ID: 527899
Sample Name:
REVGKXx6Ns.exe
Cookbook: default.jbs
Time: 15:19:59
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

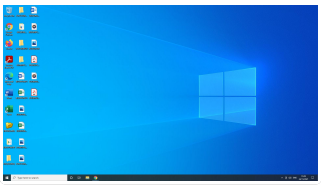
Windows Analysis Report REVGKXx6Ns.exe

Overview

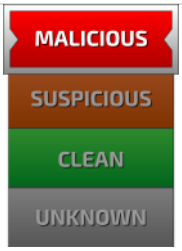
General Information

Sample Name:	REVGKXx6Ns.exe
Analysis ID:	527899
MD5:	7c91db57c98a1f0..
SHA1:	28cb0d40a73c1a..
SHA256:	12992fe3f998693..
Infos:	

Most interesting Screenshot:



Detection



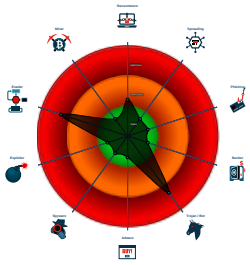
AgentTesla GuLoader

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Found detection on Joe Sandbox Clo…
- Multi AV Scanner detection for subm…
- 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 …

Classification



Process Tree

- **System is w10x64native**
- REVGKXx6Ns.exe (PID: 7208 cmdline: "C:\Users\user\Desktop\REVGKXx6Ns.exe" MD5: 7C91DB57C98A1F0E38BA65ED651B4779)
  - CasPol.exe (PID: 3300 cmdline: "C:\Users\user\Desktop\REVGKXx6Ns.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 3304 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: GuLoader


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.1029767674.0000000000F00000.00000040.00000001.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

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Found detection on Joe Sandbox Cloud Basic with higher score

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

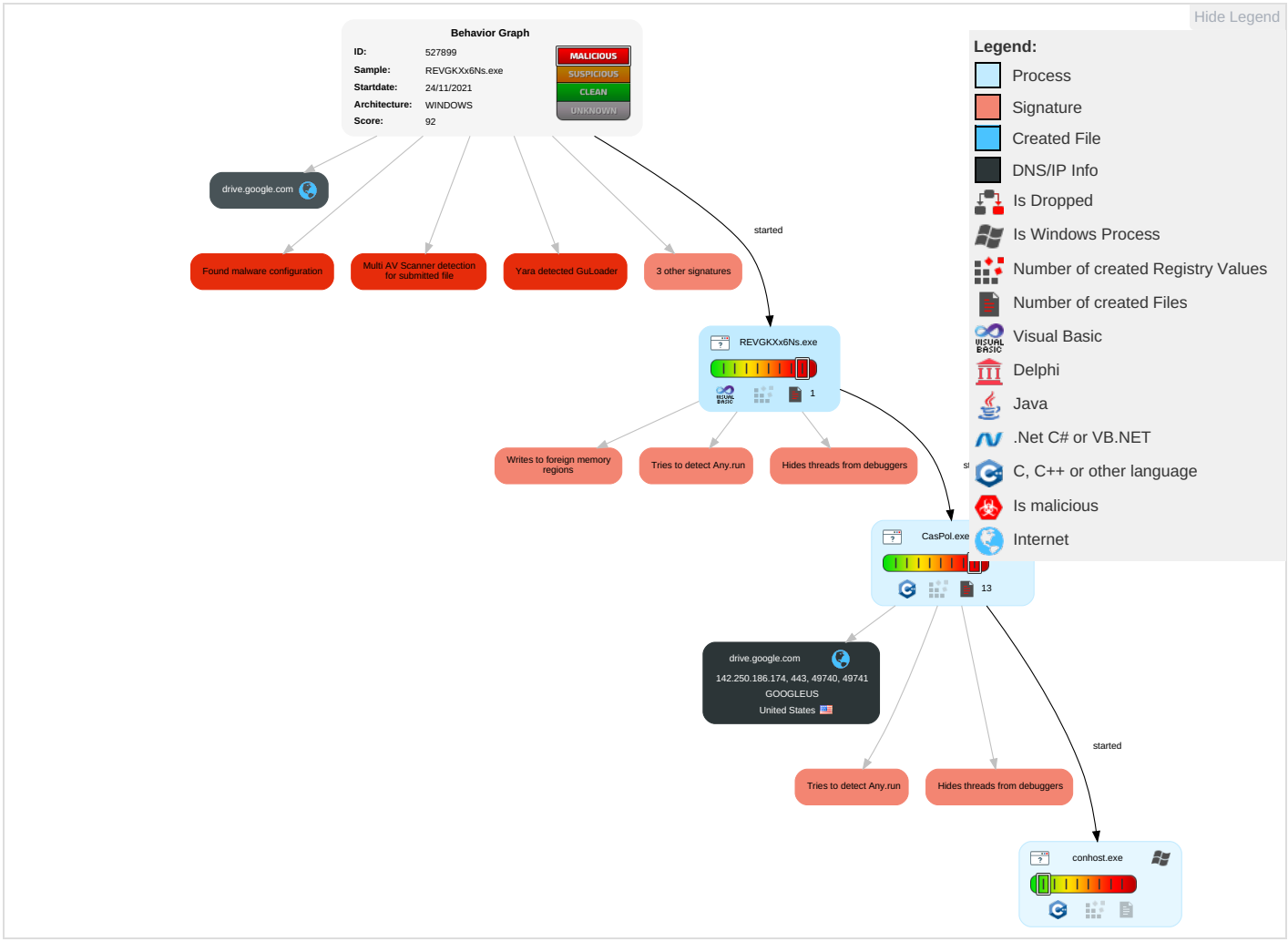
HIPS / PFW / Operating System Protection Evasion:

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	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 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

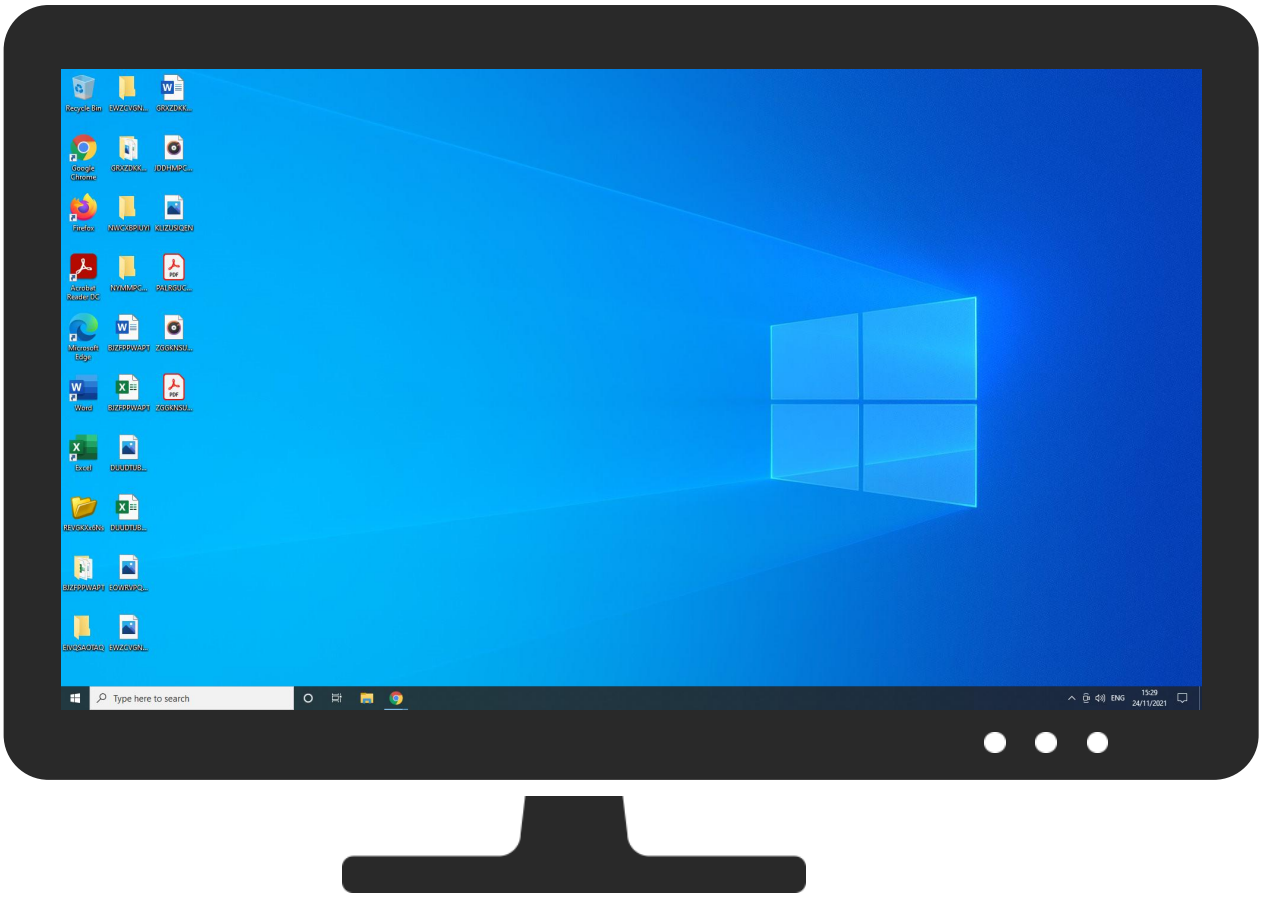
Behavior Graph



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

Source	Detection	Scanner	Label	Link
REVGKXx6Ns.exe	63%	Virustotal		Browse
REVGKXx6Ns.exe	34%	Metadefender		Browse
REVGKXx6Ns.exe	71%	ReversingLabs	Win32.Trojan.GuLoader	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.topqualityfreeware.com/	0%	Virustotal		Browse
http://www.topqualityfreeware.com/	0%	Avira URL Cloud	safe	
http://topqualityfreeware.com	0%	Virustotal		Browse
http://topqualityfreeware.com	0%	Avira URL Cloud	safe	
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	142.250.186.174	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	527899
Start date:	24.11.2021
Start time:	15:19:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	REVGKXx6Ns.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:	21
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:	mal92.troj.evad.winEXE@4/1@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
15:22:22	API Interceptor	1432x 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	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• 142.250.186.174
	TT-PRIME USD242,357,59.ppam	Get hash	malicious	Browse	• 142.250.186.174
	chase.xls	Get hash	malicious	Browse	• 142.250.186.174
	Statement from QNB.exe	Get hash	malicious	Browse	• 142.250.186.174
	private-1915056036.xls	Get hash	malicious	Browse	• 142.250.186.174
	private-1910485378.xls	Get hash	malicious	Browse	• 142.250.186.174
	doc201002124110300200.exe	Get hash	malicious	Browse	• 142.250.186.174
	t 2021.HtML	Get hash	malicious	Browse	• 142.250.186.174
	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 142.250.186.174
	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 142.250.186.174
	Justificante.exe	Get hash	malicious	Browse	• 142.250.186.174
	muhammadbad.html	Get hash	malicious	Browse	• 142.250.186.174
	MtCsSK9TK2.exe	Get hash	malicious	Browse	• 142.250.186.174
	0331C7BCA665F36513377FC301CBB32822FF35F925115.exe	Get hash	malicious	Browse	• 142.250.186.174
	6D2FF3CC83EA214E33E4105CCB1051CD85B82E052F615.exe	Get hash	malicious	Browse	• 142.250.186.174
	vAsfZhw32P.exe	Get hash	malicious	Browse	• 142.250.186.174
	FpYf5EGDO9.exe	Get hash	malicious	Browse	• 142.250.186.174
	#U0191ACTU#U0156A_unxsxdxX_f_mMT_312.vbs	Get hash	malicious	Browse	• 142.250.186.174
	FhP4JYCU7J.exe	Get hash	malicious	Browse	• 142.250.186.174
	ugeLMlEROB.exe	Get hash	malicious	Browse	• 142.250.186.174

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\~DF0E195A349794F694.TMP	
Process:	C:\Users\user\Desktop\REVGKXx6Ns.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	4.01191323271951
Encrypted:	false
SSDEEP:	384:wcZ0tADSVlx6JQhynrV7Vr9wrCIM/ZUYVPzBAPN:wcZeADSV/6qhynrV7VxwrrMvqPN
MD5:	6C4C01A4316CD9338DE51EC175EBF11D
SHA1:	8C5D5B07E0ED6AAC72705F516E25BEAEA891EFA0
SHA-256:	95876F7C1242672418DB201C02D70276EE9CC4345394DEAD3500619A39DA28F0
SHA-512:	9F60729E865B0414DB4792F76465EDCE1595D22E884D01C07389A312474D1CE916E4CF73275D5AA0CB411D8EBB0617EF661CD10467AD838FD1B0B388C44823D
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.926810109816392
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:	REVGKXx6Ns.exe
File size:	192512
MD5:	7c91db57c98a1f0e38ba65ed651b4779
SHA1:	28cb0d40a73c1a421a9720808d49da010f9ff4ef
SHA256:	12992fe3f998693d92625c53bf5aa6723e87c8c3fb7057dbba4b334742cab376
SHA512:	2ca3ac7de708b85262bd7e9d42b0cd78cd0af4f92c1da9c7be9d2e473bcc238a5935030eff688049d8c75fd3c3fd8fd80a5703eca4ab112e3a0997e74d6ac58a
SSDEEP:	3072:tdejCYyLGrRDAfor5hlNZI71PAMrc0yvhXeJ:tdeiGrRDAfA5XXMrcbeJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....*.....Rich.....PE..L.....&T.....0.....L.....@....@.....

File Icon

Icon Hash:	0ceefedec6f67c0c

Static PE Info

General

Entrypoint:	0x40134c
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:	0x54260EAF [Sat Sep 27 01:11:11 2014 UTC]

General

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:	f27a613fda76c14f4eab7dc0085d799e

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x229ac	0x23000	False	0.354959542411	data	5.0849300681	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x24000	0x13f0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x26000	0x90d5	0xa000	False	0.346411132813	data	4.35437576998	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	
Turkmen	Turkmenistan	

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2021 15:22:22.268563032 CET	192.168.11.20	1.1.1.1	0xef00	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 24, 2021 15:22:22.278042078 CET	1.1.1.1	192.168.11.20	0xef00	No error (0)	drive.google.com		142.250.186.174	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: REVGKXx6Ns.exe PID: 7208 Parent PID: 8484

General

Start time:	15:21:54
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\REVGKXx6Ns.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\REVGKXx6Ns.exe"
Imagebase:	0x400000
File size:	192512 bytes
MD5 hash:	7C91DB57C98A1F0E38BA65ED651B4779
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: CasPol.exe PID: 3300 Parent PID: 7208

General

Start time:	15:22:09
Start date:	24/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\REVGKXx6Ns.exe"
Imagebase:	0xa80000
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: 00000003.00000000.1029767674.0000000000F00000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities | Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 3304 Parent PID: 3300

General

Start time:	15:22:10
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff66ea70000
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