

JOeSandbox Cloud BASIC



ID: 383316

Sample Name: Orden de
Compra.exe

Cookbook: default.jbs

Time: 16:23:43

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
Sigma Overview	4
Signature Overview	4
AV Detection:	5
Malware Analysis System Evasion:	5
Anti Debugging:	5
Mitre Att&ck Matrix	5
Behavior Graph	5
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
Contacted IPs	8
General Information	8
Simulations	8
Behavior and APIs	8
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
Static File Info	9
General	9
File Icon	9
Static PE Info	10
General	10
Entrypoint Preview	10
Data Directories	11
Sections	12
Resources	12
Imports	12
Version Infos	12
Possible Origin	12
Network Behavior	13
Code Manipulations	13
Statistics	13
System Behavior	13
Analysis Process: Orden de Compra.exe PID: 6532 Parent PID: 6016	13
General	13

File Activities	13
Disassembly	13
Code Analysis	13

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

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

64

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

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 ...

Detected potential crypto function

Found large amount of non-executed...

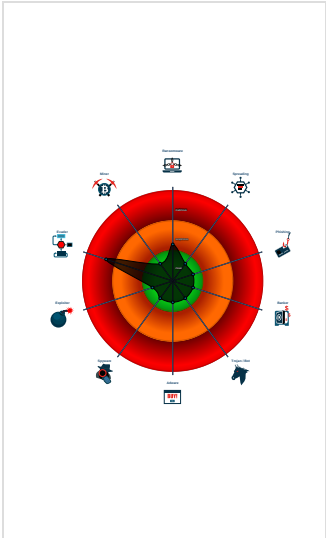
PE file contains an invalid checksum

PE file contains strange resources

Program does not show much activi...

Sample file is different than original ...

Classification



Startup

- System is w10x64
- Orden de Compra.exe (PID: 6532 cmdline: 'C:\Users\user\Desktop\Orden de Compra.exe' MD5: E6DCF6B66B611FFB7D2BC1A8045BF41F)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

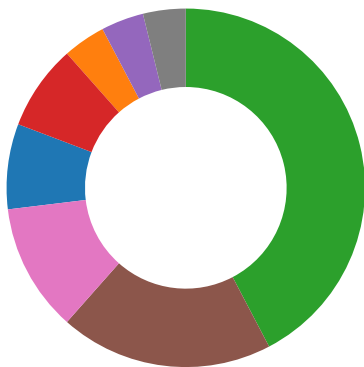
Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance

- 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

Malware Analysis System Evasion:



Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

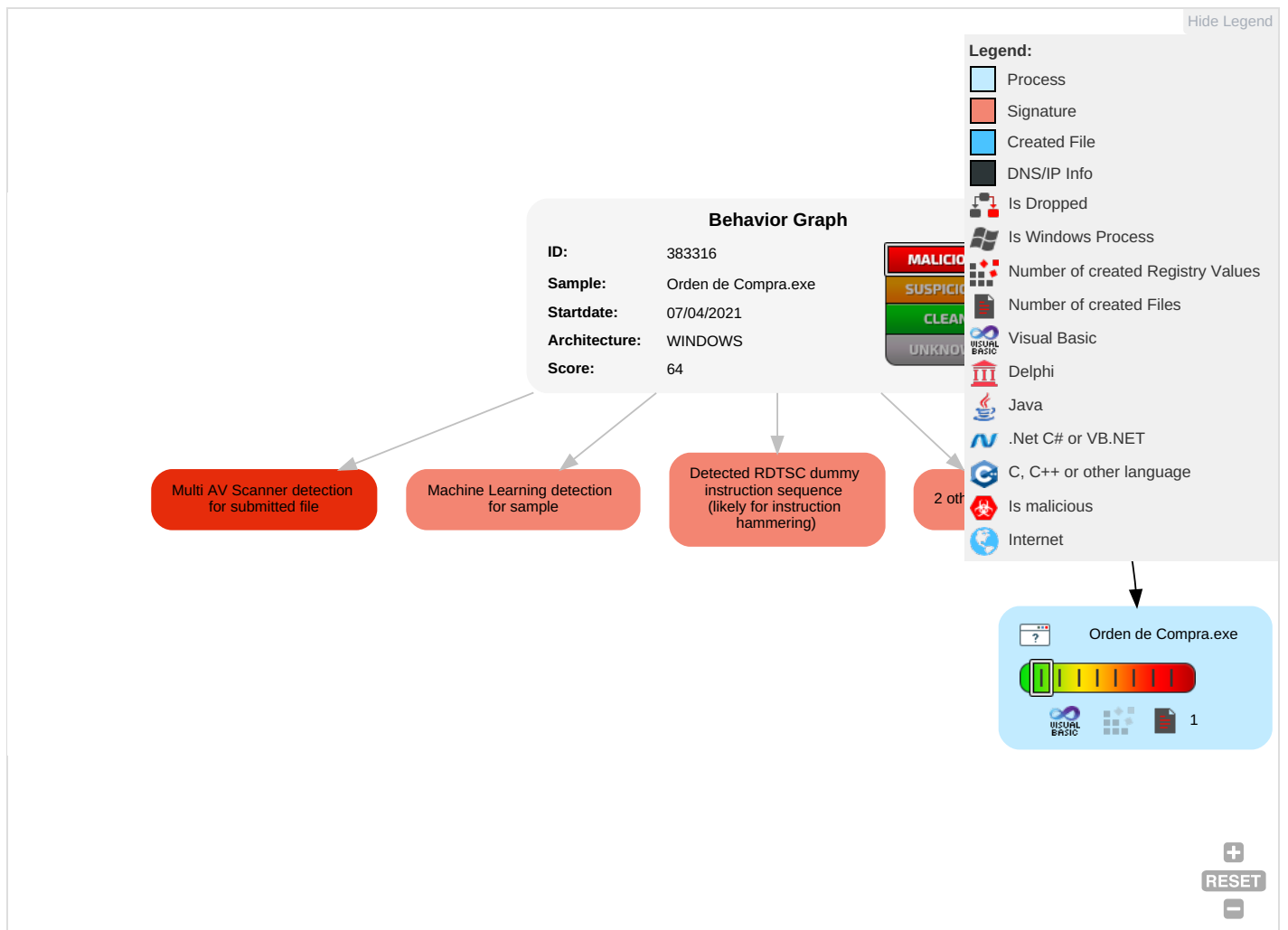


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery
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	Recovery
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	Recovery
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	Recovery

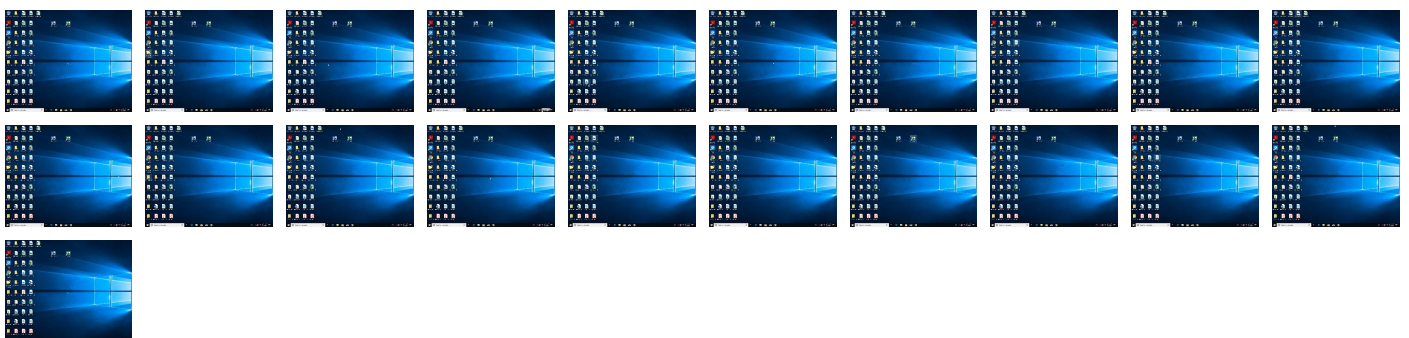
Behavior Graph



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	49%	Virustotal		Browse
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

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:	383316
Start date:	07.04.2021
Start time:	16:23:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 58s
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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	18
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:	mal64.evad.winEXE@1/0@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:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.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):	5.606827135921854
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:	280e118484090c0a9788dcad52f37995822757f44d230c5ff042c3507d8e20a3
SHA512:	93f10041774b09d0789c388c1fb1c6643e573efae1a68937c6fdb323d01b535ab6585b64badd43ec095d74573ff8d3ad887788a02d0732b928bfc4318571c10b
SSDEEP:	1536:e5+vV32eex7a2l2vL2M/FPVvm9vscwkpKcWe7yP Vm9vDd2Mf2v:eo932eQk8Vmz/pr17uVmy
File Content Preview:	MZ.....@.....!..L!Th is 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 00007F2E6481AC33h
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 00007F2E6481AC8Eh
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
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
```


Name	Virtual Address	Virtual Size	Is in Section
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	_Clos, _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_fptan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptionHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPEException, _Cilog, __vbaFileOpen, __vbaNew2, __vbaR8Str, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, _adj_fdivr_m32, _adj_fdiv_r, __vbaLateMemCall, __vbaVarAdd, __vbaVarDup, __vbaFpl4, _Clatan, __vbaStrMove, _allmul, _Cltan, _Clexp, __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

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Orden de Compra.exe PID: 6532 Parent PID: 6016

General

Start time:	16:24:58
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

Disassembly

Code Analysis