ID: 356481
Sample Name:
Hotelization1.exe
Cookbook: default.jbs
Time: 08:42:26
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

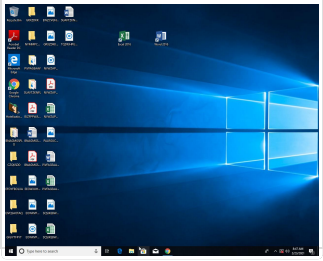
Analysis Report Hotelization1.exe

Overview

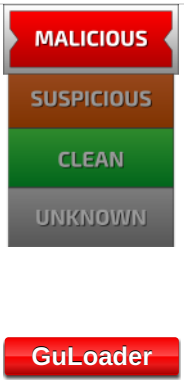
General Information

Sample Name:	Hotelization1.exe
Analysis ID:	356481
MD5:	e9fe79268216478.
SHA1:	ec474df86437d7d.
SHA256:	0b2d52ea23f3479.
Tags:	exe GuLoader

Most interesting Screenshot:



Detection



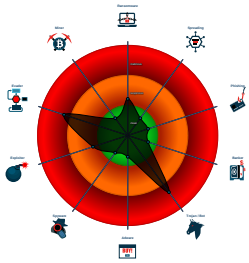
GuLoader

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to read the PEB
- Detected potential crypto function
- Found inlined nop instructions (likely…
- Uses 32bit PE files
- Uses code obfuscation techniques (…

Classification



Startup

- **System is w10x64**
- Hotelization1.exe (PID: 3360 cmdline: 'C:\Users\user\Desktop\Hotelization1.exe' MD5: E9FE792682164781809BECEA8A7A3902)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

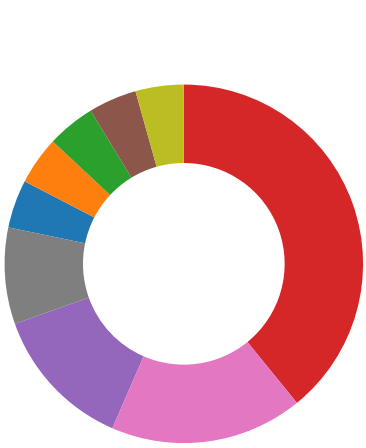
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Hotelization1.exe PID: 3360	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: Hotelization1.exe PID: 3360	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

Compliance:

Uses 32bit PE files

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

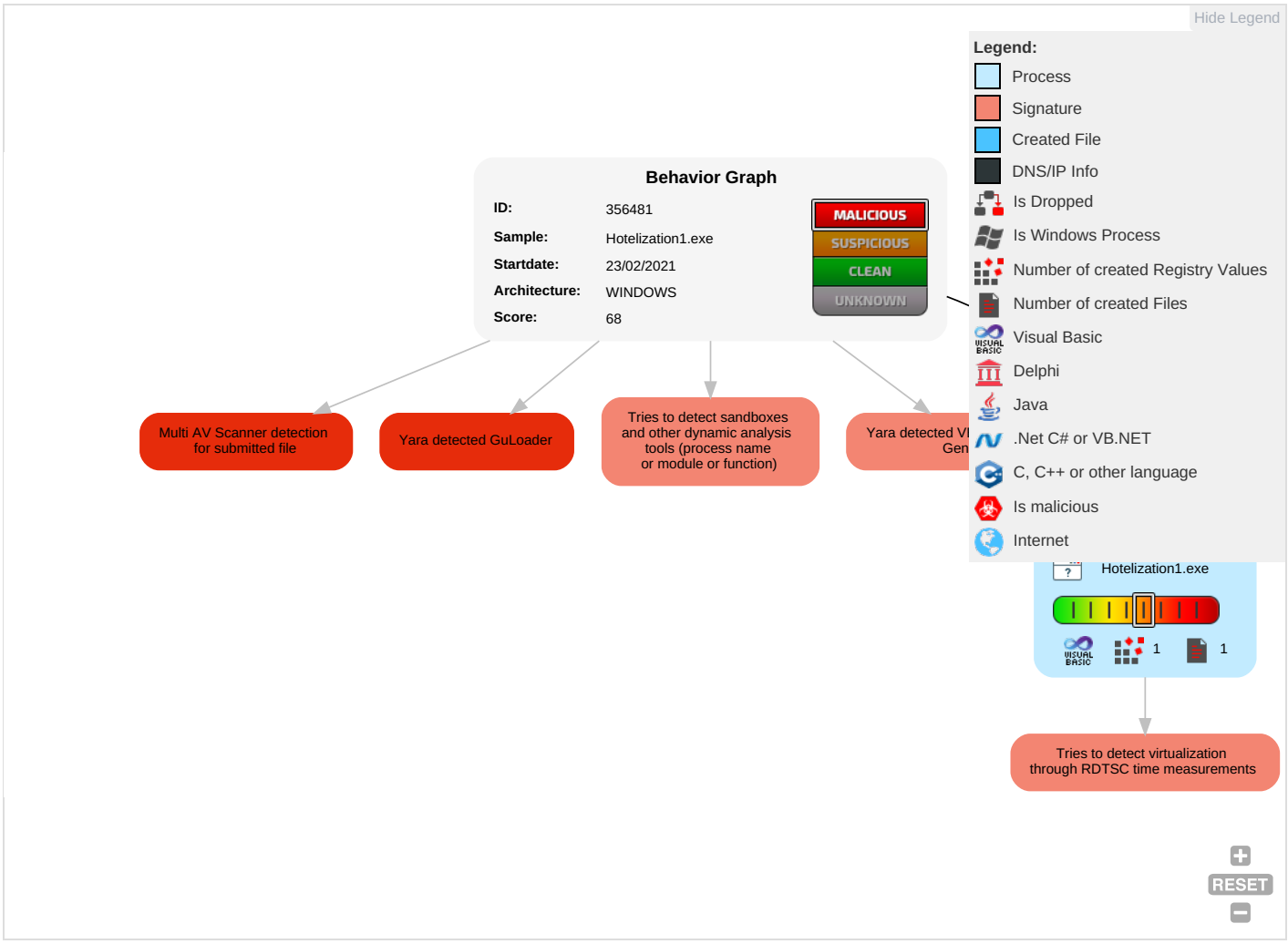
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Process Injection 1	OS Credential Dumping	Security Software Discovery 2 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 2	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

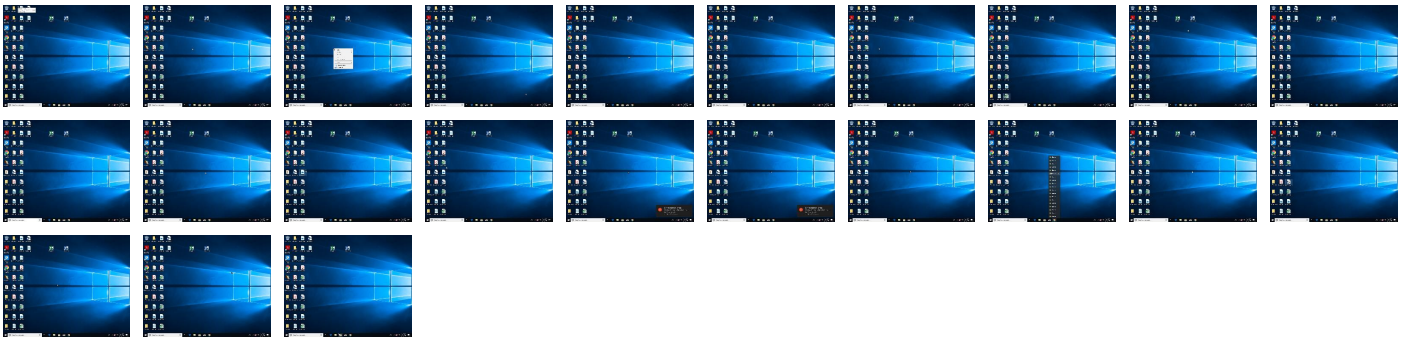
Behavior Graph



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
Hotelization1.exe	21%	ReversingLabs	Win32.Worm.Wbvb	

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:	356481
Start date:	23.02.2021
Start time:	08:42:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Hotelization1.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:	16
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:	mal68.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.3% (good quality ratio 11.7%) • Quality average: 23.9% • Quality standard deviation: 25.3%
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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe

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):	5.478532768183019
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:	Hotelization1.exe
File size:	73728
MD5:	e9fe792682164781809becea8a7a3902
SHA1:	ec474df86437d7d85b23b1e45de5b1c250ab56d6
SHA256:	0b2d52ea23f34796033d9d4f2bc2de17ad413e7fb82089faf7c55bc454a192cf
SHA512:	5b399ebeef7b57a787f84f4e0b1b76818b6f4732f0099abebcd65a4cf8eed9874b9b0dacadb7d581c3afb4c1f61d598a91e4e04f4056a98e658f00c65d6240c8
SSDEEP:	1536:mZD/Ptb05trMj2cCGQnaOSRlZTbUYJ9nGEOWD:mZjdOtOtCGQnaO0lpbU+NGEOW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L.....T.....0.....@.....

File Icon

Icon Hash:	1e74f2ea62e4a082

Static PE Info

General

Entrypoint:	0x401494
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:	0x54B5CFAE [Wed Jan 14 02:08:46 2015 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:	b84199caadebcbcd5f63d7b7de7ff518

Entrypoint Preview

Instruction
push 0040A108h
call 00007F65609EE103h
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-6EB4BD71h], ah
dec edx
dec esi
stosb
mov cl, 2Eh
fcom st(0), st(2)
movsb
xchg byte ptr [ebp+00h], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [edx+6Fh], dl
je 00007F65609EE181h
je 00007F65609EE17Bh
insb
insb
jnc 00007F65609EE112h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
or esp, ecx
sbb byte ptr [ebx-50409C5Eh], cl
inc ebx
cmpsb
popfd
fild dword ptr [ebx+775E5EDAh]
jp 00007F65609EE0AAh
mov esi, BE15D362h
dec esi
mov al, byte ptr [ebx]
sbb dword ptr [edi+73F8EEF4h], ebx
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
jnc 00007F65609EE09Dh
add byte ptr [eax], al
adc eax, 00000009h
or al, byte ptr [eax]
imul ebp, dword ptr [esp+ebp*2+61h], 62617370h
insb
add byte ptr [42000901h], cl
imul ebp, dword ptr [esp+ebp*2+65h], 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf214	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x12000	0xc14	.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	0x150	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xe7b4	0xf000	False	0.399593098958	data	6.01634189749	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x10000	0x1218	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x12000	0xc14	0x1000	False	0.264892578125	data	2.91279049322	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1236c	0x8a8	data		
RT_GROUP_ICON	0x12358	0x14	data		
RT_VERSION	0x120f0	0x268	MS Windows COFF Motorola 68000 object file	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaLenBstr, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaVarForInit, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaVarTstEq, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, __vbaUI1I2, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaErrorOverflow, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaLateMemCall, __vbaStrToAnsi, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, _CItan, __vbaVarForNext, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	Hotelization1
FileVersion	1.00
CompanyName	Log
ProductName	Log Inverter
ProductVersion	1.00
FileDescription	Log Inverter
OriginalFilename	Hotelization1.exe

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: Hotelization1.exe PID: 3360 Parent PID: 5636

General

Start time:	08:43:18
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Hotelization1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Hotelization1.exe'
Imagebase:	0x400000
File size:	73728 bytes
MD5 hash:	E9FE792682164781809BECEA8A7A3902
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 Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\TANKRENSNING	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\TANKRENSNING\Sequences	success or wait	1	660E2872	RegCreateKeyW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\TANKRENSNING\Sequences	Koinciderede4	unicode	MS Sans Serif	success or wait	1	660E2183	RegSetValueExW

Disassembly

Code Analysis