

JoeSandbox Cloud BASIC



**ID:** 502075

**Sample Name:**

REQUIREMENT.exe

**Cookbook:** default.jbs

**Time:** 15:36:14

**Date:** 13/10/2021

**Version:** 33.0.0 White Diamond




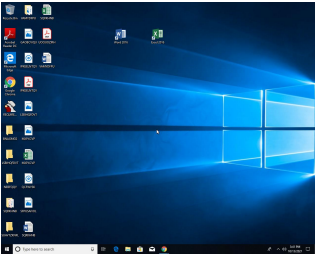
## Table of Contents

Table of Contents	2
Windows Analysis Report REQUIREMENT.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	4
AV Detection:	4
Networking:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	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	6
Contacted Domains	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
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	8
General	8
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	9
System Behavior	9
Analysis Process: REQUIREMENT.exe PID: 6976 Parent PID: 900	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

# Windows Analysis Report REQUIREMENT.exe

## Overview

### General Information

Sample Name:	REQUIREMENT.exe
Analysis ID:	502075
MD5:	fb70ff484021669...
SHA1:	6820b136319676..
SHA256:	2b40757a6763aa..
Tags:	exe guloader
Infos:	  
Most interesting Screenshot:	
	

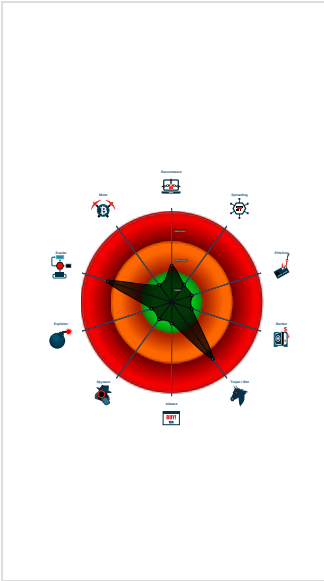
### Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div>	
<div>GuLoader</div>	
Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

### Signatures

Found malware configuration
Yara detected GuLoader
Found potential dummy code loops (...)
Tries to detect virtualization through...
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 ...
Abnormal high CPU Usage
Detected potential crypto function

### Classification



## Process Tree

- System is w10x64
-  REQUIREMENT.exe (PID: 6976 cmdline: 'C:\Users\user\Desktop\REQUIREMENT.exe' MD5: FB70FF484021669624233D0FBD77EC6A)
- cleanup

## Malware Configuration

### Threatname: GuLoader

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

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1188115207.0000000002C 50000.00000040.00000001.sdmf	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

## Networking:



## C2 URLs / IPs found in malware configuration

### Data Obfuscation:



## Yara detected GuLoader

## Malware Analysis System Evasion:



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

## Anti Debugging:

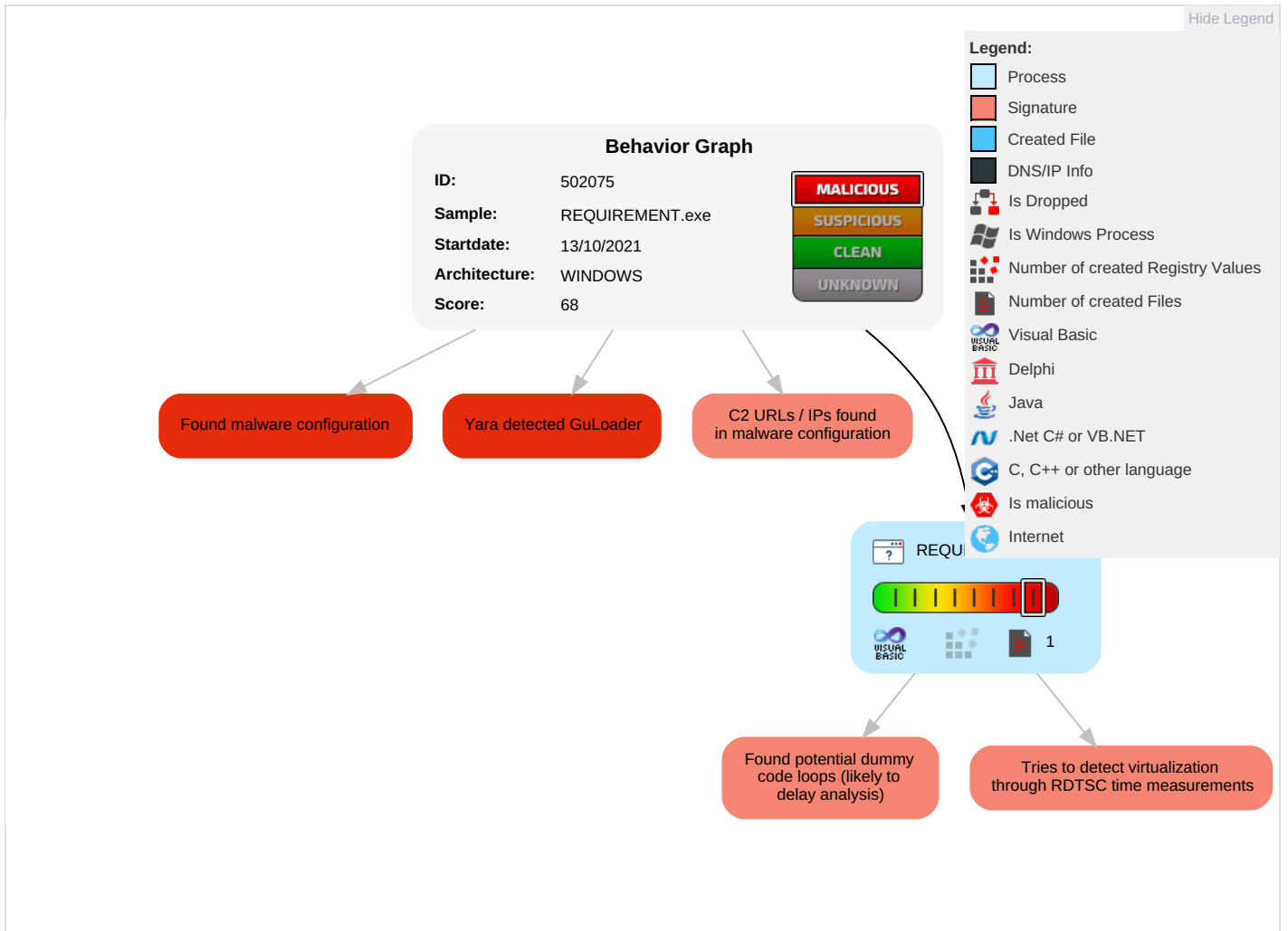


**Found potential dummy code loops (likely to delay analysis)**

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection <span>1</span>	Virtualization/Sandbox Evasion <span>1</span> <span>1</span>	OS Credential Dumping	Security Software Discovery <span>2</span> <span>1</span>	Remote Services	Archive Collected Data <span>1</span>	Exfiltration Over Other Network Medium	Encrypted Channel <span>1</span>	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection <span>1</span>	LSASS Memory	Virtualization/Sandbox Evasion <span>1</span> <span>1</span>	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol <span>1</span>	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information <span>1</span>	Security Account Manager	Process Discovery <span>1</span>	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery <span>1</span> <span>1</span>	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

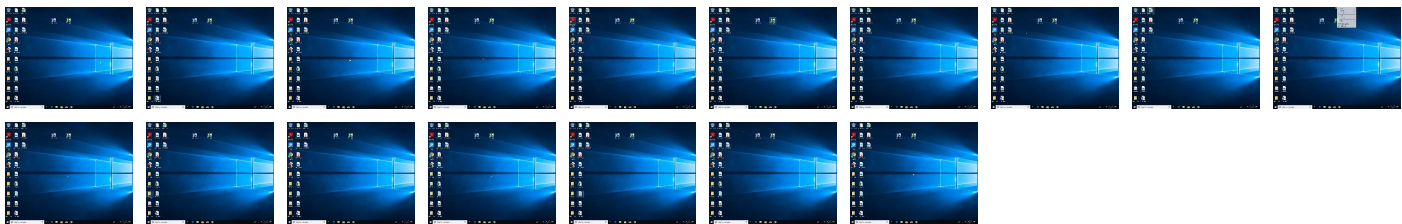
## Behavior Graph



## 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

No Antivirus matches

### 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:	33.0.0 White Diamond
Analysis ID:	502075
Start date:	13.10.2021
Start time:	15:36:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	REQUIREMENT.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:	mal68.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 35.8% (good quality ratio 16.8%)</li><li>• Quality average: 28.9%</li><li>• Quality standard deviation: 35.7%</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


No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.945342837977056
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:	REQUIREMENT.exe
File size:	102400
MD5:	fb70ff484021669624233d0fbd77ec6a
SHA1:	6820b13631967663ec2637c43c828468633051fd
SHA256:	2b40757a6763aa725d86426ce3cd16fcf1380a9152837d4f5e5b085710054c
SHA512:	57bcac78a12191df511dbb96f6d494096b56f269c3d009f373993574ff529698239bcc886dcc10ef162ef0c1d9ac0a4c6008813dc88becf4db8c700c35c0f47e
SSDEEP:	1536:tWD8iCOQRnNBM9rJvWMYwWjkuIM6AnhmXDLZBD:tW4iCOING9rAMy+M6KYB
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......i..... .....*.....Rich.....PE..L...& Q..... P...0.....X.....`.....@.....

File Icon

	
Icon Hash:	69e1c892f664c884

Static PE Info

General

Entrypoint:	0x401378
Entrypoint Section:	.text
Digitally signed:	false



<b>General</b>	
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x51B926D4 [Thu Jun 13 01:56:36 2013 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:	669316531b5190f02843878b6ed87394

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x14fe8	0x15000	False	0.514962332589	data	6.38314027792	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x16000	0xd0c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x1cb2	0x2000	False	0.348388671875	data	3.76635467806	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

## General

Start time:	15:37:10
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\REQUIREMENT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\REQUIREMENT.exe'
Imagebase:	0x400000
File size:	102400 bytes
MD5 hash:	FB70FF484021669624233D0FBD77EC6A
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: 00000000.00000002.1188115207.0000000002C50000.00000040.00000001.sdmp, Author: Joe Security</li></ul>
Reputation:	low

## File Activities

[Show Windows behavior](#)

## Disassembly

## Code Analysis