ID: 384221
Sample Name: Remodeller8.exe
Cookbook: default.jbs
Time: 18:53:53
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

Analysis Report Remodeller8.exe

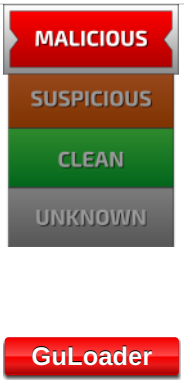
Overview

General Information

Sample Name:	Remodeller8.exe
Analysis ID:	384221
MD5:	147eeed85d5999..
SHA1:	15a85b8d36ec5b..
SHA256:	60bc4eef19e2c54..
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:

Detection

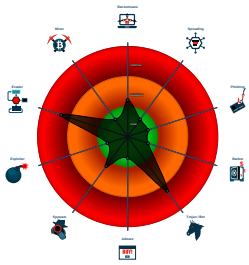


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Creates a DirectInput object (often fo…
- Detected potential crypto function
- PE file contains an invalid checksum
- PE file contains strange resources
- Program does not show much activi…
- Sample file is different than original …

Classification



Startup

- **System is w10x64**
- Remodeller8.exe (PID: 6860 cmdline: 'C:\Users\user\Desktop\Remodeller8.exe' MD5: 147EEED85D599916758D6BBA7D86B434)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

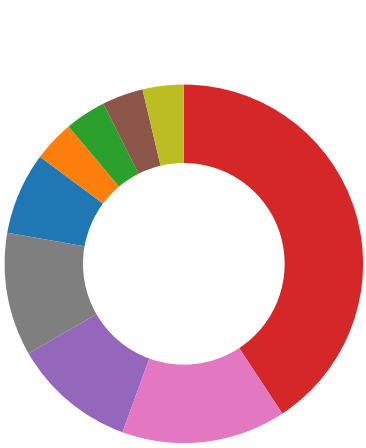
Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.847967336.0000000000530000.00000040.00000001.sdmp	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

Machine Learning detection for sample

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect virtualization through RDTSC time measurements

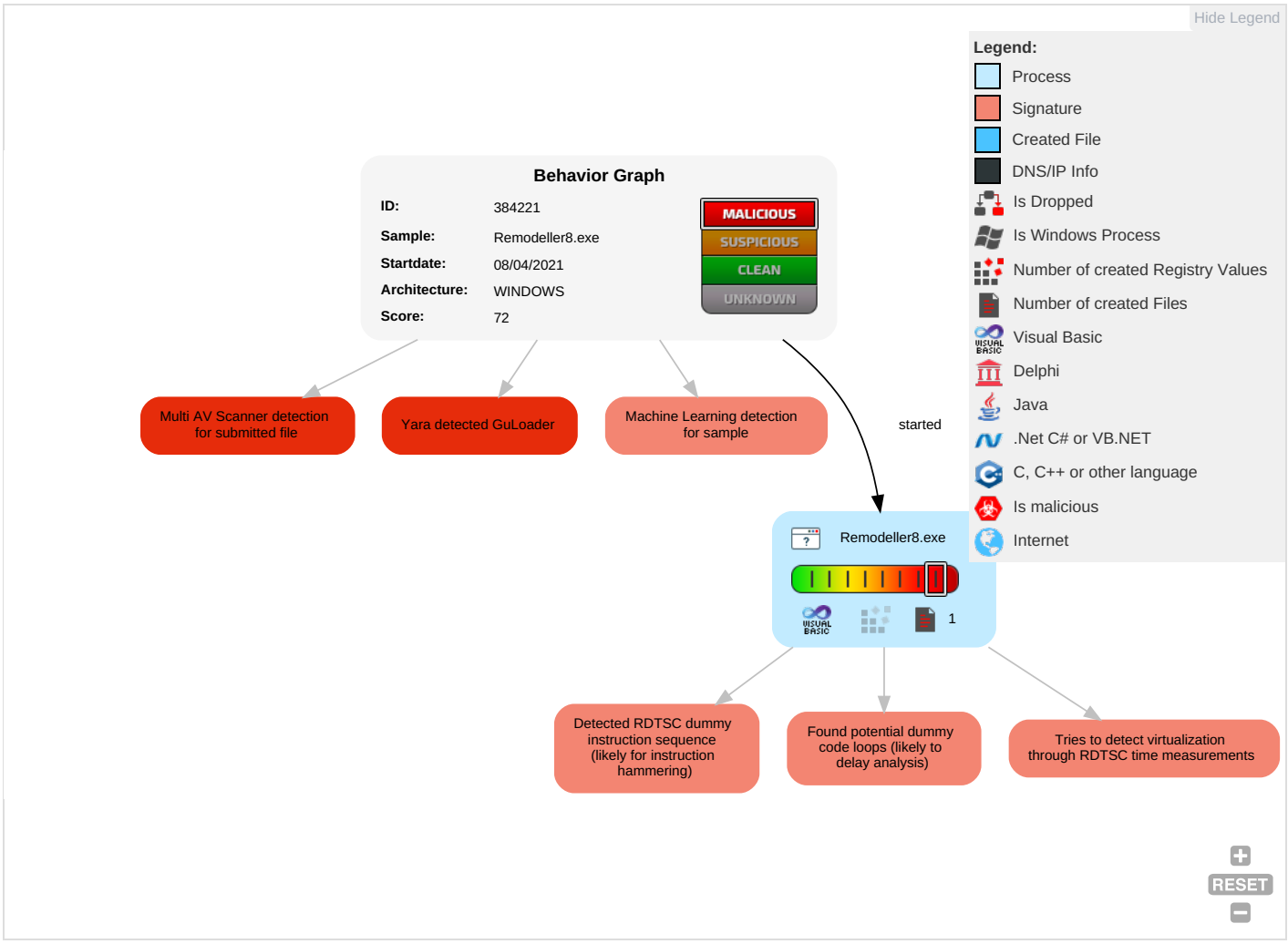
Anti Debugging:

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	Re Se Ef
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	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
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	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
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	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

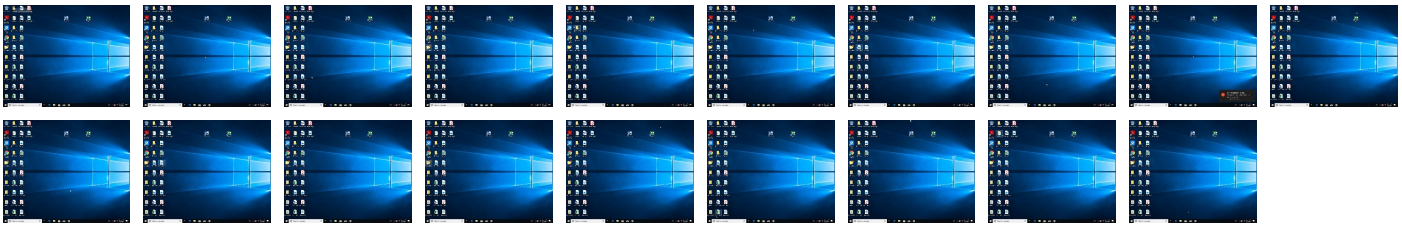
Behavior Graph



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
Remodeller8.exe	53%	Virustotal		Browse
Remodeller8.exe	56%	ReversingLabs	Win32.Trojan.GuLoader	
Remodeller8.exe	100%	Joe Sandbox ML		

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:	384221
Start date:	08.04.2021
Start time:	18:53:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Remodeller8.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:	20
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: 97.1% (good quality ratio 37%) • Quality average: 20.9% • Quality standard deviation: 30.2%
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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.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):	5.623110196923232
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:	Remodeller8.exe
File size:	110592
MD5:	147eeed85d599916758d6bba7d86b434
SHA1:	15a85b8d36ec5baeac941a32450026d610358961
SHA256:	60bc4eef19e2c547add07b45bdbd4aeb00ca75fe7269cac5fa71a8ceb87e5cb9
SHA512:	dfeeb831eac7d1e2f1f806cac44271a031f3457a8a844a2388cbcfa702c376dc8a98cbf5842bdc950eb70be123ff4cac15189d4b31942c6f96936e5f34d8b75d
SSDEEP:	1536:c11KYD/YRqwXvKQeCPd2vL2M/FPVm9vyIhyEDPVm9vDd2Mf2v:YKawq2vKQJP18VmHsEzVmy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....Y.....0.....@....@.....

File Icon

Icon Hash:	c0c6f2e0e4fefe3f

Static PE Info

General

Entrypoint:	0x4013e8
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:	0x59EB0BB4 [Sat Oct 21 08:56:20 2017 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:	d1ed0dda3501483d16a7ad09b76f3b08

Entrypoint Preview

Instruction
push 004111D8h
call 00007F0900AA8AE3h
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 dh, dh
mov byte ptr [ecx+0Eh], bh
shl dword ptr [ebx-0044BAFCh], 13h
mov dword ptr [00F560B8h], eax
add byte ptr [eax], al
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], 53h
jns 00007F0900AA8B5Eh
insb
outsd
imul esi, dword ptr [bp+di+61h], 6E6F6974h
add byte ptr [ebx], cl
add eax, dword ptr [eax]
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
or ebp, ebp
and dl, byte ptr [bp+di-2Dh]
pop ecx

Instruction
inc ebx
inc esi
xchg eax, ebx
push edi
dec edx
test eax, edx
mov byte ptr [edi-03h], ch
or al, 79h
sal byte ptr [eax+32h], 1
mov dword ptr [esi-73h], eax
xchg eax, ebp
mov bp, 593Bh
insb
test dword ptr [edx], edi
dec edi
lodsd
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
add byte ptr [eax], al
pushfd
cld
add byte ptr [eax], al
retf
cli
add byte ptr [eax], al
add byte ptr [ebx], dl
add byte ptr [ebp+6Dh], al
bound esp, dword ptr [ebp+64h]
jnc 00007F0900AA8B57h
imul esi, dword ptr [ebx+61h], 6Dh
imul ebp, dword ptr [esi+65h], 73656E72h
aaa

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x13604	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x16000	0x5c42	.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	

Name	Virtual Address	Virtual Size	Is in Section
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	0x108	.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	0x12aac	0x13000	False	0.417878803454	data	6.02715738089	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x14000	0x117c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x16000	0x5c42	0x6000	False	0.35986328125	data	5.27314891378	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1ad9a	0xea8	data		
RT_ICON	0x1a4f2	0x8a8	data		
RT_ICON	0x19f8a	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x179e2	0x25a8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x1693a	0x10a8	data		
RT_ICON	0x164d2	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x16478	0x5a	data		
RT_VERSION	0x161e0	0x298	data	Guarani	Paraguay

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaLineInputStr, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, _adj_fprem1, __vbaHresultCheckObj, __vbaLenBstrB, _adj_fdiv_m32, __vbaAryDestruct, __vbaOnError, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaChkstk, __vbaFileClose, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaObjVar, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaFileOpen, __vbaNew2, __vbaR8Str, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, _adj_fdivr_m32, _adj_fdiv_r, __vbaLateMemCall, __vbaVarAdd, __vbaVarDup, __vbaFpI4, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0474 0x04b0
InternalName	Remodeller8
FileVersion	1.00
CompanyName	Pana-sonic
Comments	Pana-sonic
ProductName	Pana-sonic
ProductVersion	1.00
FileDescription	Pana-sonic
OriginalFilename	Remodeller8.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Guarani	Paraguay	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Remodeller8.exe PID: 6860 Parent PID: 5980

General

Start time:	18:54:41
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\Remodeller8.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Remodeller8.exe'
Imagebase:	0x400000
File size:	110592 bytes
MD5 hash:	147EEED85D599916758D6BBA7D86B434
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000001.00000002.847967336.0000000000530000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis