

JoeSandbox Cloud BASIC



ID: 502290

Sample Name: PEDIDO.exe

Cookbook: default.jbs

Time: 19:19:10

Date: 13/10/2021

Version: 33.0.0 White Diamond

Table of Contents

| | |
|---|----|
| Table of Contents | 2 |
| Windows Analysis Report PEDIDO.exe | 3 |
| Overview | 3 |
| General Information | 3 |
| Detection | 3 |
| Signatures | 3 |
| Classification | 3 |
| Process Tree | 3 |
| Malware Configuration | 3 |
| Threatname: GuLoader | 3 |
| Yara Overview | 3 |
| Memory Dumps | 3 |
| Sigma Overview | 3 |
| Jbx Signature Overview | 4 |
| AV Detection: | 4 |
| Networking: | 4 |
| Data Obfuscation: | 4 |
| Malware Analysis System Evasion: | 4 |
| Anti Debugging: | 4 |
| Mitre Att&ck Matrix | 4 |
| Behavior Graph | 4 |
| Screenshots | 5 |
| Thumbnails | 5 |
| Antivirus, Machine Learning and Genetic Malware Detection | 6 |
| Initial Sample | 6 |
| Dropped Files | 6 |
| Unpacked PE Files | 6 |
| Domains | 6 |
| URLs | 6 |
| Domains and IPs | 7 |
| Contacted Domains | 7 |
| Contacted IPs | 7 |
| General Information | 7 |
| Simulations | 7 |
| Behavior and APIs | 7 |
| Joe Sandbox View / Context | 7 |
| IPs | 8 |
| Domains | 8 |
| ASN | 8 |
| JA3 Fingerprints | 8 |
| Dropped Files | 8 |
| Created / dropped Files | 8 |
| Static File Info | 8 |
| General | 8 |
| File Icon | 8 |
| Static PE Info | 8 |
| General | 8 |
| Entrypoint Preview | 9 |
| Data Directories | 9 |
| Sections | 9 |
| Resources | 9 |
| Imports | 9 |
| Version Infos | 9 |
| Possible Origin | 9 |
| Network Behavior | 9 |
| Code Manipulations | 9 |
| Statistics | 9 |
| System Behavior | 10 |
| Analysis Process: PEDIDO.exe PID: 5460 Parent PID: 3272 | 10 |
| General | 10 |
| File Activities | 10 |
| Disassembly | 10 |
| Code Analysis | 10 |

Windows Analysis Report PEDIDO.exe

Overview

General Information

Sample Name:

PEDIDO.exe

Analysis ID:

502290

MD5:

83046fa32e56328.

SHA1:

fdacb1537161c01..

SHA256:




6b3d06b20b3ae5..

Tags:

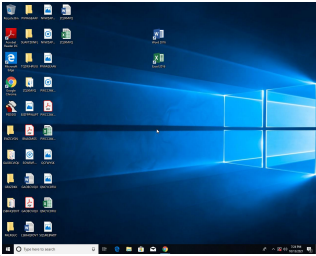
exe

guloader

Infos:

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

68

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Yara detected GuLoader

Found potential dummy code loops (...)

Tries to detect virtualization through...

C2 URLs / IPs found in malware con...

Creates a DirectInput object (often fo...

Uses 32bit PE files

Contains functionality to call native f...

Sample file is different than original ...

Contains functionality to read the PEB

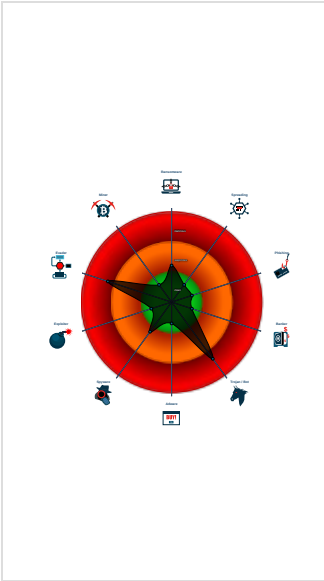
Program does not show much activi...

Uses code obfuscation techniques (...)

Contains functionality for execution ...

Abnormal high CPU Usage

Classification



Process Tree

System is w10x64

 PEDIDO.exe (PID: 5460 cmdline: 'C:\Users\user\Desktop\PEDIDO.exe' MD5: 83046FA32E563289DBD98EFE27F884F4)

cleanup

Malware Configuration

Threatname: GuLoader

{

"Payload URL": "https://drive.google.com/uc?expordJ|"

}

Yara Overview


Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|------------------------|------------------------|--------------|---------|
| 00000000.00000002.778170637.000000000021D 0000.00000040.00000001.sdump | 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

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:

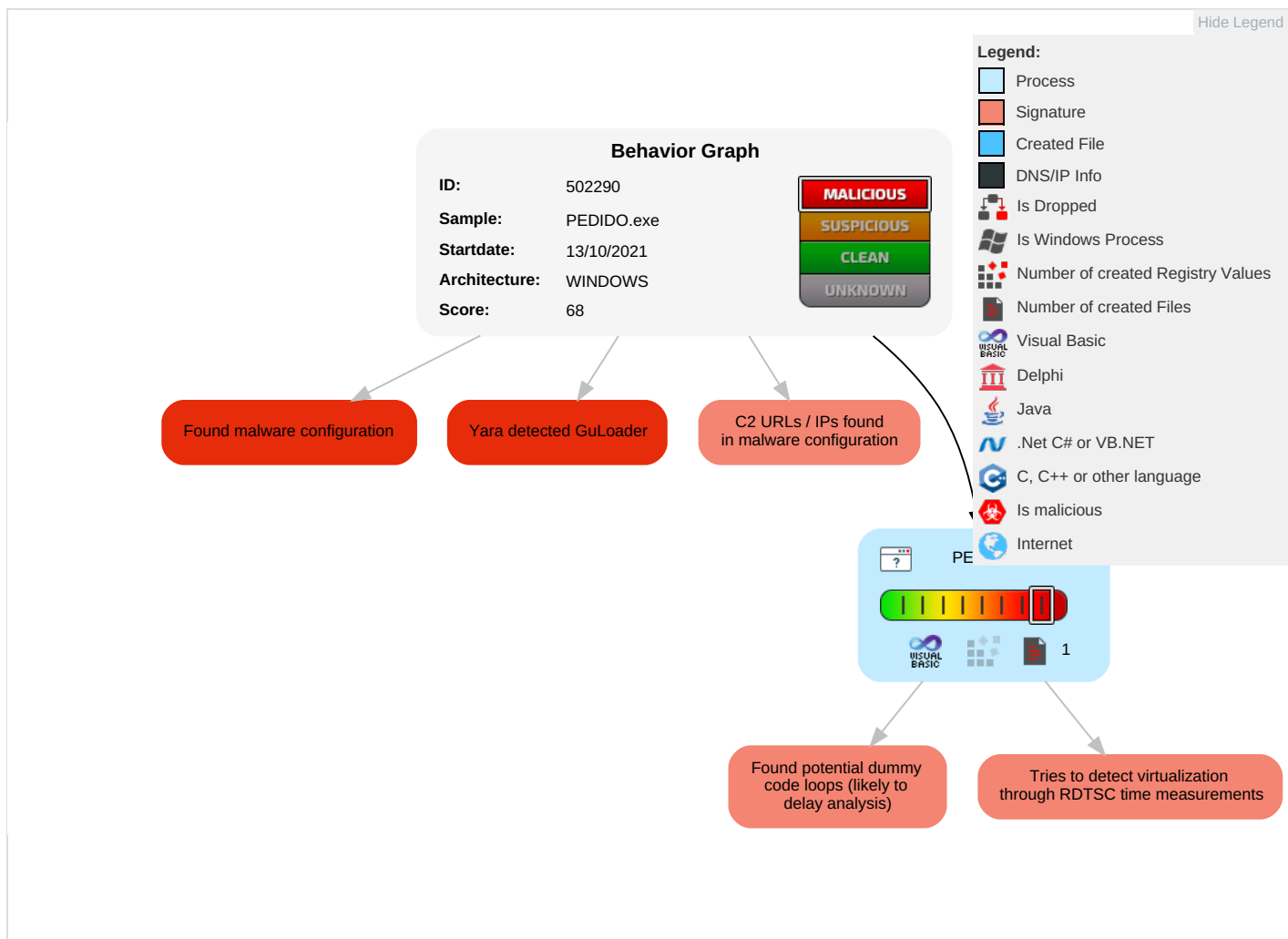


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Recovery |
|------------------|------------------------------------|--------------------------------------|--------------------------------------|------------------------------------|--------------------------|------------------------------------|------------------------------------|--------------------------------|--|------------------------------|---|----------|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Process Injection 1 | Virtualization/Sandbox Evasion 1 1 | Input Capture 1 | Security Software Discovery 2 1 | Remote Services | Input Capture 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 | Archive Collected Data 1 | Exfiltration Over Bluetooth | Application Layer Protocol 1 | 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 1 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 |
|------------|-----------|---------------|-------------------|------|
| PEDIDO.exe | 8% | ReversingLabs | Win32.Trojan.Mucc | |

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: | 502290 |
| Start date: | 13.10.2021 |
| Start time: | 19:19:10 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 7m 41s |
| 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: | 28 |
| 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: | <ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal68.troj.evad.winEXE@1/0@0/0 |
| EGA Information: | Failed |
| HDC Information: | <ul style="list-style-type: none">• Successful, ratio: 29.4% (good quality ratio 18.4%)• Quality average: 42.8%• Quality standard deviation: 38.9% |
| HCA Information: | Failed |
| Cookbook Comments: | <ul style="list-style-type: none">• 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): | 5.757968809183827 |
| TrID: | <ul style="list-style-type: none">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: | 83046fa32e563289dbd98efe27f884f4 |
| SHA1: | fdacb1537161c011f5803471b6971225010d4e71 |
| SHA256: | 6b3d06b20b3ae5a3dd8d3a2eb9eb1f1a86d9ba5eb59f5ef75cfa1b2f28dcfd6c |
| SHA512: | 9669be8d89c08729dbb62da4cdf54a6dc43fe7b59ecc93ac756a6ed35f42ba38981316465a2b286e124656350993d76f7e6fd5ed51e88324e9d66edcb26df282 |
| SSDEEP: | 1536:t9BDgiAEkkSAIJQpaehY0gB0PXUhzYMns1h7luDhaD:t9BXAZAADehhgB0PXAzYMnekuDha |
| File Content Preview: | MZ.....@.....!..L.!Th is program cannot be run in DOS mode...\$......i.....*.....Rich.....PE..L.....(N..... @...0.....P....@..... |

File Icon



Icon Hash: 69e1c892f664c884

Static PE Info

General

| | |
|-------------|----------|
| Entrypoint: | 0x4012b4 |
|-------------|----------|

| | |
|-----------------------------|---|
| General | |
| 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: | 0x4E28E7F0 [Fri Jul 22 03:01:04 2011 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 | 0x13528 | 0x14000 | False | 0.504711914063 | data | 6.20991689297 | 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 | 0x1c2a | 0x2000 | False | 0.346557617188 | data | 3.68630783779 | 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: 5460 Parent PID: 3272

General

| | |
|-------------------------------|--|
| Start time: | 19:20:08 |
| Start date: | 13/10/2021 |
| 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: | 83046FA32E563289DBD98EFE27F884F4 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Yara matches: | <ul style="list-style-type: none">Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.778170637.00000000021D0000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

File Activities

Show Windows behavior

Disassembly

Code Analysis