ID: 383316
Sample Name: Orden de Compra.exe
Cookbook: default.jbs
Time: 16:14:52
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report Orden de Compra.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 4
Signature Overview 5
AV Detection: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
HIPS / PFW / Operating System Protection Evasion: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
General Information 8
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 10
General 10
File Icon 11
Static PE Info 11
General 11
Entrypoint Preview 11
Data Directories 12
Sections 13
Resources 13
Imports 13
Version Infos 13
Possible Origin 13
Network Behavior 14
UDP Packets 14

Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 16
Analysis Process: Orden de Compra.exe PID: 6960 Parent PID: 6044 16
General 16
File Activities 16
Analysis Process: RegAsm.exe PID: 5700 Parent PID: 6960 16
General 16
Analysis Process: RegAsm.exe PID: 2988 Parent PID: 6960 16
General 16
Analysis Process: RegAsm.exe PID: 784 Parent PID: 6960 17
General 17
Analysis Process: RegAsm.exe PID: 6128 Parent PID: 6960 17
General 17
File Activities 17
File Created 17
Analysis Process: conhost.exe PID: 5980 Parent PID: 6128 18
General 18
Disassembly 18
Code Analysis 18

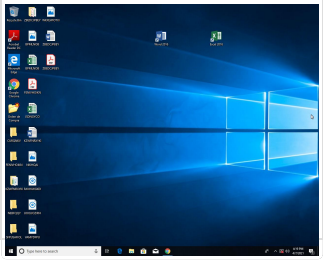
Analysis Report Orden de Compra.exe

Overview

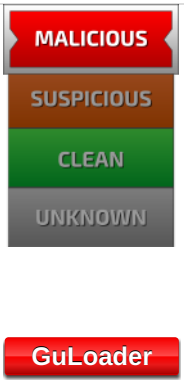
General Information

Sample Name:	Orden de Compra.exe
Analysis ID:	383316
MD5:	e6dcf6b66b611ff…
SHA1:	7b3871b1b077f76.
SHA256:	280e118484090c..
Infos:	

Most interesting Screenshot:



Detection



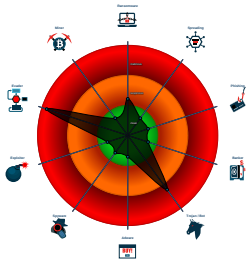
GuLoader

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Hides threads from debuggers
- Machine Learning detection for samp…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Writes to foreign memory regions

Classification



Startup

- **System is w10x64**
- Orden de Compra.exe (PID: 6960 cmdline: 'C:\Users\user\Desktop\Orden de Compra.exe' MD5: E6DCF6B66B611FFB7D2BC1A8045BF41F)
  - RegAsm.exe (PID: 5700 cmdline: 'C:\Users\user\Desktop\Orden de Compra.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 2988 cmdline: 'C:\Users\user\Desktop\Orden de Compra.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 784 cmdline: 'C:\Users\user\Desktop\Orden de Compra.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 6128 cmdline: 'C:\Users\user\Desktop\Orden de Compra.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 5980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

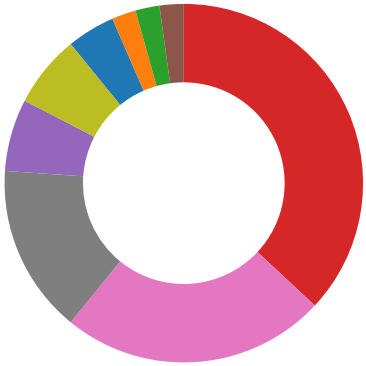
Memory Dumps

Source	Rule	Description	Author	Strings
00000017.00000002.849537125.0000000001100000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 6128	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

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:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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:

Contains functionality to hide a thread from the debugger

Found potential dummy code loops (likely to delay analysis)

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

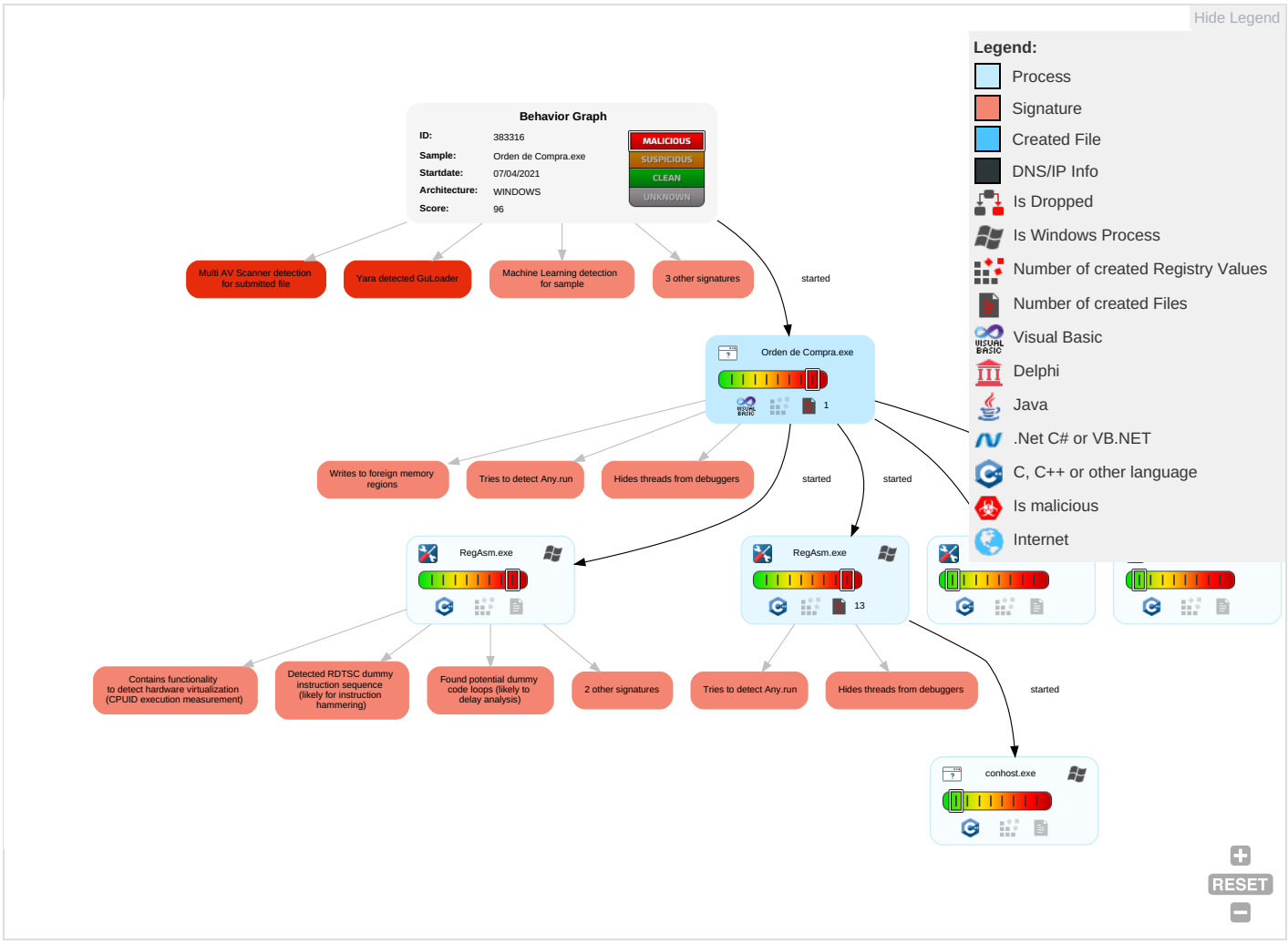
Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 3 2 1	OS Credential Dumping	Security Software Discovery 8 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Information Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat

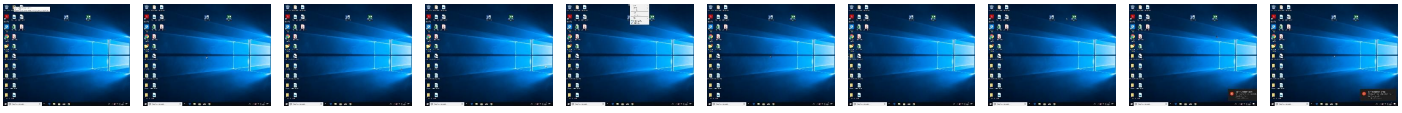
Behavior Graph



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
Orden de Compra.exe	10%	ReversingLabs	Win32.Worm.GenericML	
Orden de Compra.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://pki.goog/gsr2/GTS1O1.crt0	RegAsm.exe, 00000017.00000002.849852280.0000000001439000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	RegAsm.exe, 00000017.00000002.849831122.000000000141B000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	RegAsm.exe, 00000017.00000002.849831122.000000000141B000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	RegAsm.exe, 00000017.00000002.849831122.000000000141B000.00000004.00000020.sdmp, RegAsm.exe, 00000017.00000002.849852280.0000000001439000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383316
Start date:	07.04.2021
Start time:	16:14:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Orden de Compra.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:	25
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:	mal96.troj.evad.winEXE@10/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 96.1% (good quality ratio 38.6%) • Quality average: 20.6% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 75% • Number of executed functions: 0 • Number of non-executed functions: 0
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 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 23.54.113.53, 104.42.151.234, 104.43.193.48, 104.43.139.144, 13.64.90.137, 20.82.209.104, 23.10.249.43, 23.10.249.26, 168.61.161.212, 13.107.4.50, 51.103.5.186, 52.155.217.156, 40.88.32.150, 20.54.26.129, 95.100.54.203, 20.50.102.62, 172.217.168.14 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, drive.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, elasticShed.au.au-msedge.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, afdap.au.au-msedge.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, au.au-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, Edge-Prod-ZRH.env.au.au-msedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, au.c-0001.c-msedge.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/383316/sample/Orden de Compra.exe

Simulations

Behavior and APIs

Time	Type	Description
16:18:31	API Interceptor	258x Sleep call for process: RegAsm.exe modified

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):	5.606827135921854
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:	Orden de Compra.exe
File size:	110592
MD5:	e6dcf6b66b611ffb7d2bc1a8045bf41f
SHA1:	7b3871b1b077f764175c6d387e846372128a89ee
SHA256:	280e118484090c0a9788dcad52f37995822757f44d230c9ff042c3507d8e20a3
SHA512:	93f10041774b09d0789c388c1fb1c6643e573efae1a68937c6fdb323d01b535ab6585b64badd43ec095d74573ff8d3ad887788a02d0732b928bfc4318571c10b

General

SSDEEP:	1536:e5+vV32eex7a2I2vL2M/FPVm9vscwkpKcWe7yPVm9vDd2Mf2v:eo932eQk8Vmz/pr17uVmy
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:	0x59D2AEA6 [Mon Oct 2 21:24:54 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 00411024h
call 00007EFEA8D4C983h
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, dl
cmp al, B9h
jnc 00007EFEA8D4C9DEh
in al, 4Fh
dec esp
call far B6B4h : 1BC6E520h
add dword ptr [eax], 00000000h
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [ecx+00h], al
push es
push eax
xchg eax, ebx
add al, byte ptr [ebx+41h]
dec esi
dec ecx

Instruction
inc ebx
dec eax
inc ecx
dec esi
inc ecx
add byte ptr [eax], al
add byte ptr [edx+ebp+000002FFh], ah
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
or ebp, dword ptr [esi-683F24C6h]
adc ebp, edx
inc ebp
mov bh, byte ptr [eax+13h]
retf D69Dh
jl 00007EFEA8D4C992h
cmp eax, EBFEFE9Fh
movsd
jnl 00007EFEA8D4C9DBh
mov seg?, word ptr [ebx+ecx+00718674h]
aam 3Ah
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
mov ebx, edi
add byte ptr [eax], al
test al, F9h
add byte ptr [eax], al
add byte ptr [eax], cl
add byte ptr [ecx+edi*2+74h], ch
je 00007EFEA8D4C9F7h
jc 00007EFEA8D4CA00h
add byte ptr [41000B01h], cl
insb
je 00007EFEA8D4C9FFh
outsd
imul eax, dword ptr fs:[eax], 00000000h

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	0x134e4	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	
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	0x1298c	0x13000	False	0.421450966283	data	6.01111486713	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	0.360026041667	data	5.27238648737	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	Gulvhoejde9
FileVersion	1.00
CompanyName	Pana-sonic
Comments	Pana-sonic
ProductName	Pana-sonic
ProductVersion	1.00
FileDescription	Pana-sonic
OriginalFilename	Gulvhoejde9.exe

Possible Origin

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

Network Behavior

UDP Packets

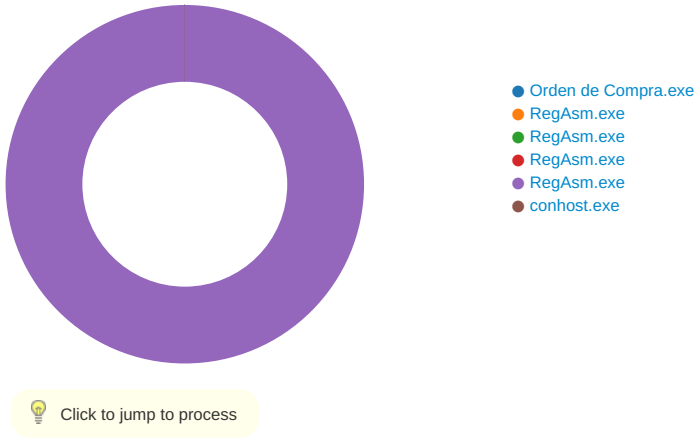
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 16:15:33.104764938 CEST	62044	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:15:33.120260954 CEST	53	62044	8.8.8.8	192.168.2.6
Apr 7, 2021 16:15:34.092418909 CEST	63791	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:15:34.113867044 CEST	53	63791	8.8.8.8	192.168.2.6
Apr 7, 2021 16:15:36.412851095 CEST	64267	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:15:36.425412893 CEST	53	64267	8.8.8.8	192.168.2.6
Apr 7, 2021 16:15:37.539197922 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:15:37.551731110 CEST	53	49448	8.8.8.8	192.168.2.6
Apr 7, 2021 16:15:39.513669968 CEST	60342	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:15:39.526567936 CEST	53	60342	8.8.8.8	192.168.2.6
Apr 7, 2021 16:15:40.467571974 CEST	61346	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:15:40.482719898 CEST	53	61346	8.8.8.8	192.168.2.6
Apr 7, 2021 16:15:41.460514069 CEST	51774	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:15:41.475016117 CEST	53	51774	8.8.8.8	192.168.2.6
Apr 7, 2021 16:15:43.907953024 CEST	56023	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:15:43.920675039 CEST	53	56023	8.8.8.8	192.168.2.6
Apr 7, 2021 16:15:44.654238939 CEST	58384	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:15:44.667623997 CEST	53	58384	8.8.8.8	192.168.2.6
Apr 7, 2021 16:15:58.750540018 CEST	60261	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:15:58.762518883 CEST	53	60261	8.8.8.8	192.168.2.6
Apr 7, 2021 16:15:59.512046099 CEST	56061	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:15:59.524298906 CEST	53	56061	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:05.114721060 CEST	58336	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:05.129053116 CEST	53	58336	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:06.268214941 CEST	53781	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:06.282241106 CEST	53	53781	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:07.165368080 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:07.178927898 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:07.909548998 CEST	52811	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:07.922127962 CEST	53	52811	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:08.335704088 CEST	55299	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:08.350513935 CEST	53	55299	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:17.864222050 CEST	63745	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:17.882713079 CEST	53	63745	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:21.625291109 CEST	50055	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:21.637953043 CEST	53	50055	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:23.110431910 CEST	61374	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:23.124610901 CEST	53	61374	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:29.247642040 CEST	50339	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:29.260672092 CEST	53	50339	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:30.358724117 CEST	63307	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:30.372255087 CEST	53	63307	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:32.209223032 CEST	49694	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:32.314316988 CEST	53	49694	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:33.400372982 CEST	54982	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:33.453996897 CEST	53	54982	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:33.778000116 CEST	50010	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:33.791913033 CEST	53	50010	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:34.003056049 CEST	63718	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:34.044306040 CEST	53	63718	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 16:16:34.827584028 CEST	62116	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:34.842129946 CEST	53	62116	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:35.343364000 CEST	63816	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:36.366708994 CEST	63816	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:36.380497932 CEST	53	63816	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:36.806963921 CEST	55014	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:36.848423004 CEST	53	55014	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:37.082979918 CEST	62208	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:37.097588062 CEST	53	62208	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:37.257606983 CEST	57574	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:37.272097111 CEST	53	57574	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:37.525474072 CEST	51818	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:37.558182955 CEST	53	51818	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:37.985945940 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:38.000463009 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:38.225332975 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:38.238691092 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:39.254580975 CEST	53799	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:39.268831968 CEST	53	53799	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:39.342791080 CEST	54683	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:39.354752064 CEST	53	54683	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:39.760382891 CEST	59329	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:39.774312973 CEST	53	59329	8.8.8.8	192.168.2.6
Apr 7, 2021 16:16:45.014624119 CEST	64021	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:16:45.034246922 CEST	53	64021	8.8.8.8	192.168.2.6
Apr 7, 2021 16:17:16.339049101 CEST	56129	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:17:16.357769966 CEST	53	56129	8.8.8.8	192.168.2.6
Apr 7, 2021 16:17:19.268028975 CEST	58177	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:17:19.281272888 CEST	53	58177	8.8.8.8	192.168.2.6
Apr 7, 2021 16:17:22.406878948 CEST	50700	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:17:22.438817978 CEST	53	50700	8.8.8.8	192.168.2.6
Apr 7, 2021 16:18:30.551539898 CEST	54069	53	192.168.2.6	8.8.8.8
Apr 7, 2021 16:18:30.577713013 CEST	53	54069	8.8.8.8	192.168.2.6

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Orden de Compra.exe PID: 6960 Parent PID: 6044

General

Start time:	16:15:40
Start date:	07/04/2021
Path:	C:\Users\user\Desktop\Orden de Compra.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Orden de Compra.exe'
Imagebase:	0x400000
File size:	110592 bytes
MD5 hash:	E6DCF6B66B611FFB7D2BC1A8045BF41F
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 5700 Parent PID: 6960

General

Start time:	16:18:15
Start date:	07/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\Orden de Compra.exe'
Imagebase:	0xd0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 2988 Parent PID: 6960

General

Start time:	16:18:15
Start date:	07/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\Orden de Compra.exe'
Imagebase:	0xf0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 784 Parent PID: 6960

General

Start time:	16:18:15
Start date:	07/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\Orden de Compra.exe'
Imagebase:	0x4a0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 6128 Parent PID: 6960

General

Start time:	16:18:16
Start date:	07/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Orden de Compra.exe'
Imagebase:	0xc60000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000017.00000002.849537125.0000000001100000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1103D1C	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1103D1C	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1103D1C	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1103D1C	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1103D1C	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1103D1C	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5980 Parent PID: 6128

General

Start time:	16:18:16
Start date:	07/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis