

JoeSandbox Cloud BASIC



**ID:** 502656

**Sample Name:** mU9H96igb3

**Cookbook:** default.jbs

**Time:** 08:27:11

**Date:** 14/10/2021

**Version:** 33.0.0 White Diamond

## Table of Contents

Table of Contents	2
Windows Analysis Report mU9H96igb3	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
System Summary:	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	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	10
Statistics	10
System Behavior	10
Analysis Process: mU9H96igb3.exe PID: 5184 Parent PID: 5372	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

# Windows Analysis Report mU9H96igb3

## Overview

### General Information

Sample Name:

mU9H96igb3 (renamed file extension from none to exe)

Analysis ID:

502656

MD5:

8777020a37b679..

SHA1:

a1ed1029b96729..

SHA256:

8a45d901cab57a..

Tags:

32

exe

trojan

Infos:

Most interesting Screenshot:

### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

88

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

### Signatures

Found malware configuration

Potential malicious icon found

Multi AV Scanner detection for subm...

Yara detected GuLoader

Tries to detect virtualization through...

C2 URLs / IPs found in malware con...

Found potential dummy code loops (...)

Machine Learning detection for samp...

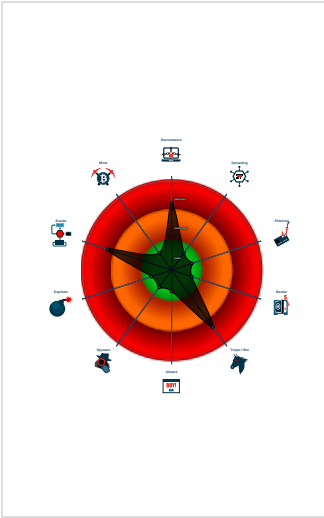
Uses 32bit PE files

Sample file is different than original ...

PE file contains strange resources

Contains functionality to read the PEB

### Classification



## Process Tree

- System is w10x64
- mU9H96igb3.exe (PID: 5184 cmdline: 'C:\Users\user\Desktop\mU9H96igb3.exe' MD5: 8777020A37B6797241A489A707B9784B)
- cleanup

## Malware Configuration

Threatname: GuLoader

```
{  "Payload URL": "http://implantecapilarpereira.com/NetGen"}
```

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1193811530.0000000004B F0000.00000040.00000001.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

Machine Learning detection for sample

## Networking:



C2 URLs / IPs found in malware configuration

## System Summary:



Potential malicious icon found

## Data Obfuscation:



Yara detected GuLoader

## Malware Analysis System Evasion:



Tries to detect virtualization through RDTS time measurements

## Anti Debugging:

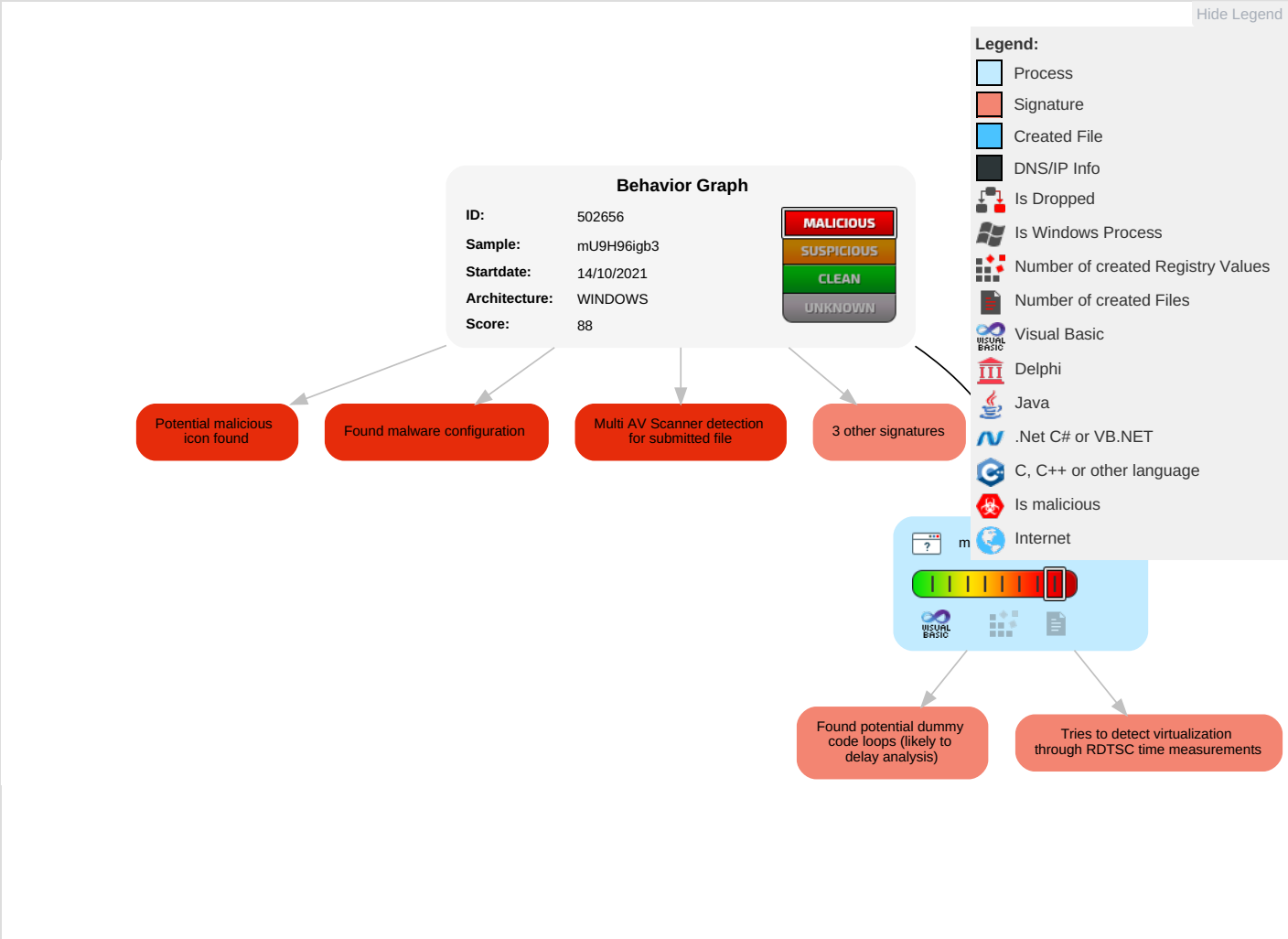


Found potential dummy code loops (likely to delay analysis)

## 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	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 2 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 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

## Behavior Graph





## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

Source	Detection	Scanner	Label	Link
mU9H96igb3.exe	33%	Virustotal		<a href="#">Browse</a>
mU9H96igb3.exe	26%	Metadefender		<a href="#">Browse</a>
mU9H96igb3.exe	24%	ReversingLabs	Win32.Trojan.Mucc	
mU9H96igb3.exe	100%	Joe Sandbox ML		

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

Source	Detection	Scanner	Label	Link
<a href="http://implantecapilarpereira.com/NetGen">http://implantecapilarpereira.com/NetGen</a>	0%	Avira URL Cloud	safe	

## Domains and IPs

### Contacted Domains

No contacted domains info

### Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://implantecapilarpereira.com/NetGen	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:	502656
Start date:	14.10.2021
Start time:	08:27:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mU9H96igb3 (renamed file extension from none to 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:	1
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:	mal88.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>Successful, ratio: 24.7% (good quality ratio 7.7%)</li><li>Quality average: 19.5%</li><li>Quality standard deviation: 31.3%</li></ul>
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none"><li>Adjust boot time</li><li>Enable AMSI</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):	4.14906794472717
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:	mU9H96igb3.exe
File size:	208896
MD5:	8777020a37b6797241a489a707b9784b
SHA1:	a1ed1029b967295f9ce5e9d219f41dc6c7fc4d1a
SHA256:	8a45d901cab57a1b65c32aea2452f56436dcf01c37bdf7875838e6054f395d90
SHA512:	0a9d13ca582dd72b4cdce8c91a5226aeb8c70ac7a73fa5f9775c6d03753bf7ec856371f55bf5f5e38f0a1d84e375c80916e5508f89d91e7100a82c4e544174d8
SSDEEP:	1536:tTEDegofhrRAnvzYFBWigYcgkOwijQkwY+EhBK DID:tQeZpR47YeigqVX+SK8
File Content Preview:	MZ.....@.....!..!Th is program cannot be run in DOS mode....\$......i..... .....*.....Rich.....PE..L.....R..... ...P..... .....@.....

File Icon



	
Icon Hash:	20047c7c70f0e004

### Static PE Info

#### General

Entrypoint:	0x40137c
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:	0x52EAF782 [Fri Jan 31 01:08:18 2014 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:	5daabd92eded5d2026efd3adb9b442c0

#### Entrypoint Preview

#### Data Directories

#### Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2d484	0x2e000	False	0.23853069803	data	4.22024266439	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2f000	0x13ec	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x31000	0x2526	0x3000	False	0.168375651042	data	2.83539382363	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: mU9H96igb3.exe PID: 5184 Parent PID: 5372

### General

Start time:	08:28:08
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\mU9H96igb3.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\mU9H96igb3.exe'
Imagebase:	0x400000
File size:	208896 bytes
MD5 hash:	8777020A37B6797241A489A707B9784B
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: 00000000.00000002.1193811530.0000000004BF0000.00000040.00000001.sdmp, Author: Joe Security</li></ul>
Reputation:	low

### File Activities

Show Windows behavior

## Disassembly

## Code Analysis