Joe Sandbox Cloud BASIC

ID: 502709
Sample Name: PEDIDO.exe
Cookbook: default.jbs
Time: 10:36:11
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

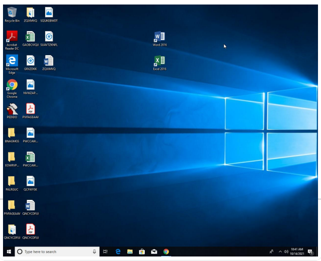
Windows Analysis Report PEDIDO.exe

Overview

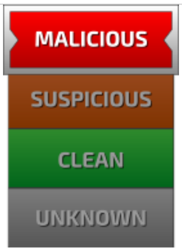
General Information

Sample Name:	PEDIDO.exe
Analysis ID:	502709
MD5:	8bc016e5779262..
SHA1:	5fa020fa3a63a48..
SHA256:	69a8e2fa9664dce.
Tags:	exe Guloader
Infos:	

Most interesting Screenshot:



Detection



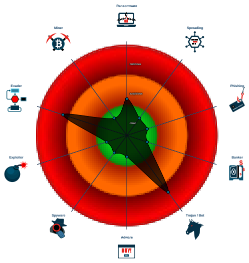
GuLoader

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

Signatures

- Found malware configuration
- Yara detected GuLoader
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Sample file is different than original …
- Contains functionality to read the PEB
- Program does not show much activi…
- Uses code obfuscation techniques (…
- Contains functionality for execution …

Classification



Process Tree

- **System is w10x64**
- PEDIDO.exe (PID: 4724 cmdline: 'C:\Users\user\Desktop\PEDIDO.exe' MD5: 8BC016E5779262B772D16903AF6E142C)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1G3zuBgFp"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.779265380.00000000020F0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

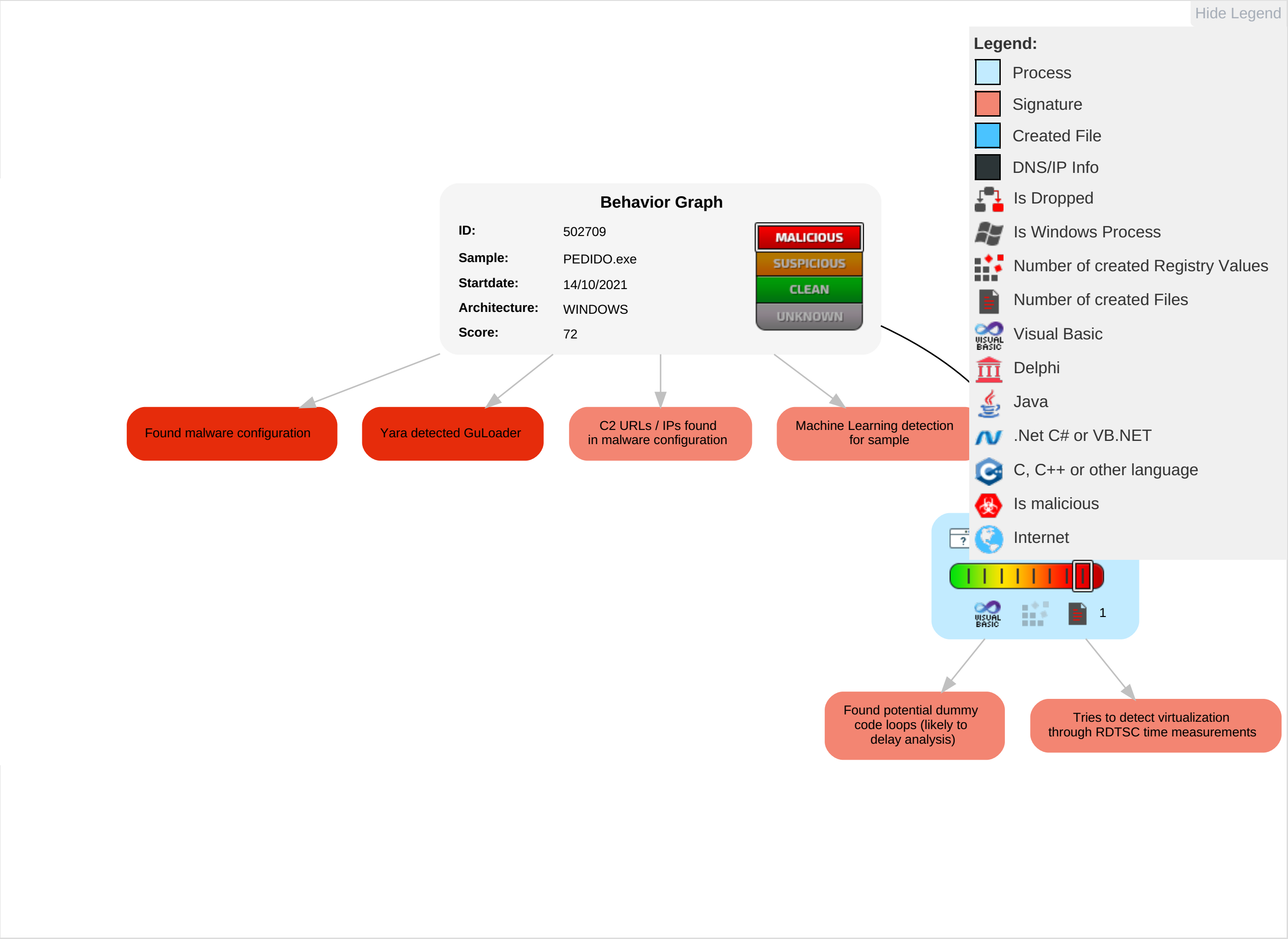
Anti Debugging:

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 2 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 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph


Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Yara detected GuLoader
C2 URLs / IPs found in malware configuration
Machine Learning detection for sample
1
Found potential dummy code loops (likely to delay analysis)
Tries to detect virtualization through RDTSC time measurements

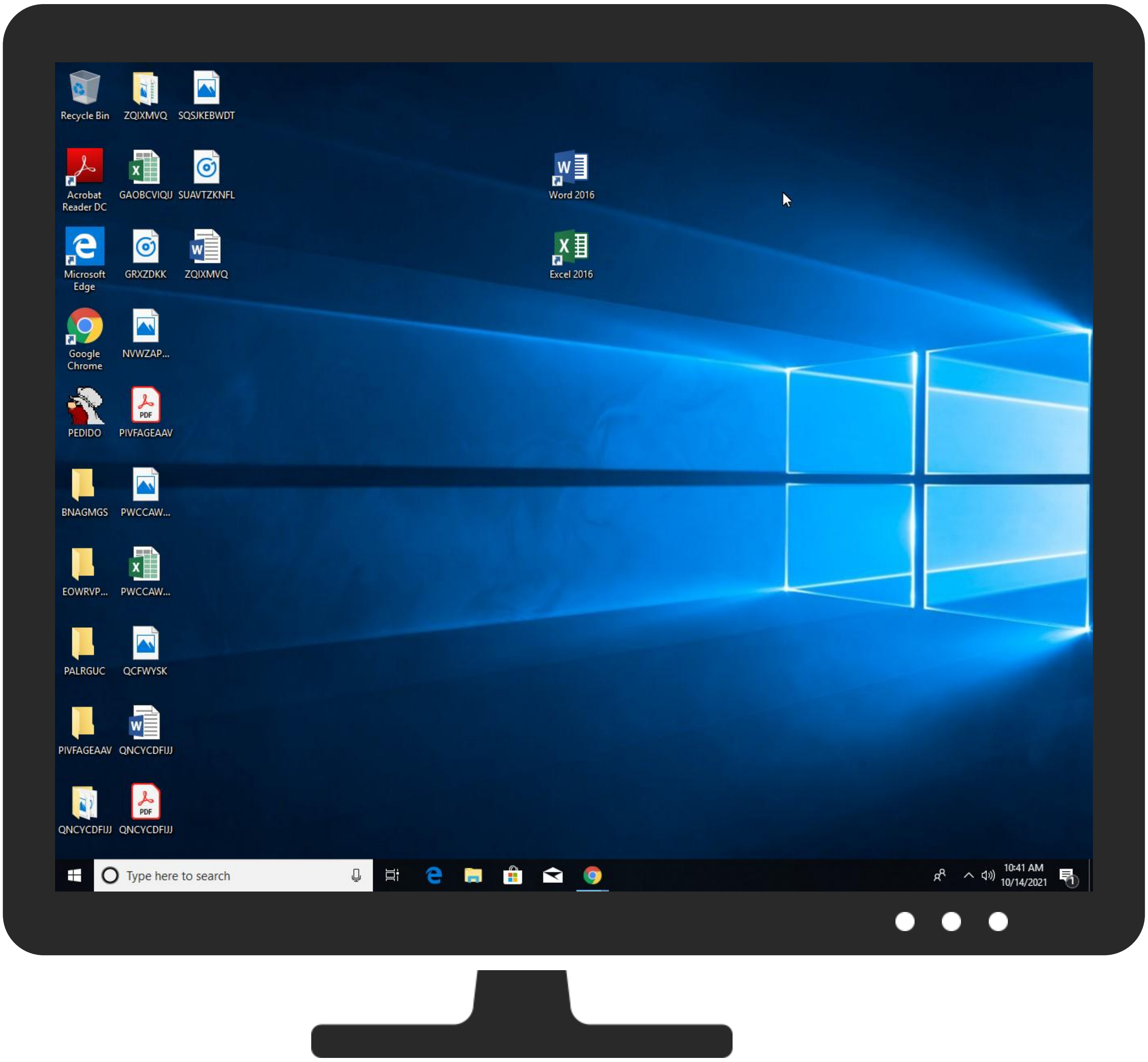
Behavior Graph

ID:	502709
Sample:	PEDIDO.exe
Startdate:	14/10/2021
Architecture:	WINDOWS
Score:	72

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
PEDIDO.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:	33.0.0 White Diamond
Analysis ID:	502709
Start date:	14.10.2021
Start time:	10:36:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PEDIDO.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:	mal72.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 37.7% (good quality ratio 21.6%) • Quality average: 35.8% • Quality standard deviation: 37.2%
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

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):	5.79980248716969
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:	PEDIDO.exe
File size:	98304
MD5:	8bc016e5779262b772d16903af6e142c
SHA1:	5fa020fa3a63a481eff19fca06e11c424d346e9f
SHA256:	69a8e2fa9664dce4cb9ab2d1a2e7ba67bd0516b9e4c8608e9c246d614be3241f
SHA512:	75705b51a700371ab9211b81bf0e36aeae80825418a3e260c9b9e6610cb3f31833349b309ac88f6e67bf3f16a34d349802c617a25f9a52e8bcfb989bf7289a53
SSDEEP:	1536:tqD1R2xaclNLo4V4UQhH03JYVtKP2BlxS6pE5LD:tqPkNLo4VRQh8OKettS5L
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........i......................*..............Rich...................PE..L...i..T................@...0...............P....@........

File Icon

Icon Hash:	69e1c892f664c884

Static PE Info

General

Entrypoint:	0x4012b4
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:	0x5402F169 [Sun Aug 31 09:56:57 2014 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:	3d3cd1bd8dcc611a5734bf41f4e1a6a6

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x132f8	0x14000	False	0.50859375	data	6.25990201424	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0xcc4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x16000	0x1c32	0x2000	False	0.346435546875	data	3.68560912734	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
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: PEDIDO.exe PID: 4724 Parent PID: 6096

General

Start time:	10:37:12
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\PEDIDO.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PEDIDO.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	8BC016E5779262B772D16903AF6E142C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.779265380.00000000020F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 33.0.0 White Diamond