ID: 531043
Sample Name: Confirming - Aviso de pago.exe
Cookbook: default.jbs
Time: 10:28:10
Date: 30/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

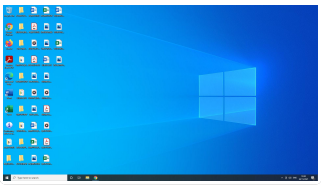
Windows Analysis Report Confirming - Aviso de pago.exe

Overview

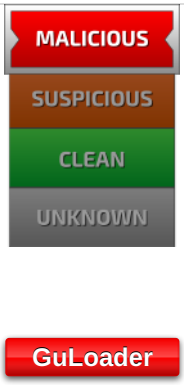
General Information

Sample Name:	Confirming - Aviso de pago.exe
Analysis ID:	531043
MD5:	660a906018931a..
SHA1:	adc917568cdfb8d..
SHA256:	520c53fa3cc5121..
Infos:	

Most interesting Screenshot:



Detection



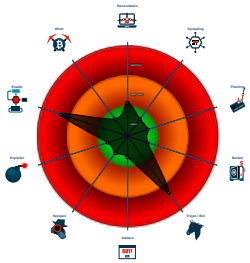
GuLoader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected GuLoader
- Hides threads from debuggers
- Writes to foreign memory regions
- Tries to detect Any.run
- C2 URLs / IPs found in malware con…
- Tries to detect sandboxes and other…
- Uses 32bit PE files
- Found a high number of Window / Us…
- Sample file is different than original …
- PE file contains strange resources
- Tries to load missing DLLs

Classification



Process Tree

- **System is w10x64native**
- Confirming - Aviso de pago.exe (PID: 4196 cmdline: "C:\Users\user\Desktop\Confirming - Aviso de pago.exe" MD5: 660A906018931AD7D39AAAF72B0B8E58)
  - conhost.exe (PID: 5596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - CasPol.exe (PID: 6552 cmdline: "C:\Users\user\Desktop\Confirming - Aviso de pago.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - CasPol.exe (PID: 3980 cmdline: "C:\Users\user\Desktop\Confirming - Aviso de pago.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 5968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: GuLoader


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.227087484559.000000000B00000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000002.00000002.227746386233.000000002350000.00000040.00000001.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

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Anti Debugging:

Hides threads from debuggers

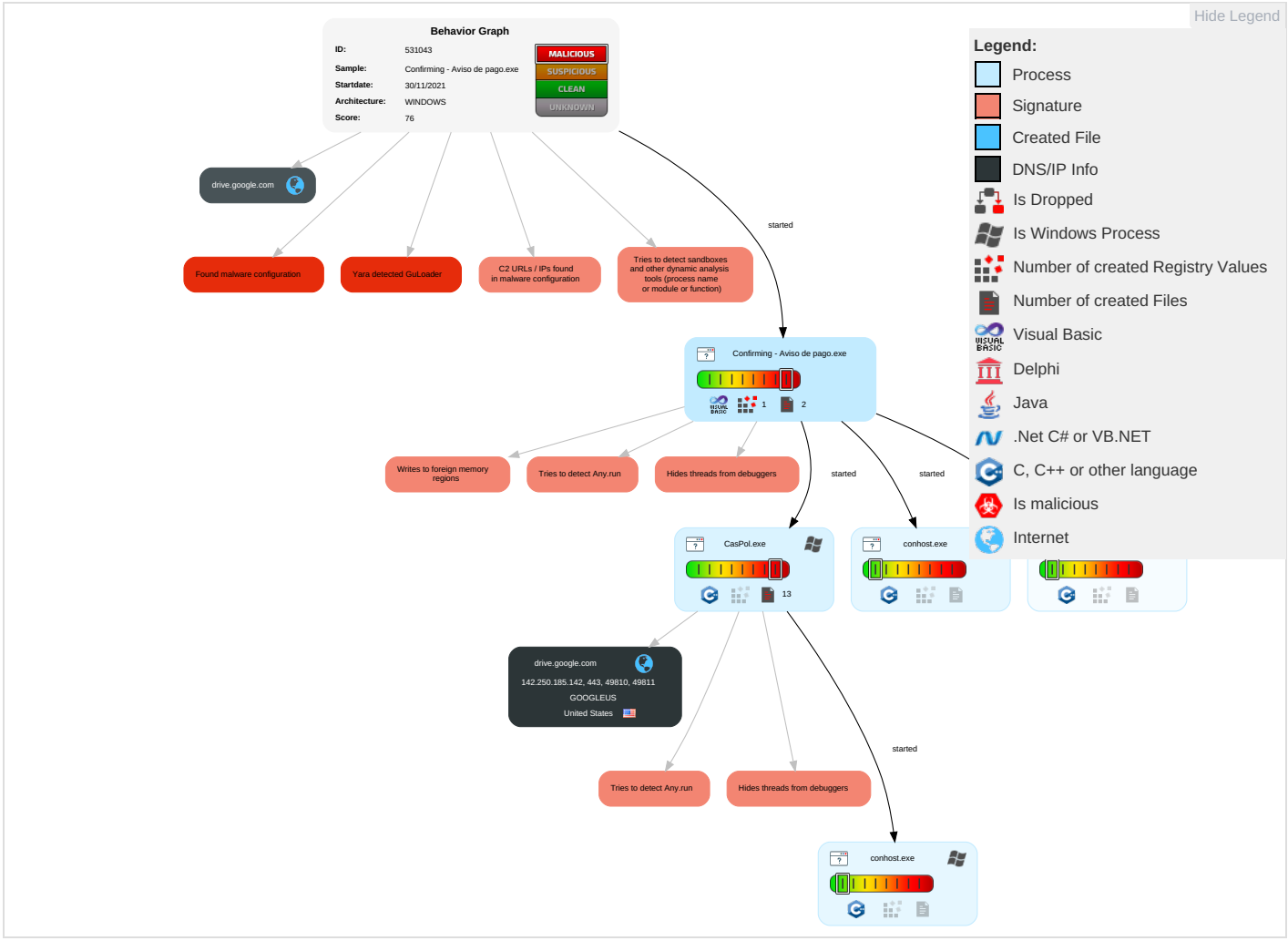
HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1 1 1	Virtualization/Sandbox Evasion 2 2	OS Credential Dumping	Security Software Discovery 3 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 1 1	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	Application Window Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

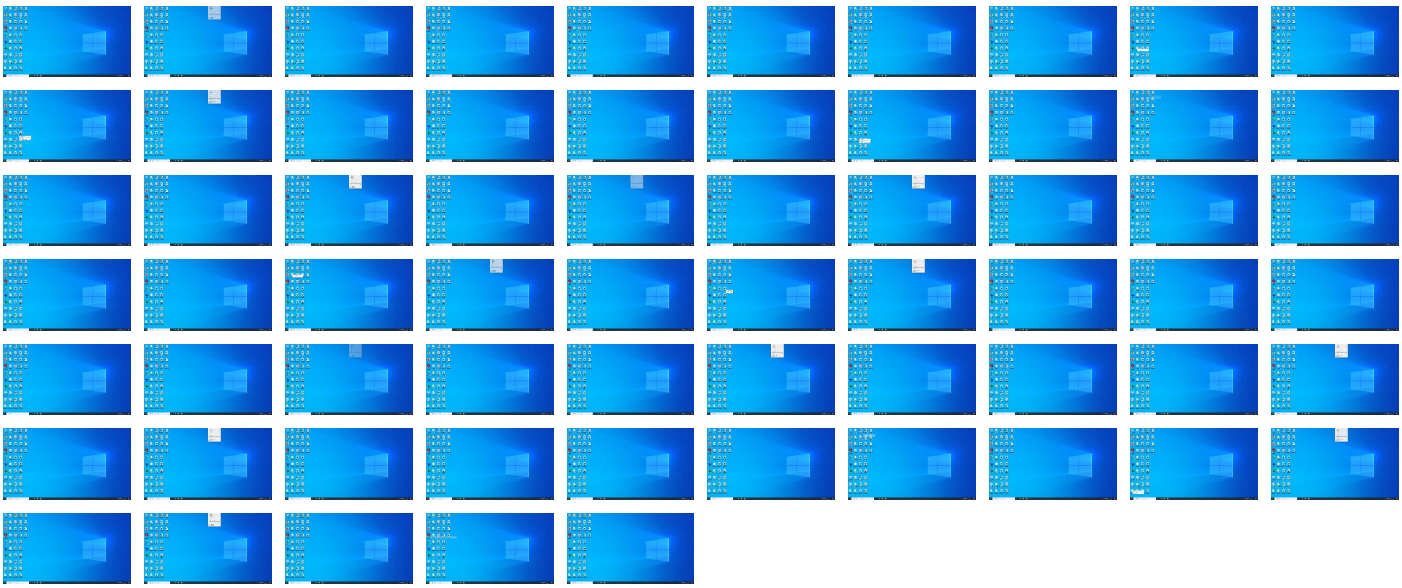
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://csp.withgoogle.com/csp/report-to/gse_l9ocaq	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.185.142	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.142	drive.google.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	531043
Start date:	30.11.2021
Start time:	10:28:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Confirming - Aviso de pago.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
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:	mal76.troj.evad.winEXE@7/1@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:30:33	API Interceptor	1353x Sleep call for process: CasPol.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	7Q8PBbf6W1.exe	Get hash	malicious	Browse	• 142.250.185.142
	desc-1753454091.xls	Get hash	malicious	Browse	• 142.250.185.142
	uI6mJo4TJQ.exe	Get hash	malicious	Browse	• 142.250.185.142
	ggLhVts2RG.exe	Get hash	malicious	Browse	• 142.250.185.142
	uI6mJo4TJQ.exe	Get hash	malicious	Browse	• 142.250.185.142
	5ZNjNuKyMn.exe	Get hash	malicious	Browse	• 142.250.185.142
	desc-1196210401.xls	Get hash	malicious	Browse	• 142.250.185.142
	desc-1257712778.xls	Get hash	malicious	Browse	• 142.250.185.142
	win-1776374194.xls	Get hash	malicious	Browse	• 142.250.185.142
	wvYbWkOPqJ.exe	Get hash	malicious	Browse	• 142.250.185.142
	wvYbWkOPqJ.exe	Get hash	malicious	Browse	• 142.250.185.142
	QOnVnFwt66.exe	Get hash	malicious	Browse	• 142.250.185.142
	Order confirmation.214254257766.PDF.exe	Get hash	malicious	Browse	• 142.250.185.142
	098765545355.DOC.exe	Get hash	malicious	Browse	• 142.250.185.142
	win-1529645453.xls	Get hash	malicious	Browse	• 142.250.185.142
	Download_Statement_(0 seconds).htm	Get hash	malicious	Browse	• 142.250.185.142
	win-1464437280.xls	Get hash	malicious	Browse	• 142.250.185.142
	win-1424700355.xls	Get hash	malicious	Browse	• 142.250.185.142
	win-1315809616.xls	Get hash	malicious	Browse	• 142.250.185.142
	order.exe	Get hash	malicious	Browse	• 142.250.185.142

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\~DF7BE08CD817A0C567.TMP	
Process:	C:\Users\user\Desktop\Confirming - Aviso de pago.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.9866006611106688

C:\Users\user\AppData\Local\Temp\~DF7BE08CD817A0C567.TMP	
Encrypted:	false
SSDEEP:	96:jWpahLKAycVxc4LlvnffSIPW0wLzzj1ylDHn3Rs:KMhLKCxV5vnffl0wIdHBs
MD5:	A256BBA112F7FA34FE9E19ED07D0DF83
SHA1:	3E86ADD7C0890C55E8F22334A3E26134D7AB1EE8
SHA-256:	AB9F6744C55428A62F4696BC1779409A30420D0983EDD5536A0D280DF5EE7FE0
SHA-512:	9E762DFE82611778602E8BF19439E48AF7278D3D9399FF44666EB8A196206F4B1B50B9B623710B138BD7A7E9C1E0A05BE85CE6FB7B0F208C9664669297C416EA
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.072456251172297
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:	Confirming - Aviso de pago.exe
File size:	155648
MD5:	660a906018931ad7d39aaaf72b0b8e58
SHA1:	adc917568cdfb8dea81c2f5793f69720609ee086
SHA256:	520c53fa3cc5121f1a8ab6600e9ee4cbe40d0f61712a4fc062c9db02953f5420
SHA512:	614ce1f2f1a0e0933c732a6bd41173ddb54862347947182c71a95f04def137802cc90d6583a791db69e4f9305ff2e1ed96edbccbf170d8eb6f10cba3286e14c4
SSDEEP:	1536:dafJffdYUfpeAxZcswCVWHSBrO4efc1SAnGlrWAEEKLBl5l1TM03fJffpfJff:YfJffnMw7BrO4AMS8pOKb3fJffpfJff
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L...d..V.....P..... ....@.....

File Icon

Icon Hash:	70ecccaececc71e2

Static PE Info

General

Entrypoint:	0x4015a8
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:	0x56E5BC64 [Sun Mar 13 19:15:48 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	458ac857eb15a6ebaad7748f2f663dae

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20998	0x21000	False	0.357577237216	data	5.23763922867	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1250	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x2f4c	0x3000	False	0.232991536458	data	4.21003728308	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

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 30, 2021 10:30:34.011313915 CET	192.168.11.20	1.1.1.1	0x544e	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 30, 2021 10:30:34.021145105 CET	1.1.1.1	192.168.11.20	0x544e	No error (0)	drive.google.com		142.250.185.142	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Confirming - Aviso de pago.exe PID: 4196 Parent PID: 1816

General

Start time:	10:30:01
Start date:	30/11/2021
Path:	C:\Users\user\Desktop\Confirming - Aviso de pago.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Confirming - Aviso de pago.exe"
Imagebase:	0x400000
File size:	155648 bytes
MD5 hash:	660A906018931AD7D39AAAF72B0B8E58
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.227746386233.0000000002350000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: conhost.exe PID: 5596 Parent PID: 4196

General

Start time:	10:30:01
Start date:	30/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6bcbe0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: CasPol.exe PID: 6552 Parent PID: 4196

General

Start time:	10:30:17
Start date:	30/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\Confirming - Aviso de pago.exe"
Imagebase:	0x180000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: 3980 Parent PID: 4196

General

Start time:	10:30:17
Start date:	30/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Confirming - Aviso de pago.exe"
Imagebase:	0x720000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000006.00000000.227087484559.0000000000B00000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 5968 Parent PID: 3980

General

Start time:	10:30:18
Start date:	30/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6bcbe0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Disassembly

Code Analysis