

JOeSandbox Cloud BASIC



**ID:** 500790

**Sample Name:** Foreign\_Bank  
Account Details.exe

**Cookbook:** default.jbs

**Time:** 09:27:23

**Date:** 12/10/2021

**Version:** 33.0.0 White Diamond

## Table of Contents

Table of Contents	2
Windows Analysis Report Foreign_Bank Account Details.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	3
AV Detection:	4
Networking:	4
System Summary:	4
Data Obfuscation:	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 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	8
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	9
System Behavior	10
Analysis Process: Foreign_Bank Account Details.exe PID: 3240 Parent PID: 6036	10
General	10
Disassembly	10
Code Analysis	10

# Windows Analysis Report Foreign\_Bank Account Detail...

## Overview

### General Information

Sample Name:

Foreign\_Bank Account Details.exe

Analysis ID:

500790

MD5:

8906fa5fed7b1d3..

SHA1:

f4488a79fcb657e..

SHA256:




d1a3f5513cfa50...

Tags:

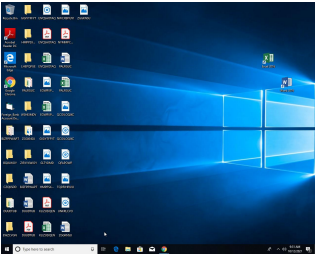
exe

guloader

Infos:

Most interesting Screenshot:



### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

80

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

### Signatures

Found malware configuration

Potential malicious icon found

Multi AV Scanner detection for subm...

Yara detected GuLoader

C2 URLs / IPs found in malware con...

Found potential dummy code loops (...)

Creates a DirectInput object (often fo...

Uses 32bit PE files

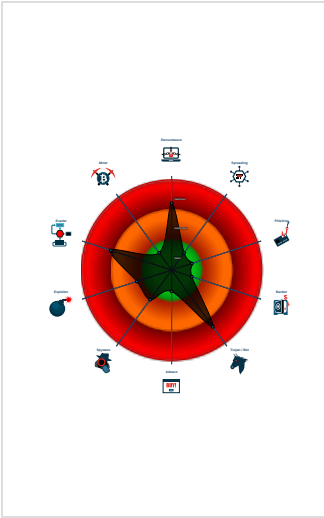
Found inlined nop instructions (likely...

Sample file is different than original ...

PE file contains strange resources


Contains functionality to read the PEB

### Classification



## Process Tree

System is w10x64

 Foreign\_Bank Account Details.exe (PID: 3240 cmdline: 'C:\Users\user\Desktop\Foreign\_Bank Account Details.exe' MD5: 8906FA5FED7B1D3D2E5579D97419C076)

cleanup

## Malware Configuration

Threatname: GuLoader

{

"Payload URL": "https://drive.google.com/uc?export=download&id=1hKAWruhccvaKL72"

}

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.766503580.00000000020C 0000.00000040.00000001.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

## Networking:



C2 URLs / IPs found in malware configuration

## System Summary:



Potential malicious icon found

## Data Obfuscation:



Yara detected GuLoader

## Anti Debugging:

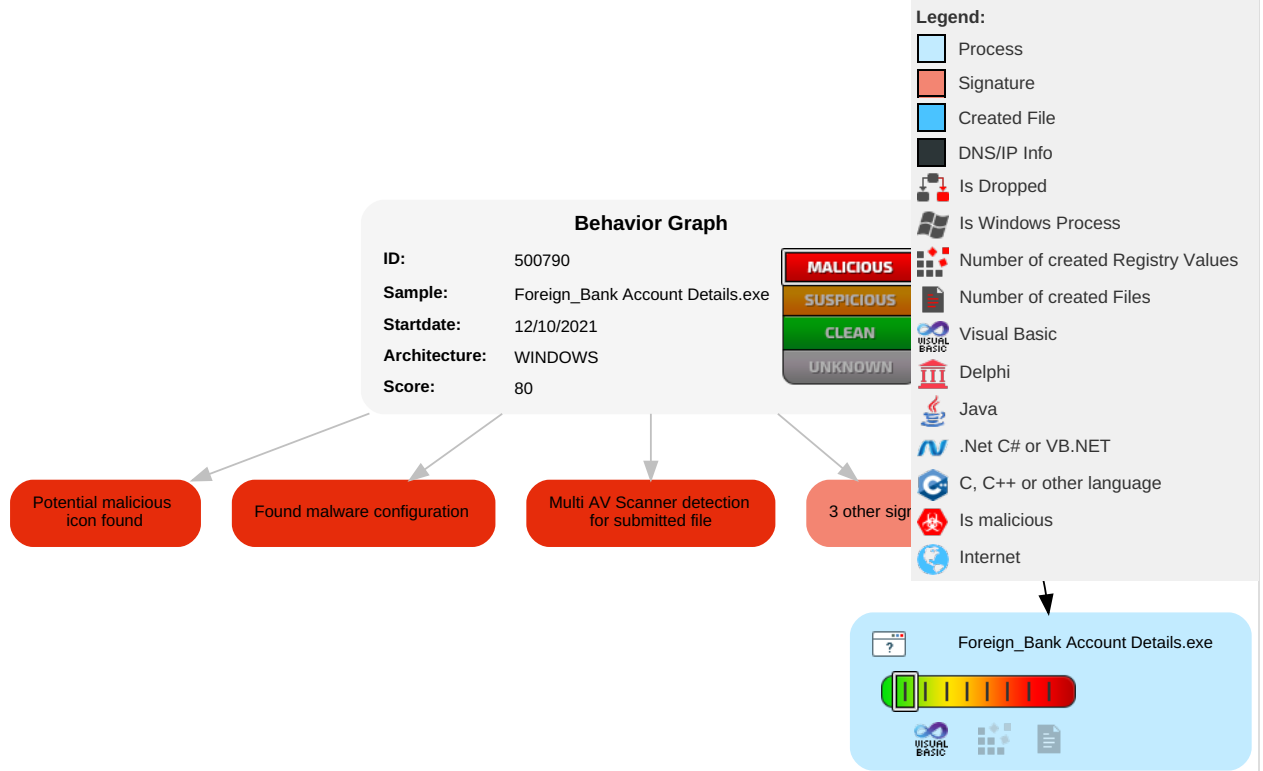


Found potential dummy code loops (likely to delay analysis)

## 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	Input Capture 1	Security Software Discovery 1 1	Remote Services	Input Capture 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	Archive Collected Data 1	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 2	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	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

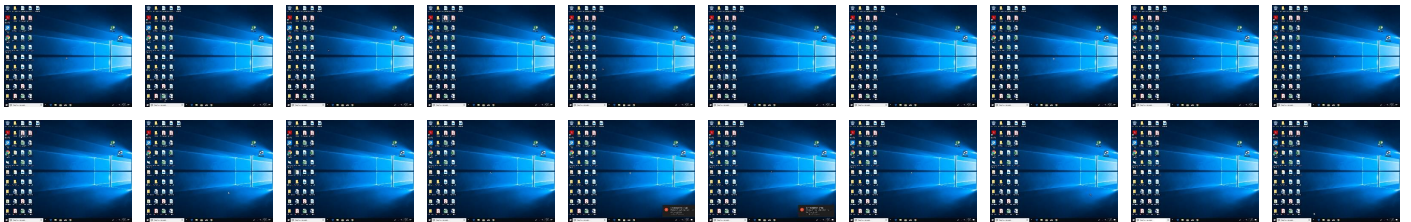
## Behavior Graph



## 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

Source	Detection	Scanner	Label	Link
Foreign_Bank Account Details.exe	33%	ReversingLabs	Win32.Trojan.FormBook	

### 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:	500790
Start date:	12.10.2021
Start time:	09:27:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Foreign_Bank Account Details.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:	29
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.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 37.3% (good quality ratio 17.3%)</li><li>• Quality average: 23.5%</li><li>• Quality standard deviation: 29.7%</li></ul>
HCA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 55%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>
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):	6.50003203322486
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:	Foreign_Bank Account Details.exe
File size:	135168
MD5:	8906fa5fed7b1d3d2e5579d97419c076
SHA1:	f4488a79fcb657eb1f3f23c6ce181ae7176fb11c
SHA256:	d1a3f5513cfaf506e96e6304d259fb03f5dc23542301fc9c7335a6e921ad65f9
SHA512:	e34aa27e530b1e57a33e483eca15739570b105485d722ca4a7a2f921abfe2383e5044d85bdd91e6d0ac80a5c3e88f6d6dc7ed5b662ddb1ab56c7c8349777871
SSDEEP:	3072:wHohMc/81QScUhU7FeiRaz+7kOMr7d2PhOdnXhWZ2QLqw9mh7ObETDuvTuqZccm4:wHoBzsuRcw4rCh
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode...\$.....+.[J...J. ..J..9V...J...h...J...l...J..Rich.J.....PE..L...].R..... .....P.....\.....@.....

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info



<b>General</b>	
Entrypoint:	0x4012d8
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:	0x5288055D [Sat Nov 16 23:53:01 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:	0a8e5f9658f839d07c08aa4f38837bac

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x14518	0x15000	False	0.578311011905	data	6.68181233004	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x16000	0x15fc	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x18000	0x9749	0xa000	False	0.217749023437	data	5.47873434424	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: Foreign\_Bank Account Details.exe PID: 3240 Parent PID: 6036

### General

Start time:	09:28:21
Start date:	12/10/2021
Path:	C:\Users\user\Desktop\Foreign_Bank Account Details.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Foreign_Bank Account Details.exe'
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	8906FA5FED7B1D3D2E5579D97419C076
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: 00000000.00000002.766503580.00000000020C0000.00000040.00000001.sdmp, Author: Joe Security</li></ul>
Reputation:	low

## Disassembly

### Code Analysis