ID: 379006
Sample Name: Bank details.exe
Cookbook: default.jbs
Time: 12:54:36
Date: 31/03/2021
Version: 31.0.0 Emerald

Table of Contents

Analysis Report Bank details.exe

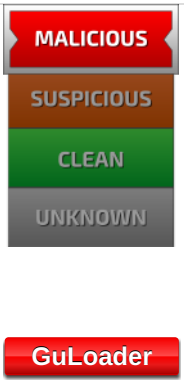
Overview

General Information

Sample Name:	Bank details.exe
Analysis ID:	379006
MD5:	2b96d5a21ce0c5..
SHA1:	aafbb78f4c8fdba…
SHA256:	33a9607ff967289..
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:

Detection

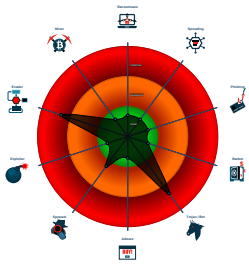


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Found potential dummy code loops (…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Creates a DirectInput object (often fo…
- Program does not show much activi…
- Sample file is different than original …
- Uses 32bit PE files
- Uses code obfuscation techniques (…

Classification



Startup

- **System is w10x64**
- Bank details.exe (PID: 6464 cmdline: 'C:\Users\user\Desktop\Bank details.exe' MD5: 2B96D5A21CE0C535E5558175F5157BC3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

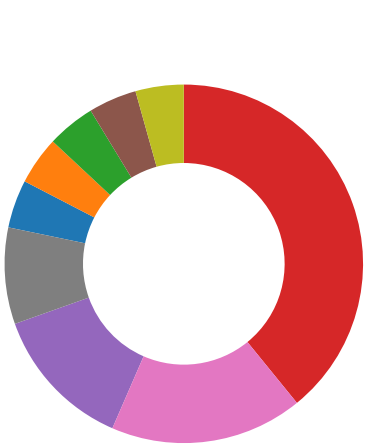
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Bank details.exe PID: 6464	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: Bank details.exe PID: 6464	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

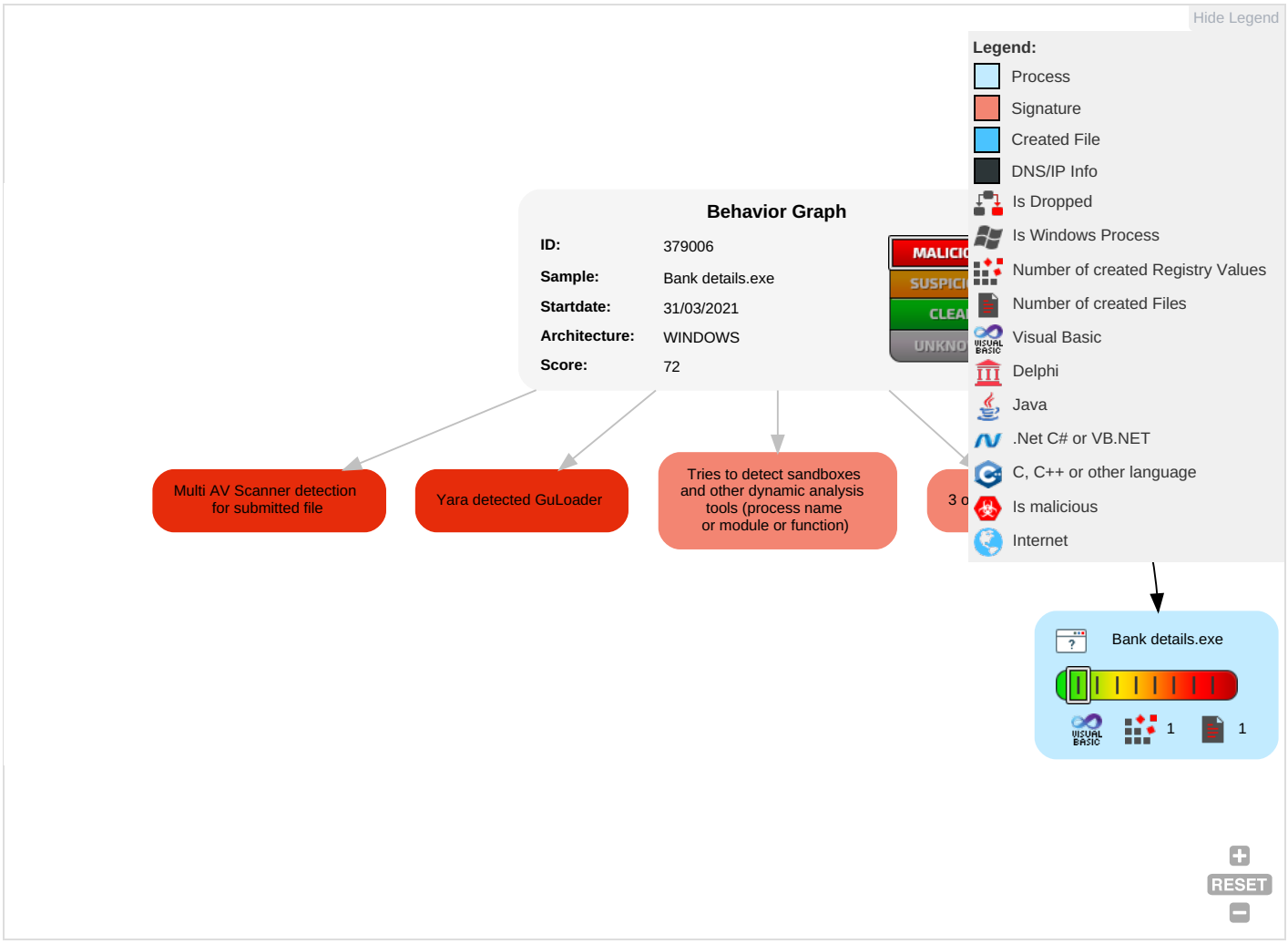
Anti Debugging:

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	Input Capture 1	Security Software Discovery 3 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Data Obfuscation	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	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	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	Process Discovery 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	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

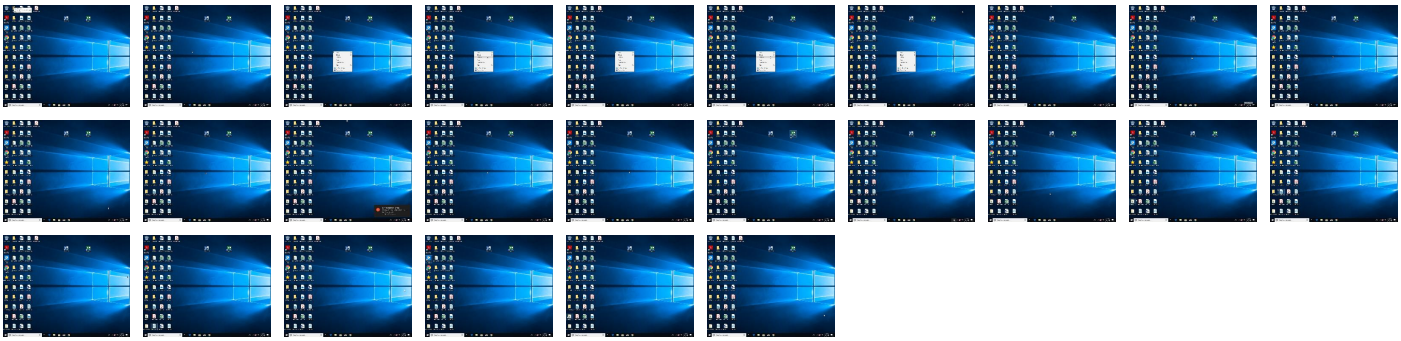
Behavior Graph



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

Source	Detection	Scanner	Label	Link
Bank details.exe	45%	Virustotal		Browse
Bank details.exe	48%	ReversingLabs	Win32.Trojan.Generic	

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:	31.0.0 Emerald
Analysis ID:	379006
Start date:	31.03.2021
Start time:	12:54:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 57s
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
Number of analysed new started processes analysed:	21
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 • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 96.7% (good quality ratio 56.7%) • Quality average: 39.2% • Quality standard deviation: 36%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found.

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):	4.702089907294954
TrID:	• 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:	131072
MD5:	2b96d5a21ce0c535e5558175f5157bc3
SHA1:	aafbb78f4c8fdba1354636f9a83affc3a55223c0
SHA256:	33a9607ff9672894cd9bf3fd3ba21dde6a220de4601c2da9479a9e059764d35b
SHA512:	b14039e3e039b1df7cfc109b2d8ef7c0850e9e307321ac5d40bbb7c565f92994dca27632995f4333f78830a91a21784c5ff402bc15885d69a1d3c61acbb1f808
SSDEEP:	1536:GLLlVJNiYwvn8qE4FnN8t/FAwBDffPz4gQkCt:GLLlZoU4FnN8dFAQX745kC
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L...;.WN.....`.....@.....

File Icon

Icon Hash:	d230f0e47064cc00

Static PE Info

General

Entrypoint:	0x4013d8
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:	0x4E570E3B [Fri Aug 26 03:08:43 2011 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:	399e3e9a5cc2cd2a186a8a2e044492e1

Entrypoint Preview

Instruction
push 00414A2Ch
call 00007FD140772F73h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], dh
stosd
popad
sbb ebp, ebx
sbb dword ptr [ebx], esp
dec esi
lea ecx, dword ptr [eax+77C97133h]
jne 00007FD140772FD5h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
push eax
dec edi
dec esp
inc ecx
push edx
dec ecx
push ebx

Instruction
inc ebp
push edx
dec ecx
dec esi
inc edi
push ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
adc al, 73h
mov bl, 17h
out 69h, al
or esi, esi
dec edi
mov ds, word ptr [ecx-07h]
fld1
pop eax
loop 00007FD140772FCAh
xchg eax, ebp
adc dword ptr [57EA1D52h], 4Ah
stosd
and dword ptr [edi], edi
fiadd dword ptr [ebx+34h]
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
mov byte ptr [32620001h], dh
add dword ptr [eax], eax
add byte ptr [eax], cl
add byte ptr [esi+61h], dl
outsb
add byte ptr fs:[72000701h], cl
outsd
jns 00007FD140772FE3h
insb
insb

Data Directories

Name	Virtual Address	Virtual Size	Is in Section

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1a494	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1d000	0x3ebc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x128	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x19954	0x1a000	False	0.307626577524	data	5.04046635888	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1b000	0x1930	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1d000	0x3ebc	0x4000	False	0.292724609375	data	3.31942687693	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1e814	0x26a8	data		
RT_ICON	0x1db6c	0xca8	data		
RT_ICON	0x1d424	0x748	data		
RT_GROUP_ICON	0x1d3f4	0x30	data		
RT_VERSION	0x1d150	0x2a4	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaVarForInit, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaI2Str, __vbaFPException, _CIlog, __vbaFileOpen, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarDup, __vbaFpI4, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, __vbaLateIdSt, _CItan, __vbaVarForNext, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	Resiccate2
FileVersion	9.04.0012
CompanyName	Jelly MUX, Inc.
Comments	Jelly MUX
ProductName	Jelly MUX
ProductVersion	9.04.0012
FileDescription	Jelly MUX
OriginalFilename	Resiccate2.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map

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: Bank details.exe PID: 6464 Parent PID: 5996

General

Start time:	12:55:23
Start date:	31/03/2021
Path:	C:\Users\user\Desktop\Bank details.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Bank details.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	2B96D5A21CE0C535E5558175F5157BC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis