ID: 438540
Sample Name: jrC504LJVe.dll
Cookbook: default.jbs
Time: 18:22:15
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report jrC504LJVe.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 5
Initial Sample 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 6
Hooking and other Techniques for Hiding and Protection: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted IPs 9
General Information 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 10
General 10
File Icon 10
Static PE Info 11
General 11
Entrypoint Preview 11
Rich Headers 11
Data Directories 11
Sections 11
Resources 11
Imports 11
Exports 11
Possible Origin 11
Network Behavior 11
Code Manipulations 12
Statistics 12
Behavior 12
System Behavior 12
Analysis Process: loaddll32.exe PID: 4220 Parent PID: 5816 12
General 12
File Activities 12
Analysis Process: cmd.exe PID: 5524 Parent PID: 4220 12
General 12
File Activities 12
Analysis Process: rundll32.exe PID: 5896 Parent PID: 4220 13
General 13
Analysis Process: rundll32.exe PID: 3512 Parent PID: 5524 13
General 13
Analysis Process: cmd.exe PID: 4120 Parent PID: 5896 13

General 13
File Activities 13
Analysis Process: cmd.exe PID: 5580 Parent PID: 3512 14
General 14
File Activities 14
Analysis Process: conhost.exe PID: 3412 Parent PID: 4120 14
General 14
Analysis Process: conhost.exe PID: 5668 Parent PID: 5580 14
General 14
Analysis Process: cmd.exe PID: 5512 Parent PID: 5896 14
General 14
File Activities 15
Analysis Process: cmd.exe PID: 4084 Parent PID: 3512 15
General 15
File Activities 15
Analysis Process: conhost.exe PID: 1304 Parent PID: 5512 15
General 15
Analysis Process: conhost.exe PID: 4808 Parent PID: 4084 15
General 15
Analysis Process: rundll32.exe PID: 1384 Parent PID: 4220 16
General 16
Analysis Process: cmd.exe PID: 5668 Parent PID: 1384 16
General 16
File Activities 16
Analysis Process: conhost.exe PID: 5808 Parent PID: 5668 16
General 16
Analysis Process: rundll32.exe PID: 1304 Parent PID: 4220 17
General 17
Analysis Process: cmd.exe PID: 4188 Parent PID: 1384 17
General 17
File Activities 17
Analysis Process: conhost.exe PID: 5516 Parent PID: 4188 17
General 17
Analysis Process: cmd.exe PID: 5660 Parent PID: 1304 18
General 18
File Activities 18
Analysis Process: conhost.exe PID: 6236 Parent PID: 5660 18
General 18
Analysis Process: rundll32.exe PID: 6276 Parent PID: 4220 18
General 18
Analysis Process: cmd.exe PID: 6292 Parent PID: 1304 18
General 18
File Activities 19
Analysis Process: conhost.exe PID: 6388 Parent PID: 6292 19
General 19
Analysis Process: cmd.exe PID: 6400 Parent PID: 6276 19
General 19
File Activities 19
Analysis Process: conhost.exe PID: 6440 Parent PID: 6400 19
General 19
Analysis Process: rundll32.exe PID: 6476 Parent PID: 4220 20
General 20
Analysis Process: cmd.exe PID: 6496 Parent PID: 6276 20
General 20
File Activities 20
Analysis Process: conhost.exe PID: 6504 Parent PID: 6496 20
General 20
Analysis Process: cmd.exe PID: 6528 Parent PID: 6476 21
General 21
File Activities 21
Analysis Process: cmd.exe PID: 6700 Parent PID: 4220 21
General 21
File Activities 21
Analysis Process: conhost.exe PID: 6724 Parent PID: 6528 21
General 21
Analysis Process: cmd.exe PID: 6908 Parent PID: 4220 21
General 22
File Activities 22
Analysis Process: cmd.exe PID: 6920 Parent PID: 6476 22
General 22
File Activities 22
Analysis Process: conhost.exe PID: 6944 Parent PID: 6920 22
General 22
Disassembly 22
Code Analysis 22

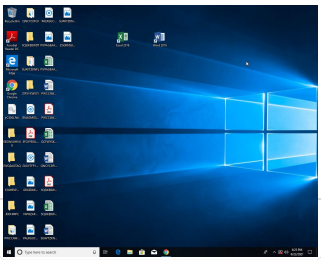
Windows Analysis Report jrC504LJVe.dll

Overview

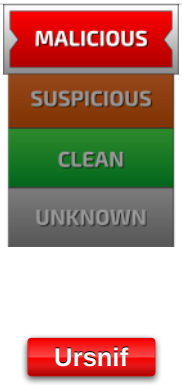
General Information

Sample Name:	jrC504LJVe.dll
Analysis ID:	438540
MD5:	4fa3dba44cab35c..
SHA1:	fed3518314015a7.
SHA256:	968b60db061083..
Tags:	dll Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection

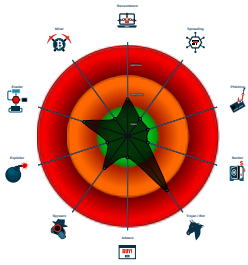


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Ursnif
- Contains functionality to check if a d…
- Contains functionality to open a port…
- Contains functionality to query CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Creates a process in suspended mo…
- Detected potential crypto function
- Found potential string decryption / a…
- PE file contains an invalid checksum
- Program does not show much activi…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4220 cmdline: loaddll32.exe 'C:\Users\user\Desktop\jrC504LJVe.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5524 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\jrC504LJVe.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3512 cmdline: rundll32.exe 'C:\Users\user\Desktop\jrC504LJVe.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 5580 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5668 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - conhost.exe (PID: 5808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 4084 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 5896 cmdline: rundll32.exe C:\Users\user\Desktop\jrC504LJVe.dll,Connectdark MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 4120 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 3412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 5512 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 1304 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - cmd.exe (PID: 5660 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 6236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - cmd.exe (PID: 6292 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 6388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 1384 cmdline: rundll32.exe C:\Users\user\Desktop\jrC504LJVe.dll,Mindlake MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 5668 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - cmd.exe (PID: 4188 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5516 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 1304 cmdline: rundll32.exe C:\Users\user\Desktop\jrC504LJVe.dll,Porthigh MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6276 cmdline: rundll32.exe C:\Users\user\Desktop\jrC504LJVe.dll,Problemscale MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 6400 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6496 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 6476 cmdline: rundll32.exe C:\Users\user\Desktop\jrC504LJVe.dll,WingGrass MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 6528 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6920 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6944 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6700 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - cmd.exe (PID: 6908 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
jrC504LJVe.dll	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.507194877.000000006E1E1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000016.00000002.529754214.000000006E1E1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000000.00000002.501190054.000000006E1E1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
0000001B.00000002.513290873.000000006E1E1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000003.00000002.507194291.000000006E1E1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.rundll32.exe.6e1e0000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.6e1e0000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
14.2.rundll32.exe.6e1e0000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
27.2.rundll32.exe.6e1e0000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
22.2.rundll32.exe.6e1e0000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
Click to see the 2 entries				

Sigma Overview

System Summary:

Sigma detected: Conhost Parent Process Executions

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

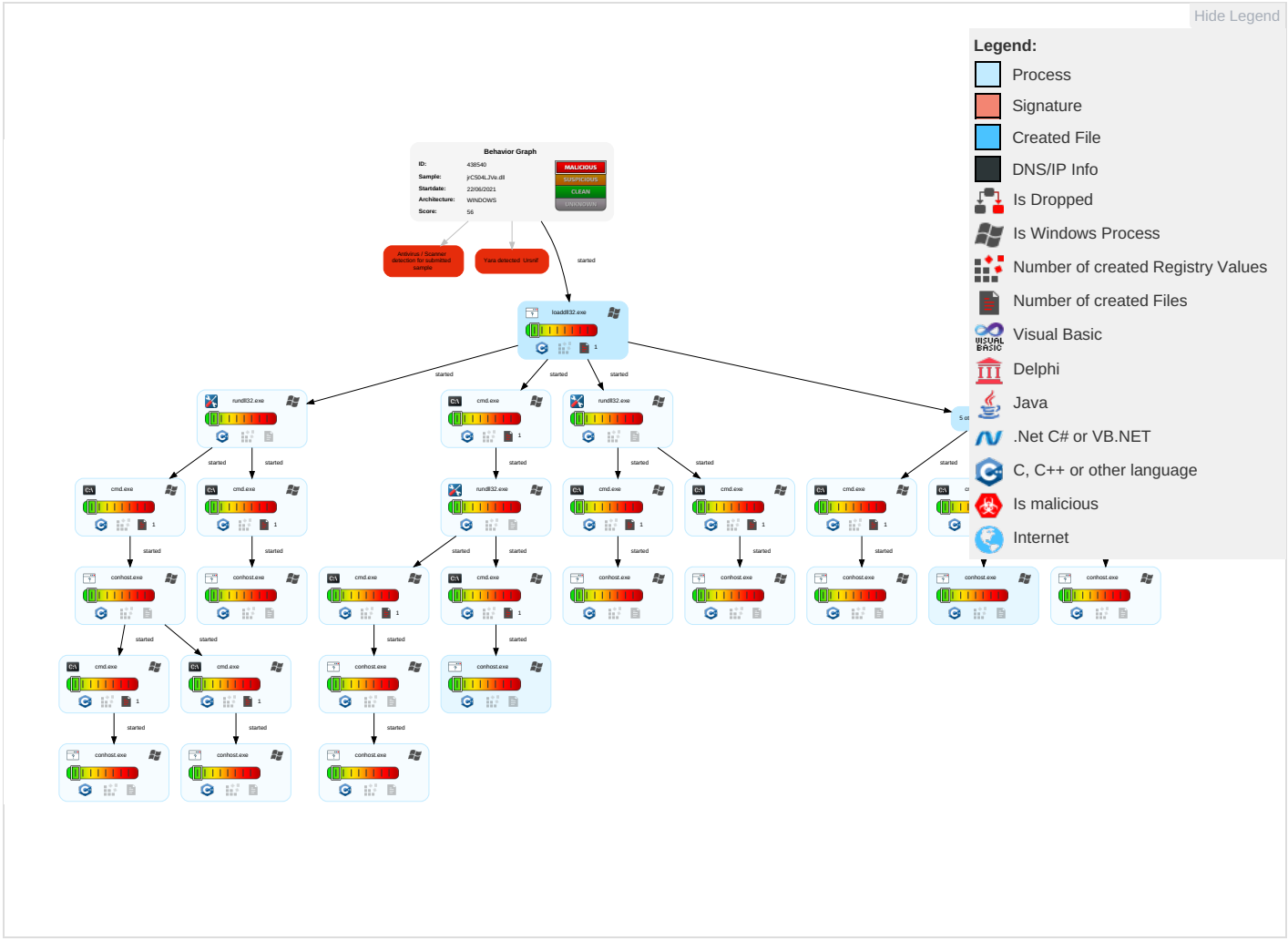
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remot Servic Effect
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Rundll32 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remot Track I Withou Author
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remot Wipe D Withou Author
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode 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	Obtain Device Cloud Backup
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Information Discovery 2 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

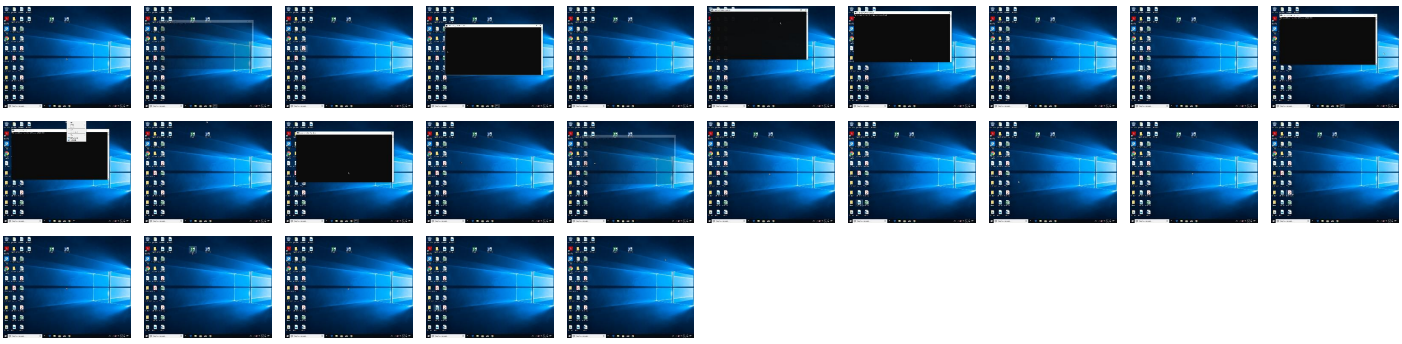
Behavior Graph



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
jrC504LJVe.dll	100%	Avira	TR/Spy.Ursnif.ozghq	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.rundll32.exe.6e1e0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
22.2.rundll32.exe.6e1e0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
27.2.rundll32.exe.6e1e0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
3.2.rundll32.exe.6e1e0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
2.2.rundll32.exe.6e1e0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
0.2.loaddll32.exe.6e1e0000.0.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
14.2.rundll32.exe.6e1e0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File

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:	32.0.0 Black Diamond
Analysis ID:	438540
Start date:	22.06.2021
Start time:	18:22:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	jrC504LJVe.dll
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:	42
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:	mal56.troj.winDLL@55/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.5% (good quality ratio 13.6%) • Quality average: 73.2% • Quality standard deviation: 27.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
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 (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.790060010800437
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	jrC504LJVe.dll
File size:	960000
MD5:	4fa3dba44cab35c7df9dc08db6afc469
SHA1:	fed3518314015a7a79e33f36aed871bbf72affdc
SHA256:	968b60db061083b1450cbf3e1011c0869429cbd5e1d304490b86257d9c1eedbb
SHA512:	2bc007b66b4408dfa8288ae17720266b6bcf314ad8475a4a52425052fbd89d40e1aa04016f361d112c95e47c539ec3cfd87648ba6f8f9849f3071cd709d49ff6
SSDEEP:	24576:HQfpzjXPgfX8CJV4X+IBIJ3cazaLwj1mCG9CpNiLi:IFDg7JV4OaIRj150CpNiLi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t...0...0...0....{i.3...9...#...b...4...b...=...b...=....{r.&...0.....b.....b...1...b.b.1...0...1...b...1...Rich0.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1040052
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5AC512FB [Wed Apr 4 18:01:31 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	7a79d10b1d4343a18a4f6e25e165b4ae

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x883dc	0x88400	False	0.544624426606	data	6.71833706378	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8a000	0x5a440	0x5a600	False	0.658643456086	data	5.95813601066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xe5000	0x17ebc	0x1c00	False	0.184291294643	data	4.04646123564	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xfd000	0x9d0	0xa00	False	0.396484375	data	3.77819611332	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfe000	0x5074	0x5200	False	0.726133765244	data	6.63977268899	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 4220 Parent PID: 5816

General

Start time:	18:23:01
Start date:	22/06/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\jrC504LJVe.dll'
Imagebase:	0x1390000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000000.00000002.501190054.000000006E1E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5524 Parent PID: 4220

General

Start time:	18:23:01
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\jrC504LJVe.dll',#1
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5896 Parent PID: 4220

General

Start time:	18:23:02
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\jrC504LJVe.dll,Connectdark
Imagebase:	0x160000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000002.00000002.507194877.000000006E1E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 3512 Parent PID: 5524

General

Start time:	18:23:02
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\jrC504LJVe.dll',#1
Imagebase:	0x160000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000003.00000002.507194291.000000006E1E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: cmd.exe PID: 4120 Parent PID: 5896

General

Start time:	18:23:02
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5580 Parent PID: 3512

General

Start time:	18:23:02
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 3412 Parent PID: 4120

General

Start time:	18:23:03
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5668 Parent PID: 5580

General

Start time:	18:23:03
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 5512 Parent PID: 5896

General

Start time:	18:23:03

Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 4084 Parent PID: 3512

General

Start time:	18:23:03
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 1304 Parent PID: 5512

General

Start time:	18:23:04
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 4808 Parent PID: 4084

General

Start time:	18:23:04
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 1384 Parent PID: 4220

General

Start time:	18:23:06
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\jrC504LJVe.dll,Mindlake
Imagebase:	0x160000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000000E.00000002.537272561.000000006E1E1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 5668 Parent PID: 1384

General

Start time:	18:23:07
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5808 Parent PID: 5668

General

Start time:	18:23:07
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 1304 Parent PID: 4220

General

Start time:	18:23:10
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\jrC504LJVe.dll,Porthigh
Imagebase:	0x160000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000011.00000002.525353874.000000006E1E1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 4188 Parent PID: 1384

General

Start time:	18:23:10
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5516 Parent PID: 4188

General

Start time:	18:23:11
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5660 Parent PID: 1304

General

Start time:	18:23:11
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6236 Parent PID: 5660

General

Start time:	18:23:13
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6276 Parent PID: 4220

General

Start time:	18:23:15
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\jrC504LJVe.dll,Problemscale
Imagebase:	0x160000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000016.00000002.529754214.000000006E1E1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 6292 Parent PID: 1304

General

Start time:	18:23:15
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6388 Parent PID: 6292

General

Start time:	18:23:20
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6400 Parent PID: 6276

General

Start time:	18:23:20
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6440 Parent PID: 6400

General

Start time:	18:23:21
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6476 Parent PID: 4220

General

Start time:	18:23:24
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\jrC504LJVe.dll,WingGrass
Imagebase:	0x160000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000001B.00000002.513290873.000000006E1E1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 6496 Parent PID: 6276

General

Start time:	18:23:25
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6504 Parent PID: 6496

General

Start time:	18:23:27
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6528 Parent PID: 6476

General

Start time:	18:23:30
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6700 Parent PID: 4220

General

Start time:	18:23:30
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6724 Parent PID: 6528

General

Start time:	18:23:32
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6908 Parent PID: 4220

General

Start time:	18:23:40
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6920 Parent PID: 6476

General

Start time:	18:23:40
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6944 Parent PID: 6920

General

Start time:	18:23:41
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis