

JoeSandbox Cloud BASIC



ID: 458685

Sample Name: BANK
DETAILS.exe

Cookbook: default.jbs

Time: 16:52:33

Date: 03/08/2021

Version: 33.0.0 White Diamond


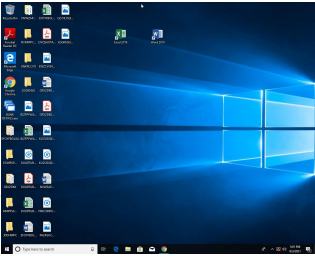
Table of Contents

Table of Contents	2
Windows Analysis Report BANK 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
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 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	10
System Behavior	10
Analysis Process: BANK DETAILS.exe PID: 5636 Parent PID: 5732	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

Windows Analysis Report BANK DETAILS.exe

Overview

General Information

Sample Name:	BANK DETAILS.exe
Analysis ID:	458685
MD5:	37ecfc300780ade..
SHA1:	4874e705a0a075..
SHA256:	552db26bdd2347..
Tags:	bat exe
Infos:	
Most interesting Screenshot:	
	

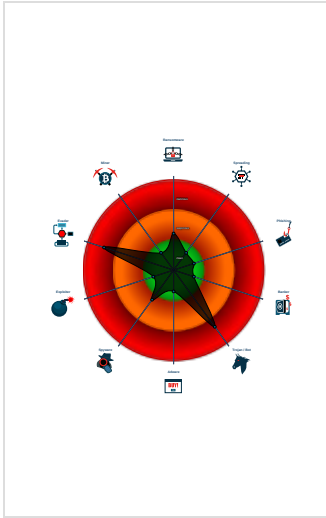
Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div>	
<div>GuLoader</div>	
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 call native f...
Contains functionality to query CPU ...

Classification



Process Tree

- System is w10x64
-  BANK DETAILS.exe (PID: 5636 cmdline: 'C:\Users\user\Desktop\BANK DETAILS.exe' MD5: 37ECFC300780ADE05B85FC969675E415)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1xfZvLwJHsJmtVI"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1308788382.00000000021 30000.00000040.00000001.sdm	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

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:

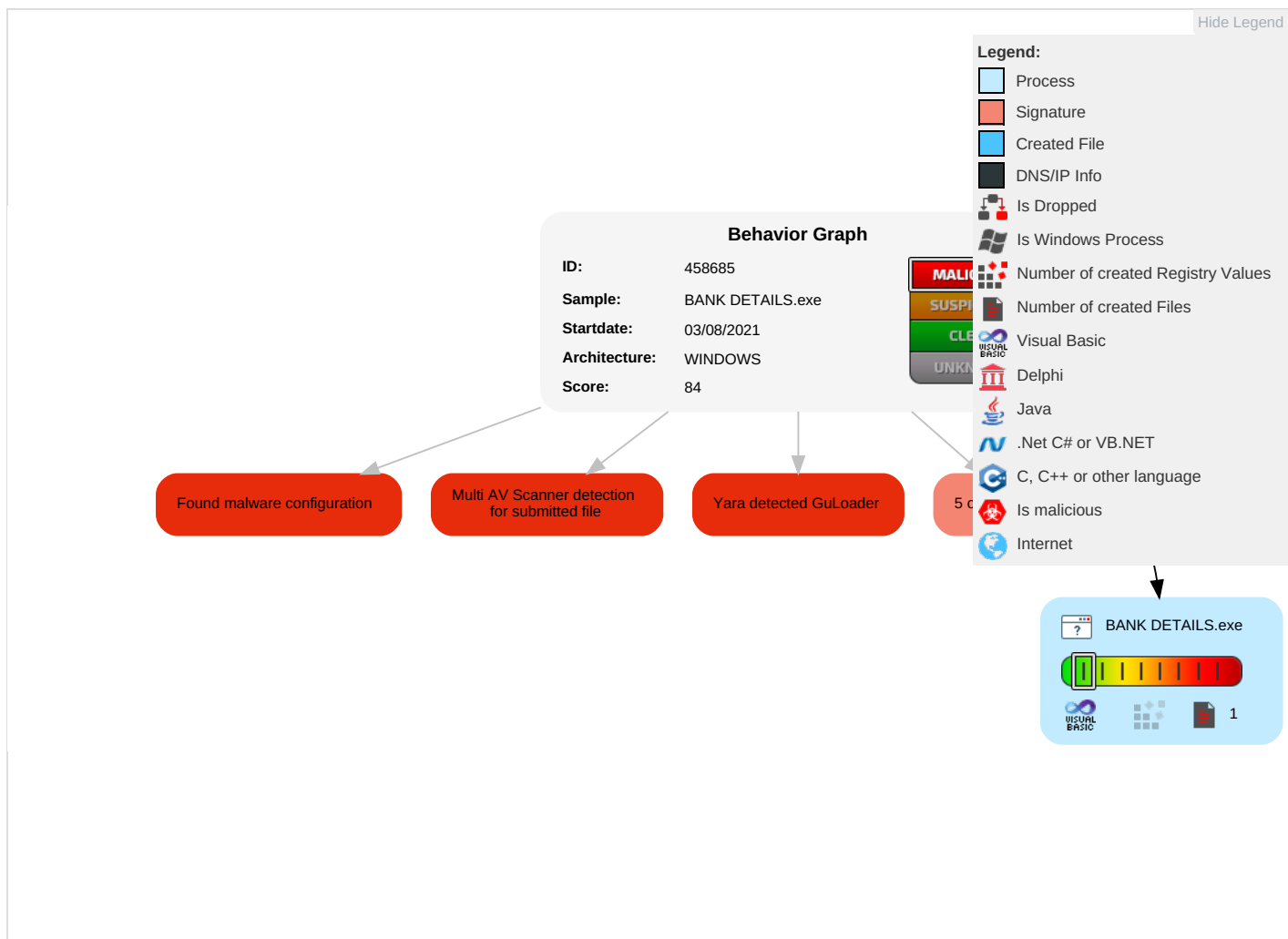


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
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	Recovery
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing 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)	Process Injection 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)	Obfuscated Files or Information 2	NTDS	System Information Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

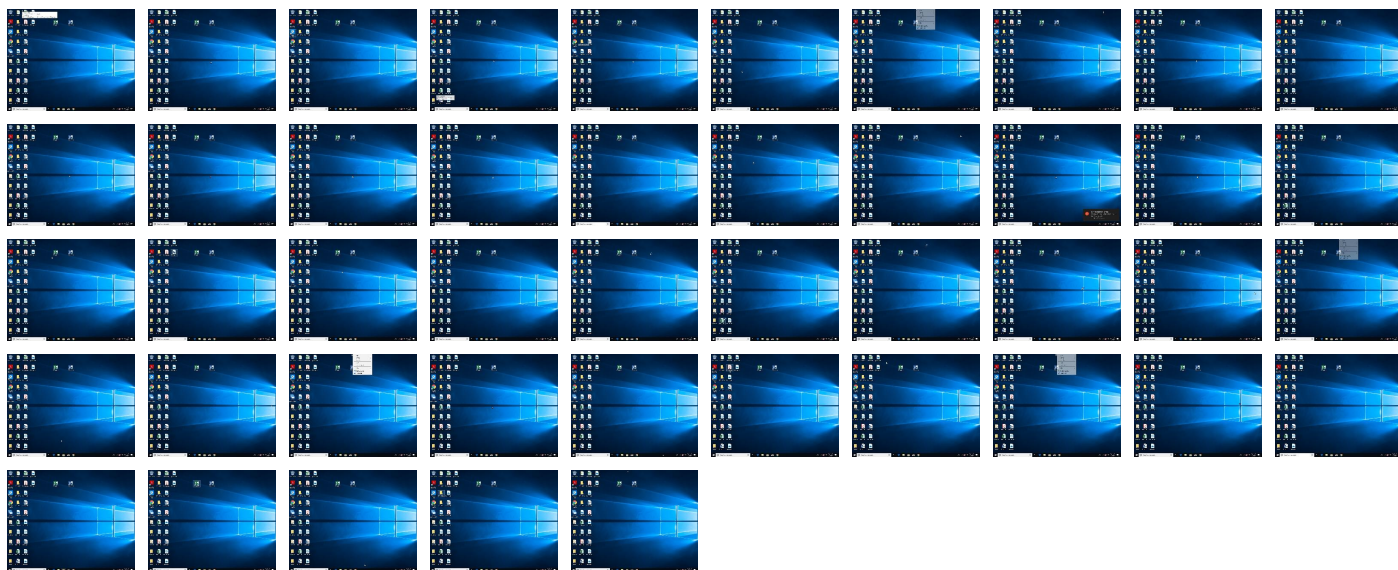
Behavior Graph



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
BANK DETAILS.exe	19%	Virustotal		Browse
BANK DETAILS.exe	15%	ReversingLabs	Win32.Trojan.Mucc	

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:	458685
Start date:	03.08.2021
Start time:	16:52:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BANK 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
Run name:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	40
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">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 16.5% (good quality ratio 5.7%)• Quality average: 22.8%• Quality standard deviation: 31.8%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .exe
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):	6.475587408087338
TrID:	<ul style="list-style-type: none">Win32 Executable (generic) a (10002005/4) 99.15%Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%Generic Win/DOS Executable (2004/3) 0.02%DOS Executable Generic (2002/1) 0.02%Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	BANK DETAILS.exe
File size:	114688
MD5:	37ecfc300780ade05b85fc969675e415
SHA1:	4874e705a0a075997da7d7bd8cf6f8608376600a
SHA256:	552db26bdd2347a216bb88e706ebf2bc9a145c8a5d38d082c53dcd2f344c162
SHA512:	4d0c2b9d0ce56400facd5955186441a62cde232db721584c1b97972fb133480e6d7a3b90daf01ce664b3b9e5216e25b548aeab014d20d3ec31555eb3504c831e
SSDEEP:	1536:UMxYU0ZIKPzkNY55AngpUS9UjoAXQXlIKUc3tsVHmwL+:!xYU0Z5PzYY557ORAV!xcKu
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.....K.....0.....@.....

File Icon

	
Icon Hash:	f67aedef6d0c0f98c

Static PE Info

General	
Entrypoint:	0x401530
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:	0x4B958B80 [Mon Mar 8 23:42:56 2010 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:	b28b105866cd7f6746798ef93a2371be

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1843c	0x19000	False	0.49474609375	data	6.81210830027	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1a000	0xb68	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1b000	0xfde	0x1000	False	0.3896484375	data	4.19517055589	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
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: BANK DETAILS.exe PID: 5636 Parent PID: 5732

General

Start time:	16:53:30
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\BANK DETAILS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BANK DETAILS.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	37ECFC300780ADE05B85FC969675E415
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1308788382.0000000002130000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis