ID: 431502
Sample Name: Facturas Pagadas Al Vencimiento.exe
Cookbook: default.jbs
Time: 20:20:46
Date: 08/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

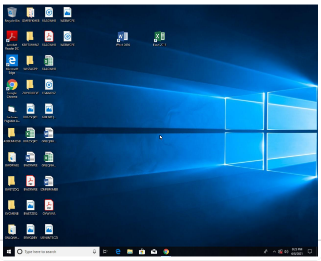
Analysis Report Facturas Pagadas Al Vencimiento.exe

Overview

General Information

Sample Name:	Facturas Pagadas Al Vencimiento.exe
Analysis ID:	431502
MD5:	882a1c19dc7f3ac..
SHA1:	9566eae6967084..
SHA256:	ebf355b0e58fcf5…
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

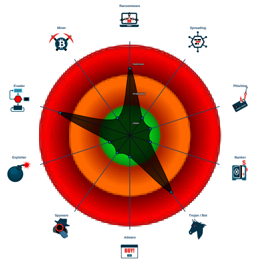
GuLoader

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to read the PEB

Classification



Process Tree

- **System is w10x64**
- Facturas Pagadas Al Vencimiento.exe (PID: 7072 cmdline: 'C:\Users\user\Desktop\Facturas Pagadas Al Vencimiento.exe' MD5: 882A1C19DC7F3AC4FADAC702125649C0)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1j7lPzKHjaJ361TpkvK1-2kTy_ducVUTL"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Facturas Pagadas Al Vencimiento.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

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 virtualization through RDTSC time measurements

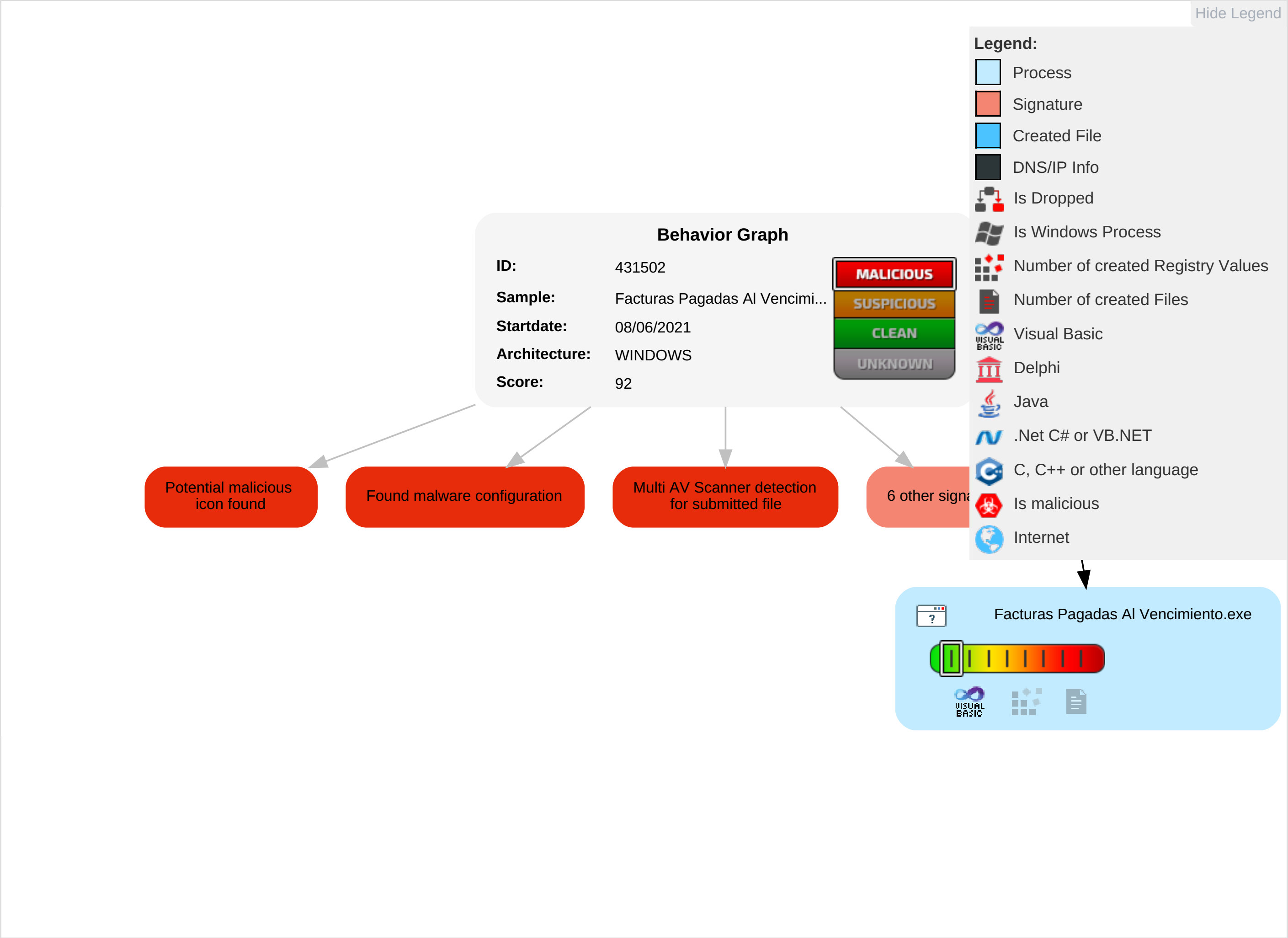
Anti Debugging:

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	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 4 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
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	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
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	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph



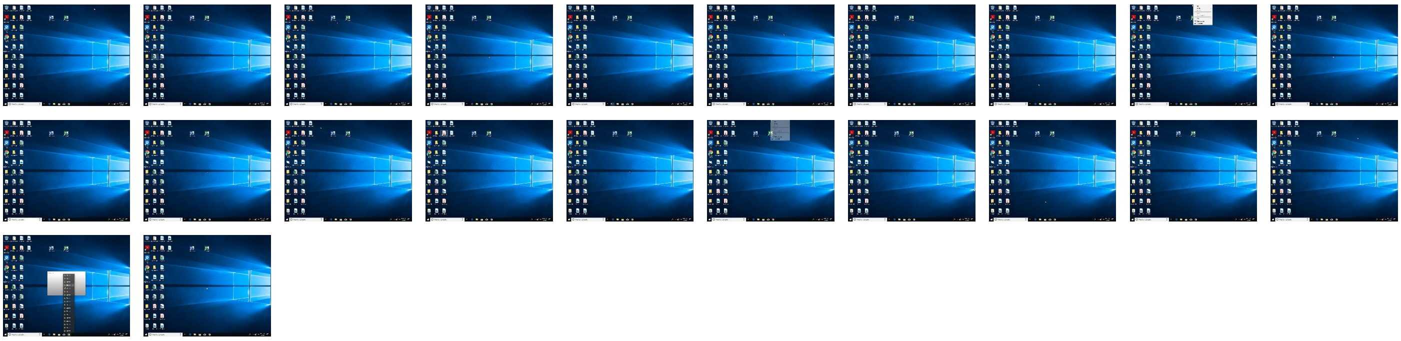
Behavior Graph

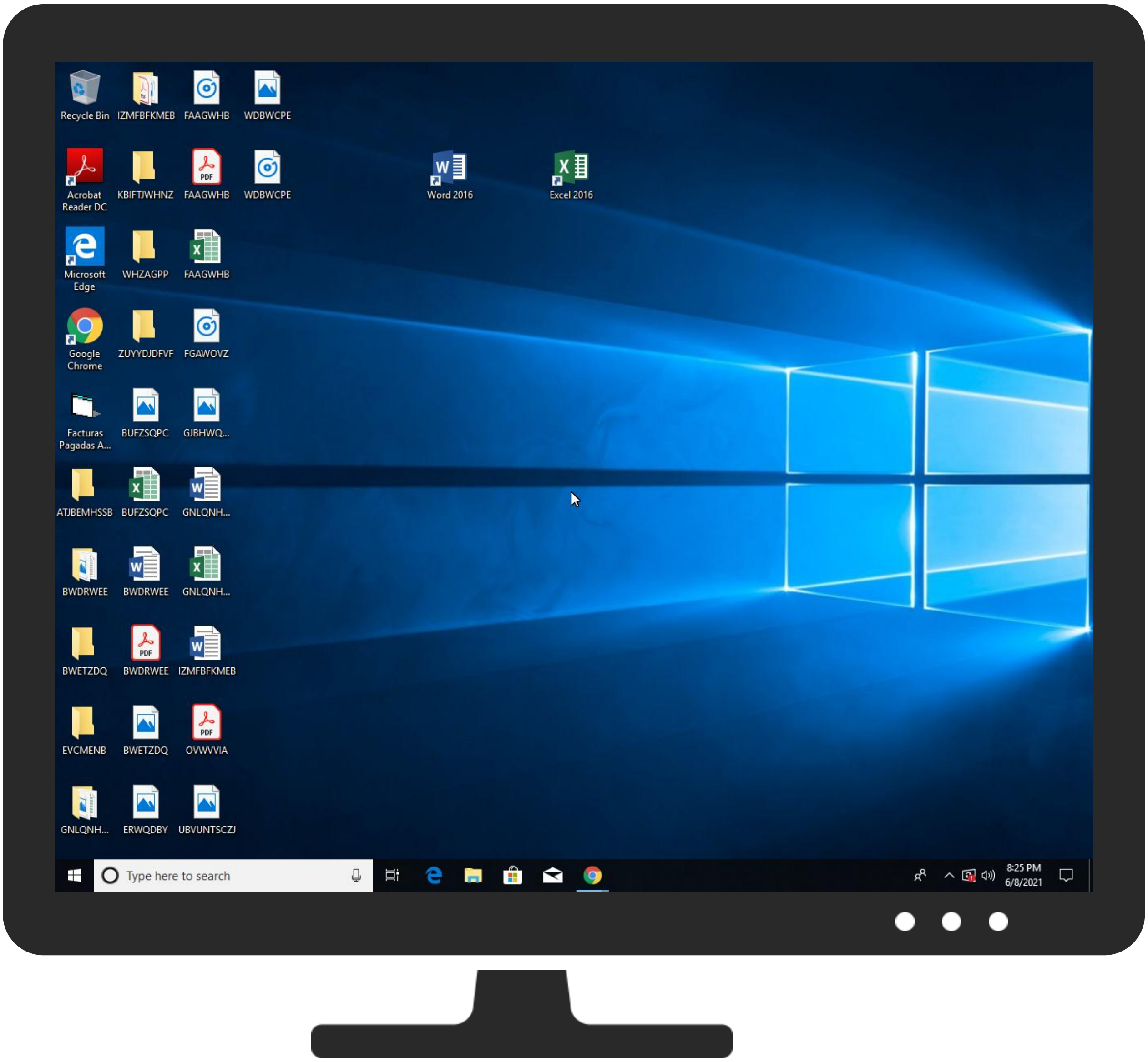
ID:	431502
Sample:	Facturas Pagadas Al Vencimi...
Startdate:	08/06/2021
Architecture:	WINDOWS
Score:	92

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
Facturas Pagadas Al Vencimiento.exe	53%	Virustotal		Browse
Facturas Pagadas Al Vencimiento.exe	30%	ReversingLabs	Win32.Trojan.VBodius	

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:	32.0.0 Black Diamond
Analysis ID:	431502
Start date:	08.06.2021
Start time:	20:20:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Facturas Pagadas Al Vencimiento.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:	17
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:	mal92.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 4.9% (good quality ratio 0.6%) • Quality average: 6.8% • Quality standard deviation: 15%
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

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

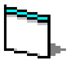
No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.619538143256787
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:	Facturas Pagadas Al Vencimiento.exe
File size:	147456
MD5:	882a1c19dc7f3ac4fadac702125649c0
SHA1:	9566eae6967084d05f21d614686eaa28a3b66a8d
SHA256:	ebf355b0e58fcf5b9cf1718b6fd09003932fe3b7ed5b08ffc9ac2f987e0d189d
SHA512:	33776a0903527f9548aa15f1f6be67388b928f602698cd711e38a010763e58c7bf14c26423ac3fec800f198d17f3d69826403b120fbd03cbeffc69269b75258d
SSDEEP:	1536:BgXhQ6fSRjYxtNejzOU0N8mopUiDhRTUaZz5jYINm1aiQny+qxp:/cNozFDdpUgRTUaZz50INiaiM4p
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......`....................0............... ....@................

File Icon



Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4014b8
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:	0x60BF1788 [Tue Jun 8 07:08:56 2021 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:	b1d5215cf0ff1abab4dacdc311d642d4

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2032c	0x21000	False	0.324329723011	data	4.86252007342	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1234	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0xa0c	0x1000	False	0.1826171875	data	2.19787994537	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Sesotho (Sutu)	South Africa	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Facturas Pagadas Al Vencimiento.exe PID: 7072 Parent PID: 5868

General

Start time:	20:21:34
Start date:	08/06/2021
Path:	C:\Users\user\Desktop\Facturas Pagadas Al Vencimiento.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Facturas Pagadas Al Vencimiento.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	882A1C19DC7F3AC4FADAC702125649C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis