

JOeSandbox Cloud BASIC



ID: 531732

Sample Name: Purchase Order
PO20211027STK.exe

Cookbook: default.jbs

Time: 09:57:30

Date: 01/12/2021

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report Purchase Order PO20211027STK.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: GuLoader	4
Yara Overview	4
Memory Dumps	4
Sigma Overview	4
Jbx Signature Overview	5
AV Detection:	5
Networking:	5
System Summary:	5
Data Obfuscation:	5
Malware Analysis System Evasion:	5
Anti Debugging:	5
HIPS / PFW / Operating System Protection Evasion:	5
Stealing of Sensitive Information:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
Contacted URLs	8
URLs from Memory and Binaries	8
Contacted IPs	8
General Information	8
Simulations	8
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
Static File Info	9
General	9
File Icon	10
Static PE Info	10
General	10
Entrypoint Preview	10
Rich Headers	10
Data Directories	10
Sections	10
Resources	11
Imports	11
Possible Origin	11
Network Behavior	11
Network Port Distribution	11
UDP Packets	11
DNS Queries	11
DNS Answers	11
Code Manipulations	11
Statistics	11
Behavior	11
System Behavior	11
Analysis Process: Purchase Order PO20211027STK.exe PID: 7088 Parent PID: 4328	12
General	12
File Activities	12
File Created	12
File Deleted	12
File Written	12
File Read	12

Analysis Process: SPORENE.exe PID: 7152 Parent PID: 7088	12
General	12
File Activities	12
Analysis Process: CasPol.exe PID: 6848 Parent PID: 7152	12
General	12
File Activities	13
Analysis Process: conhost.exe PID: 6836 Parent PID: 6848	13
General	13
Disassembly	13
Code Analysis	13

Windows Analysis Report Purchase Order PO20211027...

Overview

General Information

Sample Name:

Purchase Order PO20211027STK.exe

Analysis ID:

531732

MD5:

2f2102ec5776497.

SHA1:

1d3dd4ed88af22c.

SHA256:

7768da29cc4ef93..

Tags:

exe

guloader

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

GuLoader behavior detected

Yara detected GuLoader

Hides threads from debuggers

Initial sample is a PE file and has a ...

Writes to foreign memory regions

Tries to detect Any.run

Tries to detect sandboxes and other...

Machine Learning detection for samp...

Executable has a suspicious name (...

C2 URLs / IPs found in malware con...

Classification

Process Tree

System is w10x64

Purchase Order PO20211027STK.exe (PID: 7088 cmdline: "C:\Users\user\Desktop\Purchase Order PO20211027STK.exe" MD5: 2F2102EC5776497950E89E419515EFEE)

SPORENE.exe (PID: 7152 cmdline: C:\Users\user\AppData\Local\Temp\SPORENE.exe MD5: 582A642DF36CDAC38982E4842F370B44)

CasPol.exe (PID: 6848 cmdline: C:\Users\user\AppData\Local\Temp\SPORENE.exe MD5: F866FC1C2E928779C7119353C3091F0C)

conhost.exe (PID: 6836 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

cleanup

Malware Configuration

Threatname: GuLoader

```
{  "Payload URL": "https://onedrive.live.com/download?cid=5A15FDA1AE98540B&r"}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000000.509732142.000000000130 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000A.00000002.626110069.000000000130 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	


Sigma Overview

No Sigma rule has matched

Copyright Joe Security LLC 2021

Page 4 of 13

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

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

Stealing of Sensitive Information:



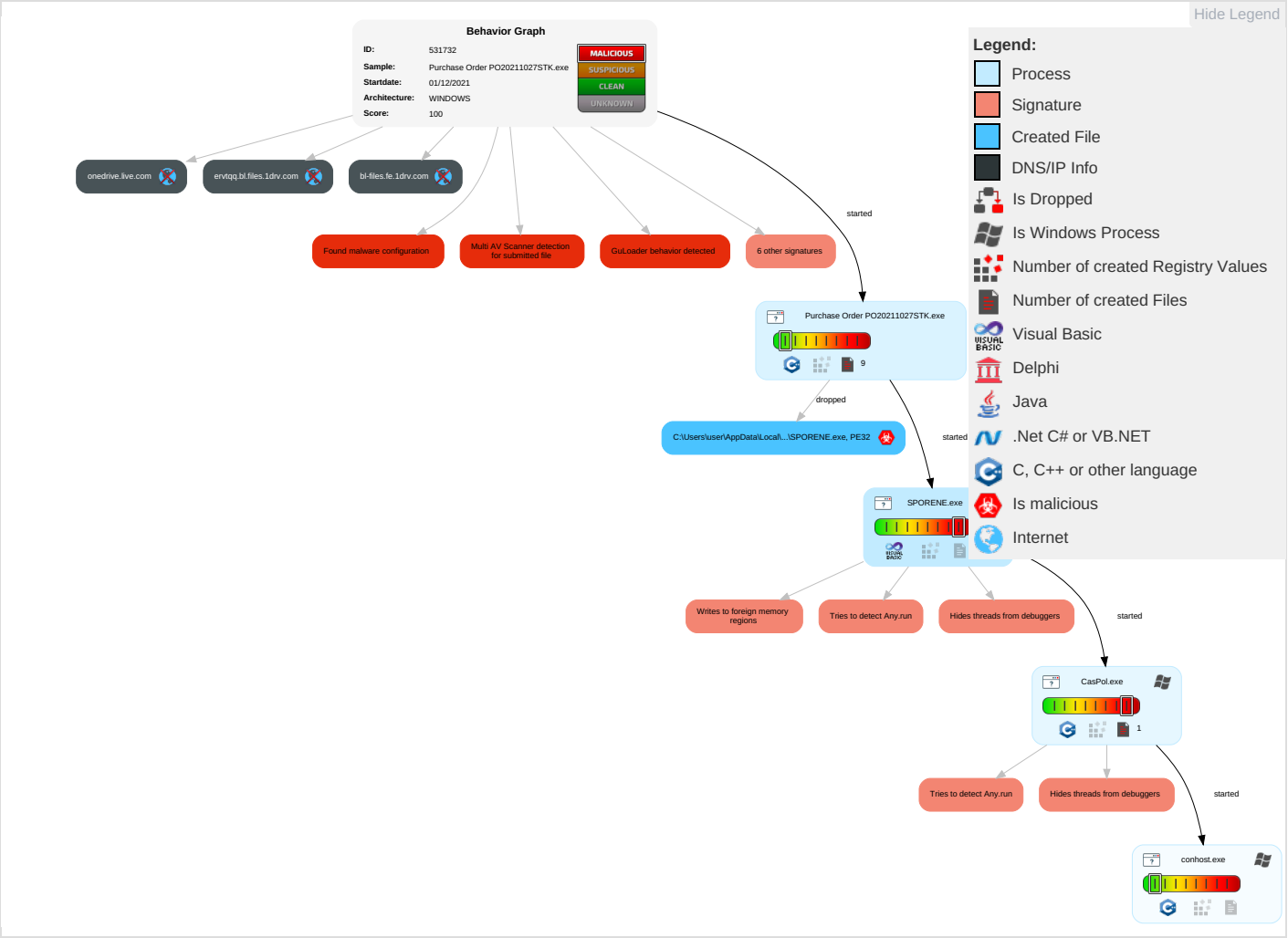
GuLoader behavior detected

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	Path Interception	Access Token Manipulation 1	Virtualization/Sandbox Evasion 2	OS Credential Dumping	Security Software Discovery 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel! 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Access Token Manipulation 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

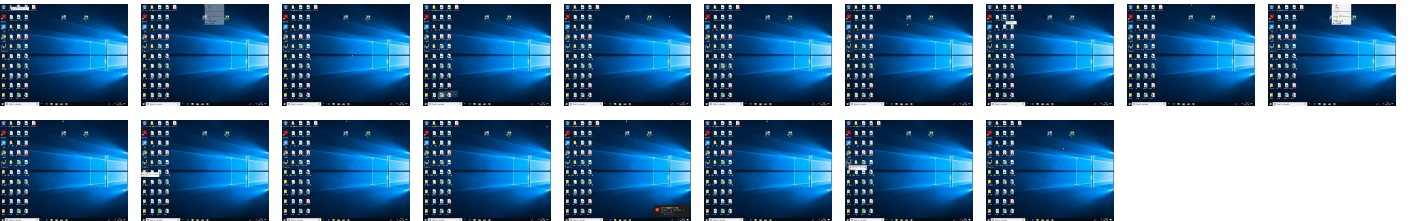
Behavior Graph



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
Purchase Order PO20211027STK.exe	11%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Purchase Order PO20211027STK.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\SPORENE.exe	9%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onedrive.live.com	unknown	unknown	false		high
ervtqq.bl.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?cid=5A15FDA1AE98540B&r	false		high

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	531732
Start date:	01.12.2021
Start time:	09:57:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order PO20211027STK.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:	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:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/1@2/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 100% (good quality ratio 97.1%)• Quality average: 83.8%• Quality standard deviation: 24.5%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">• 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\SPORENE.exe

Process:	C:\Users\user\Desktop\Purchase Order PO20211027STK.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21321008
Entropy (8bit):	0.09325738133607682
Encrypted:	false
SSDEEP:	3072:mlXeoCC869BrI49jK9oUhJSSjfv8XEHPo:madlYoUZf2EvO
MD5:	582A642DF36CDAC38982E4842F370B44
SHA1:	3DD6D0CECD4CD9414D7DF148F7C46548C5709D62
SHA-256:	361DEDDF3E436753730DBB20842FBD6D1EF2EC27C56CD9DA99E87751C3BBE890
SHA-512:	E9C94417ACEF2B33DED79182C8B397E2693A74D290E78E286AE7576C998BF14F39F370C06BC40C9DFFDF2DE2E7F680AA0F33D74DB508E15EEAF1D31BE8D06EB6
Malicious:	true
Antivirus:	<ul style="list-style-type: none">Antivirus: ReversingLabs, Detection: 9%
Reputation:	low
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....SM.SM.SM..Q..RM..o.UM.ek.RM.RichSM.....PE..L.. ...5Y.....OC...\$.....@.....@E.....qE.....(.....C.....P@E.....0.. ..txt......`.data...p.....@....rsrc....C. ... C.@...@...I.....MSVBVM60.DLL.....

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.060974988277113

General

TrID:	<ul style="list-style-type: none">Win32 Executable (generic) a (10002005/4) 99.96%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:	Purchase Order PO20211027STK.exe
File size:	131031
MD5:	2f2102ec5776497950e89e419515efee
SHA1:	1d3dd4ed88af22c3de29c918b37db6f0b73c94c4
SHA256:	7768da29cc4ef93cb4790f664e139d1d8c2972e22fe8840b6b86c50e15dba347
SHA512:	963b79cb63703ea6a6e8d70bbe76fadc660e10b801283a3812a76f773ee36210171437794dad0b4ee11e8a2f3464c88c7463526be03274ffdf48ec81823032a
SSDEEP:	3072:gbG7N2kDTHUpou4ubV4QviYqsYLYl9xxsFIRO7c3fkA:gbE/HUjV4QviYJMQXyFIR2HA
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......1...Pf..P f..Pf.*_9..Pf..Pg.LPf.*_..Pf..sv..Pf..V'..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon



Icon Hash:	b2a88c96b2ca6a72
------------	------------------

Static PE Info

General

Entrypoint:	0x40352d
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:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 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:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x16000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x4c000	0x11e0	0x1200	False	0.368489583333	data	4.48173978815	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 1, 2021 10:00:47.501432896 CET	192.168.2.6	8.8.8.8	0x9999	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:00:48.096002102 CET	192.168.2.6	8.8.8.8	0xbde	Standard query (0)	ervtqq.bl.files.1drv.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 10:00:47.535913944 CET	8.8.8.8	192.168.2.6	0x9999	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:00:48.138751984 CET	8.8.8.8	192.168.2.6	0xbde	No error (0)	ervtqq.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:00:48.138751984 CET	8.8.8.8	192.168.2.6	0xbde	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Purchase Order PO20211027STK.exe PID: 7088 Parent PID: 4328**General**

Start time:	09:58:37
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\Purchase Order PO20211027STK.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Purchase Order PO20211027STK.exe"
Imagebase:	0x400000
File size:	131031 bytes
MD5 hash:	2F2102EC5776497950E89E419515EFEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created**File Deleted****File Written****File Read****Analysis Process: SPORENE.exe PID: 7152 Parent PID: 7088****General**

Start time:	09:58:40
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\SPORENE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\SPORENE.exe
Imagebase:	0x400000
File size:	21321008 bytes
MD5 hash:	582A642DF36CDAC38982E4842F370B44
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 9%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: CasPol.exe PID: 6848 Parent PID: 7152**General**

Start time:	09:59:47
Start date:	01/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\SPORENE.exe
Imagebase:	0xea0000

File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000A.00000000.509732142.0000000001300000.00000040.00000001.sdmp, Author: Joe SecurityRule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000A.00000002.626110069.0000000001300000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

[File Activities](#)

Show Windows behavior

Analysis Process: conhost.exe PID: 6836 Parent PID: 6848

General

Start time:	09:59:49
Start date:	01/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis