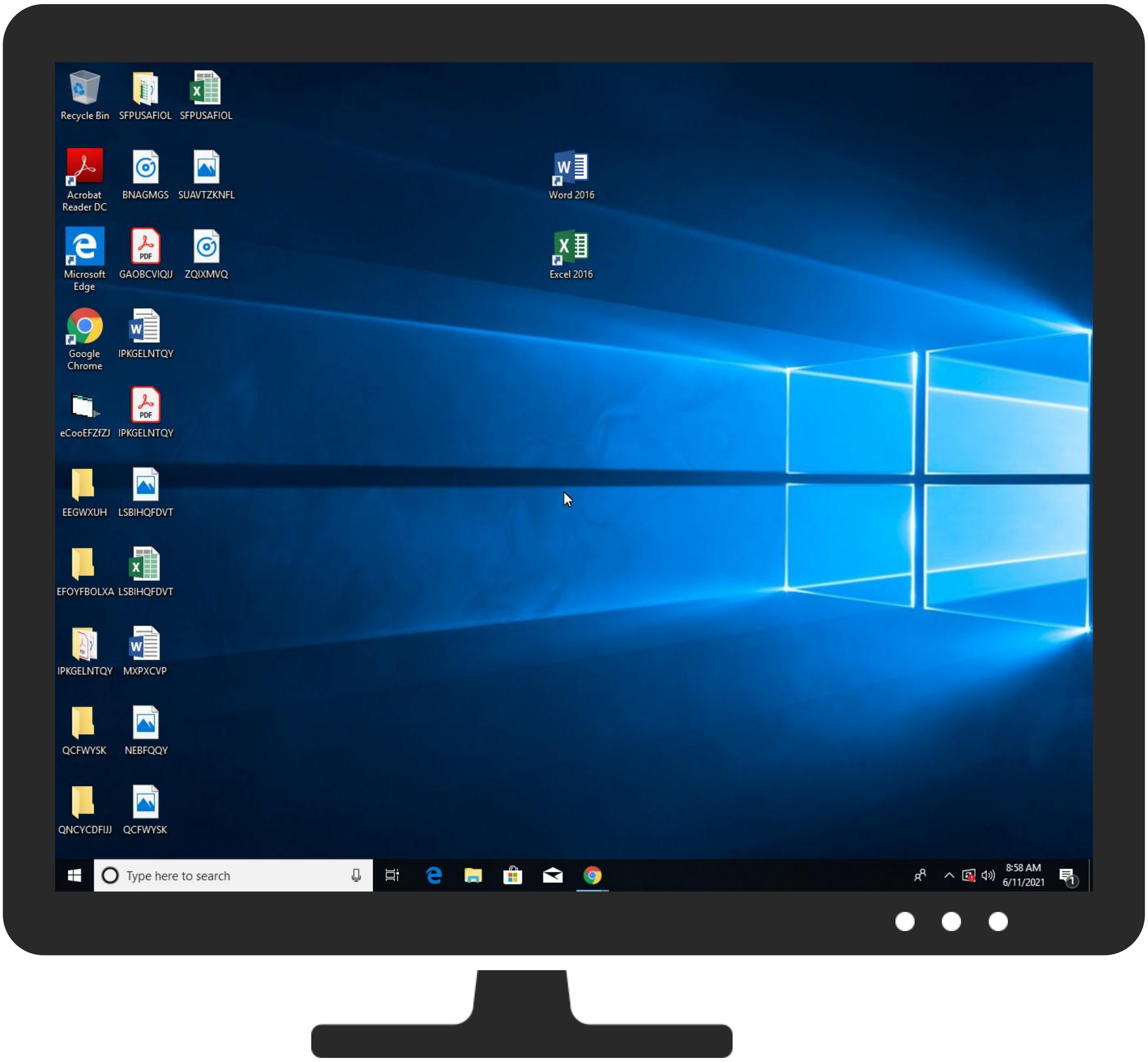
Found potential dummy code loops (likely to delay analysis)

Tries to detect virtualization through RDTSC time measurements

## 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 |
|---|---|---|---|---|
| eCooEFZfZJ.exe | 16% | Virustotal | | Browse |

## Dropped Files

**No Antivirus matches**

## Unpacked PE Files

**No Antivirus matches**

## Domains

**No Antivirus matches**

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://bara-seck.com/bin_sLFaSDyCig163.bin, benvenuti.rs/wp-content/bin_s | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://bara-seck.com/bin_sLFaSDyCig163.bin, benvenuti.rs/wp-content/bin_s | true | • Avira URL Cloud: safe | unknown |

## Contacted IPs

**No contacted IP infos**

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 32.0.0 Black Diamond |
| Analysis ID: | 433075 |
| Start date: | 11.06.2021 |
| Start time: | 08:53:11 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 7m 44s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | eCooEFZfZJ.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: | mal88.rans.troj.evad.winEXE@1/0@0/0 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 6.9% (good quality ratio 0.9%)<br>• Quality average: 7%<br>• Quality standard deviation: 20% |
| HCA Information: | • Successful, ratio: 56%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| 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): | 5.829117662846915 |
| 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: | eCooEFZfZJ.exe |
| File size: | 196608 |
| MD5: | 2db978e7cd2512c358518b1981fee079 |
| SHA1: | 22736d8d3ffe0e79cfdc0c08187bdae652d3a23c |
| SHA256: | 9ec05fd611c2df63c12cc15df8e87e411f358b7a6747a44d4a320c01e3367ca8 |
| SHA512: | 5997658234b2c8a07838610c82085838b02bc9b548b6fb22414bf278b0cd23643336346ebf4cc654c230dc36f90397750e199574ad090f30e496db6a4fd8540f |
| SSDEEP: | 1536:WNwYHz6OVtodLOhD0rd7NOG9jwvEJdx+hE+1nvK+LDWiYmGPeR2pB/uA0sicOnyQ:cH6OVt2LvdpJnJiv1CKWy8p4ALipl5Z |
| 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....N.Z....................0......0.............@................ |

## File Icon

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

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x401f30 |
| 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: | 0x5A004E93 [Mon Nov  6 11:59:15 2017 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: | 51114cc98630aad2088aa48f6e7a2e19 |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x2c16c | 0x2d000 | False | 0.311729600694 | data | 6.01771014226 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .data | 0x2e000 | 0x12ac | 0x1000 | False | 0.00634765625 | data | 0.0 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x30000 | 0x950 | 0x1000 | False | 0.172119140625 | data | 2.02186622034 | 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: eCooEFZfZJ.exe PID: 5600 Parent PID: 5728

### General

| | |
|---|---|
| Start time: | 08:54:00 |
| Start date: | 11/06/2021 |
| Path: | C:\Users\user\Desktop\eCooEFZfZJ.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\eCooEFZfZJ.exe' |
| Imagebase: | 0x400000 |
| File size: | 196608 bytes |
| MD5 hash: | 2DB978E7CD2512C358518B1981FEE079 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Yara matches: | • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.755211123.00000000021B0000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

# Disassembly

## Code Analysis

Joe Sandbox Cloud Basic 32.0.0 Black Diamond