ID: 355935
Sample Name:
EM_B43454933_7621780_573.exe
Cookbook: default.jbs
Time: 09:40:13
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

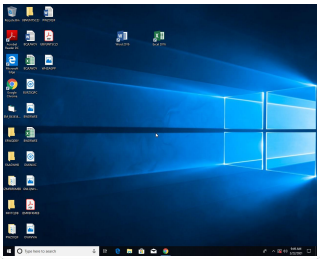
Analysis Report EM_B43454933_7621780_573.exe

Overview

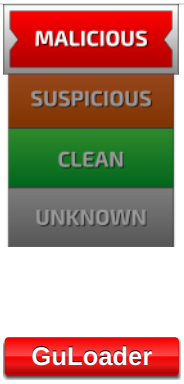
General Information

Sample Name:	EM_B43454933_7621780_573.exe
Analysis ID:	355935
MD5:	b679e85b64a7b5..
SHA1:	7c103c70859b5d..
SHA256:	a1677b7e54a0d6..

Most interesting Screenshot:



Detection

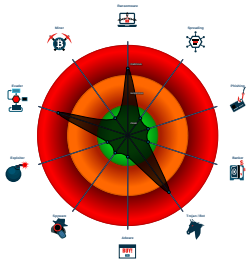


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- 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

Classification



Startup

- **System is w10x64**
- EM_B43454933_7621780_573.exe (PID: 7028 cmdline: 'C:\Users\user\Desktop\EM_B43454933_7621780_573.exe' MD5: B679E85B64A7B5851F0ABC9D69740978)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

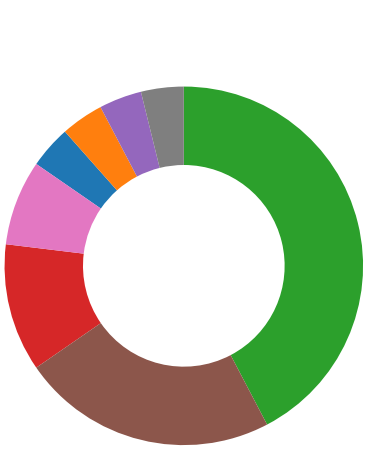
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: EM_B43454933_7621780_573.exe PID: 7028	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: EM_B43454933_7621780_573.exe PID: 7028	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

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

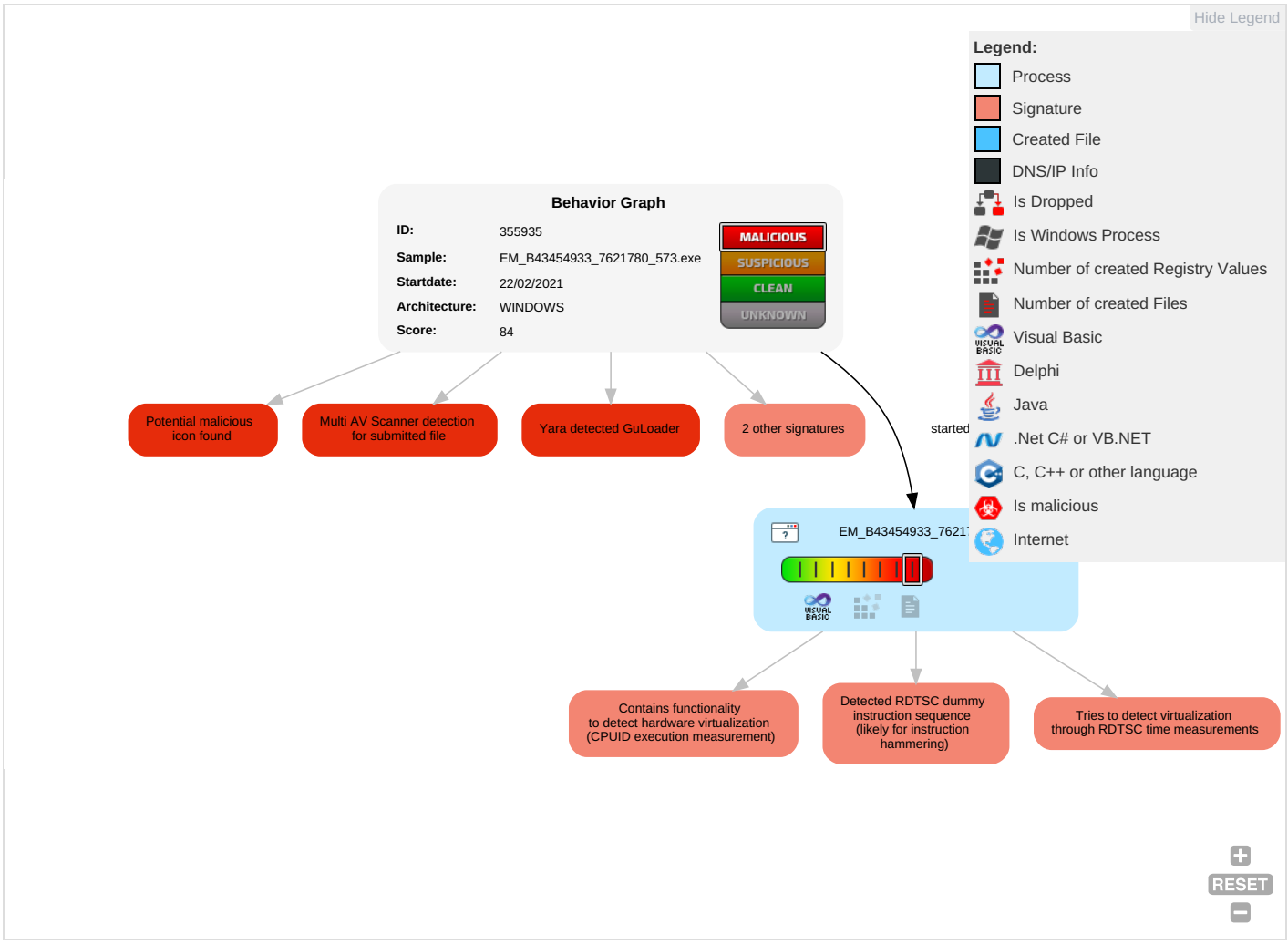
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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 4 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 1	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 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

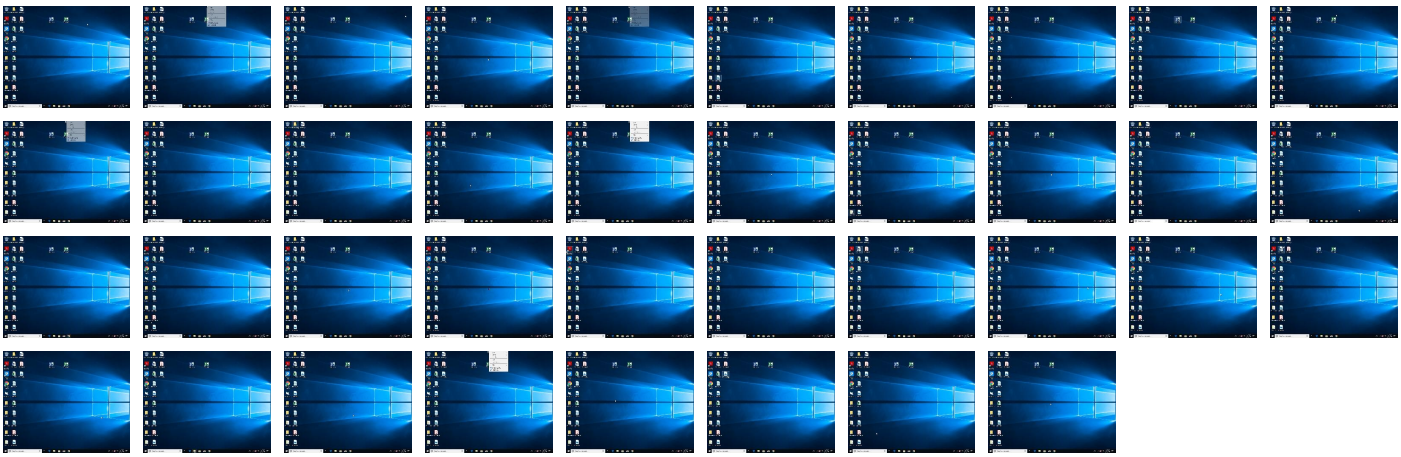
Behavior Graph



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
EM_B43454933_7621780_573.exe	19%	Virustotal		Browse
EM_B43454933_7621780_573.exe	4%	ReversingLabs		

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:	355935
Start date:	22.02.2021
Start time:	09:40:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	EM_B43454933_7621780_573.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:	27
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:	mal84.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 36.9% (good quality ratio 20.7%) • Quality average: 33.8% • Quality standard deviation: 35.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, RuntimeBroker.exe, wermgr.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.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):	5.299619096557311
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:	EM_B43454933_7621780_573.exe
File size:	65536
MD5:	b679e85b64a7b5851f0abc9d69740978
SHA1:	7c103c70859b5d708ae5ff82a65a67b71272df4d
SHA256:	a1677b7e54a0d67b9b16d0a0835187b889db434d77d8a8 f3f7714a86b01a27db
SHA512:	e40a30142c8d1232ae9157c588b26d4e0613ea01ec7636 e9c68fcf72c78a4b8815325f4fd0fda6271d7c3845424bcf 59b8671f4b7fb02b1ba595aba67d37aaed
SSDEEP:	768:X4vJqG24/Fh5pe7zWjlZnn6/fEApUHH9mCCg3YY P35R7jgVCm:oxqaF3pe7zWG0nHHtCgoW3f6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+O..E...E...E.X.K...E...L...E...H...E.Rich..E.....PE..L.....G.....0.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4013b0
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:	0x478A979E [Sun Jan 13 22:58:38 2008 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:	e040c8c04f7f9a83c53d48451cf696fa

Entrypoint Preview

Instruction
push 00401A50h
call 00007F409098EB93h
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 [esi+1CA7EB43h], dh
xchg eax, esp
jo 00007F409098EBEBh
mov edi, 6EEA2FE3h
add dword ptr [edi+0000006Ah], edi
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [edx+00h], al
push es
push eax
add dword ptr [ecx], 54h
jc 00007F409098EC03h
je 00007F409098EC08h
xor eax, dword ptr fs:[eax]
add byte ptr [eax], al
add ah, ah
sub dl, byte ptr [00000003h]
add bh, bh
int3
xor dword ptr [eax], eax
pop es
jp 00007F409098EBE5h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0xcee4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10000	0x9cc	.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	0x230	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xf8	.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	0xc368	0xd000	False	0.458646334135	data	5.98020239152	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xe000	0x1958	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x10000	0x9cc	0x1000	False	0.182373046875	data	2.14952458859	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1089c	0x130	data		
RT_ICON	0x105b4	0x2e8	data		
RT_ICON	0x1048c	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1045c	0x30	data		
RT_VERSION	0x10150	0x30c	data	Hungarian	Hungary

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaLateMemSt, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaCyStr, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaVarTstEq, __vbaObjVar, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaFpCmpCy, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaErrorOverflow, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaVarDup, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x040e 0x04b0
LegalCopyright	Copyright (C) Tulix
InternalName	Naticahartko
FileVersion	1.00
CompanyName	Tulix
LegalTrademarks	Copyright (C) Tulix
Comments	Tulix
ProductName	Tulix
ProductVersion	1.00
FileDescription	Tulix
OriginalFilename	Naticahartko.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
Hungarian	Hungary	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EM_B43454933_7621780_573.exe PID: 7028 Parent PID: 6068

General

Start time:	09:41:04
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\EM_B43454933_7621780_573.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\EM_B43454933_7621780_573.exe'
Imagebase:	0x400000
File size:	65536 bytes
MD5 hash:	B679E85B64A7B5851F0ABC9D69740978
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis