JoeSandbox Cloud BASIC

ID: 527894
Sample Name: Arrival Notice, CIA Awb Inv Form.pdf.exe
Cookbook: default.jbs
Time: 14:57:05
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

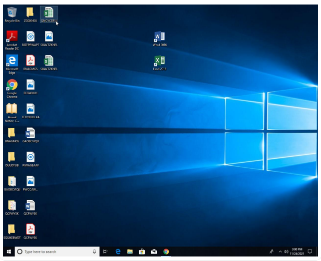
Windows Analysis Report Arrival Notice, CIA Awb Inv F…

Overview

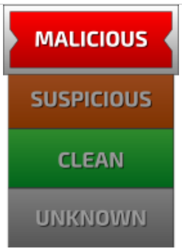
General Information

Sample Name:	Arrival Notice, CIA Awb Inv Form.pdf.exe
Analysis ID:	527894
MD5:	ff71941571d8930..
SHA1:	0a417bf568a5978.
SHA256:	bf952f1cd44de7b..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



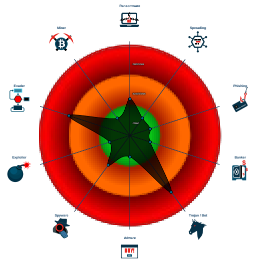
GuLoader

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Initial sample is a PE file and has a …
- Executable has a suspicious name (…
- C2 URLs / IPs found in malware con…
- Uses an obfuscated file name to hid…
- Machine Learning detection for samp…
- Uses 32bit PE files
- Queries the volume information (nam…
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- Arrival Notice, CIA Awb Inv Form.pdf.exe (PID: 6260 cmdline: "C:\Users\user\Desktop\Arrival Notice, CIA Awb Inv Form.pdf.exe" MD5: FF71941571D8930C1125B3931D400D86)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=16igyruBe"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.589123852.0000000004BB0000.00000040.00000001.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

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation:

Yara detected GuLoader

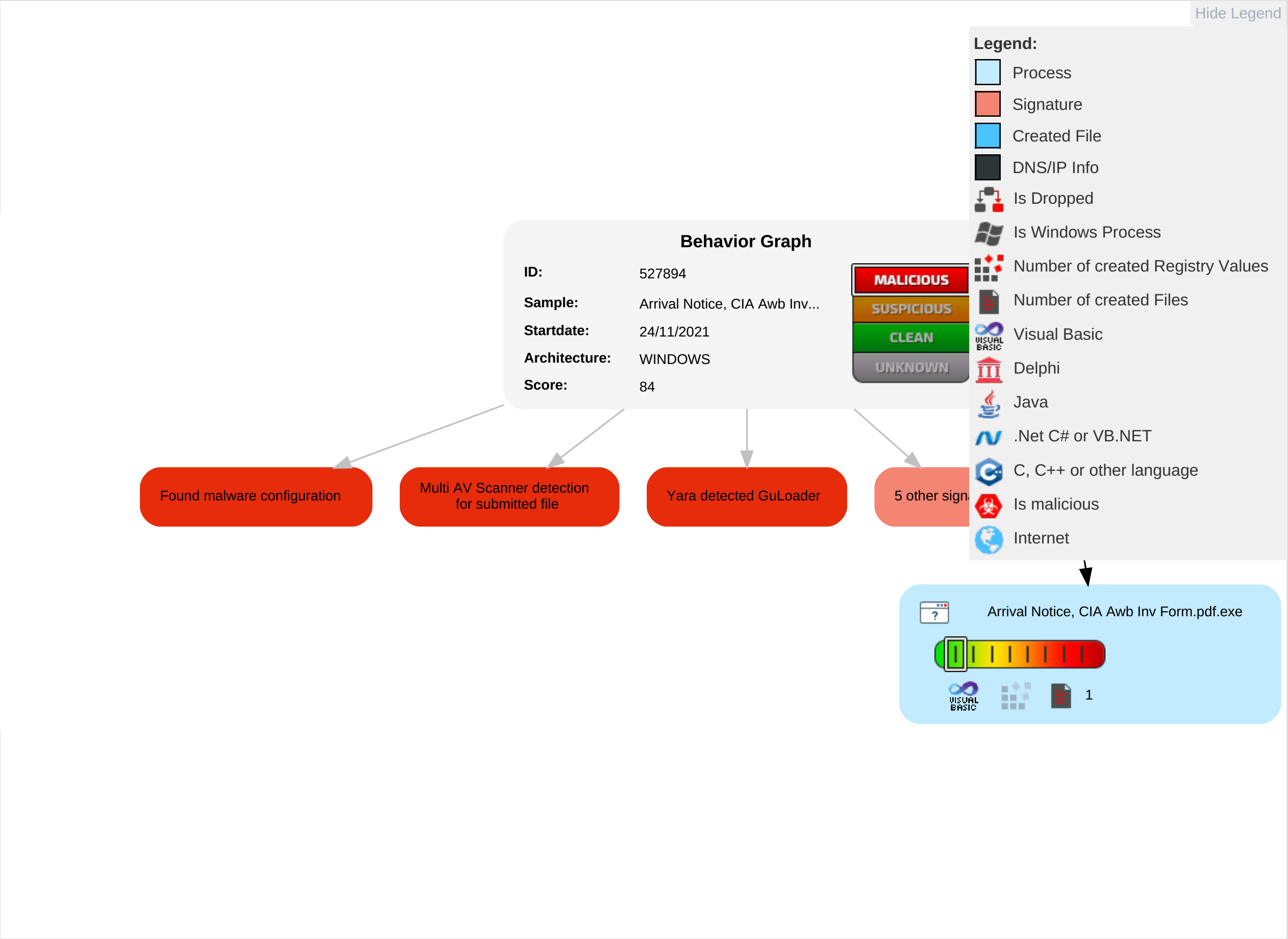
Hooking and other Techniques for Hiding and Protection:

Uses an obfuscated file name to hide its real file extension (double extension)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Process Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	System Information Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

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

Behavior Graph

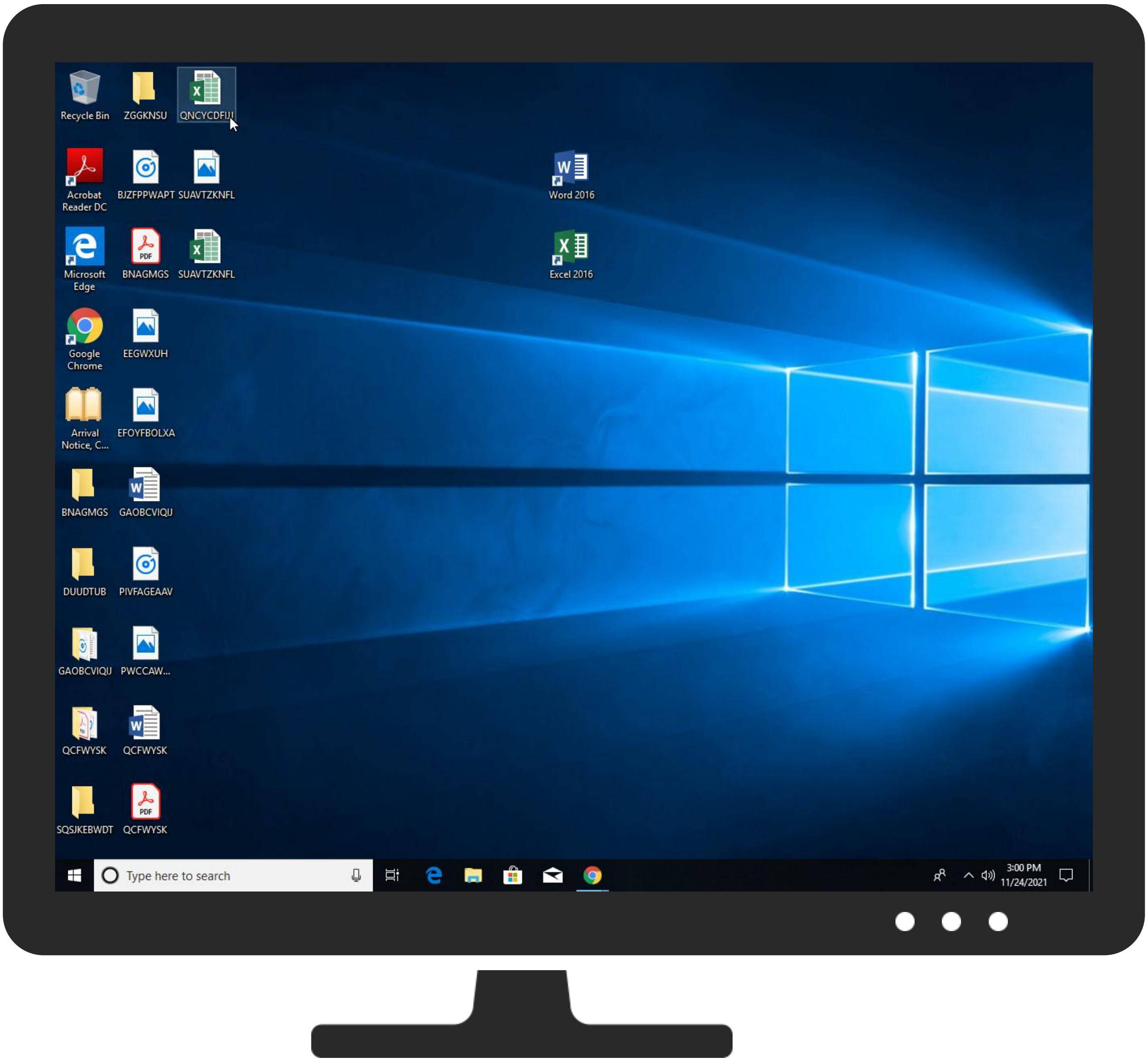
ID:	527894
Sample:	Arrival Notice, CIA Awb Inv...
Startdate:	24/11/2021
Architecture:	WINDOWS
Score:	84

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Multi AV Scanner detection for submitted file
Yara detected GuLoader
5 other signa
Arrival Notice, CIA Awb Inv Form.pdf.exe
VISUAL BASIC
1

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
Arrival Notice, CIA Awb Inv Form.pdf.exe	37%	Virustotal		Browse
Arrival Notice, CIA Awb Inv Form.pdf.exe	31%	ReversingLabs	Win32.Trojan.Tnega	
Arrival Notice, CIA Awb Inv Form.pdf.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:	34.0.0 Boulder Opal
Analysis ID:	527894
Start date:	24.11.2021
Start time:	14:57:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Arrival Notice, CIA Awb Inv Form.pdf.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:	23
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:	mal84.troj.evad.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.7% (good quality ratio 2.3%) • Quality average: 12.8% • Quality standard deviation: 25.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
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

C:\Users\user\AppData\Local\Temp\~DF09CCCFC54315C8A8.TMP	
Process:	C:\Users\user\Desktop\Arrival Notice, CIA Awb Inv Form.pdf.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.5280837450206026
Encrypted:	false
SSDEEP:	96:GNVdtlevDRZpak7m8llj9myGr0qLjLu3FM:GNVgvckac9my8LjL
MD5:	419FC2EF2A5F8F91499B182A69484E4A
SHA1:	7A4D9A94112A8FEA9067C9B02BF29384141ED15E
SHA-256:	B2ED57A9BB9C772B2F9D21D49EBA91BFD412B3135DAD6EFC05777FAADDA10540
SHA-512:	6A51467436A003C1357B9111D002F87F1A0DB9628C692AD2EA32652F1D12F790271F164B731D81E76665D28A07ED5C31EDEA51A414E4C46B46B074E9962210E4
Malicious:	false
Reputation:	low
Preview:	......................>... ....

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.490437985451051
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:	Arrival Notice, CIA Awb Inv Form.pdf.exe
File size:	214328
MD5:	ff71941571d8930c1125b3931d400d86
SHA1:	0a417bf568a5978777021e433bf4693893facd3e
SHA256:	bf952f1cd44de7bf63c63e502670d3a6a97eca1b5f7fd998 1ed0d235351e975f
SHA512:	19ba70c75a615446c3c482d3732b373f85a4622ebc0ef65 2a7e9b368eb30db1a096d6a4e71cc7c118d7192817c18c 6aa84429e6a5e2fadb9e8edad8ed4615528

General

SSDEEP:	1536:uZVG0Dx+5ddSVTrCH+Gbe99P0ezrHSjetlvrrs2gb16A7OsJ4AdDuZxnRVxekC3S:4G12TrQ4zOC5g7OK4AdD4re3RVa
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.........`.................................Rich....................PE..L....}.O..................................@........

File Icon

Icon Hash:	c4cccccc4cc9391

Static PE Info

General

Entrypoint:	0x401598
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4FE77DAE [Sun Jun 24 20:50:54 2012 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:	0866620dbb47fce5dcf62fd73a28087e

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Princeless@Pauperise9.LA, CN=Determinerede, OU=saddles, O=Organozinc1, L=stikordet, S=albueben, C=GN
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 11/22/2021 10:40:02 AM 11/22/2022 10:40:02 AM
Subject Chain	• E=Princeless@Pauperise9.LA, CN=Determinerede, OU=saddles, O=Organozinc1, L=stikordet, S=albueben, C=GN
Version:	3
Thumbprint MD5:	7034EF897C224C9C7BDB83E97DFC0132
Thumbprint SHA-1:	EF1AC1E686A6F1DE495F0BFD6280EE73EC06795C
Thumbprint SHA-256:	675A574FC88003464890E2D25C543E3FB3A82739956E09B5D312053E83CDCA9D
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x29880	0x2a000	False	0.45206124442	data	6.79025168082	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2b000	0xe88	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x6638	0x7000	False	0.391427176339	data	4.79823535625	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: Arrival Notice, CIA Awb Inv Form.pdf.exe PID: 6260 Parent PID: 6132

General

Start time:	14:58:04
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\Arrival Notice, CIA Awb Inv Form.pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Arrival Notice, CIA Awb Inv Form.pdf.exe"
Imagebase:	0x400000
File size:	214328 bytes
MD5 hash:	FF71941571D8930C1125B3931D400D86
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	- Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.589123852.0000000004BB0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal