ID: 498859
Sample Name: c3.dll
Cookbook: default.jbs
Time: 15:53:27
Date: 07/10/2021
Version: 33.0.0 White Diamond

Table of Contents

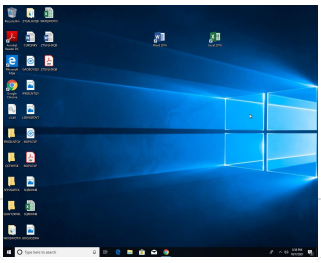
Windows Analysis Report c3.dll

Overview

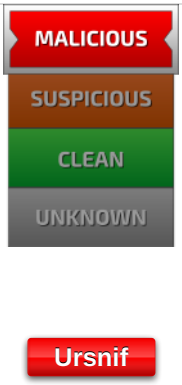
General Information

Sample Name:	c3.dll
Analysis ID:	498859
MD5:	c309ec3264c7bf7..
SHA1:	2af04c50d324bc6..
SHA256:	616255c7f069754.
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

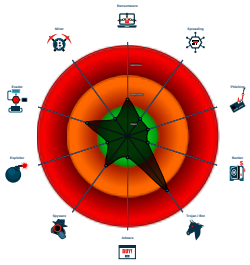


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Uses 32bit PE files
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…
- Detected potential crypto function
- Sample execution stops while proce…
- Contains functionality to call native f…
- Contains functionality to dynamically…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6364 cmdline: loaddll32.exe 'C:\Users\user\Desktop\c3.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6376 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\c3.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6396 cmdline: rundll32.exe 'C:\Users\user\Desktop\c3.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6384 cmdline: rundll32.exe C:\Users\user\Desktop\c3.dll,@Againkind@0 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6436 cmdline: rundll32.exe C:\Users\user\Desktop\c3.dll,@Consonanttime@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6456 cmdline: rundll32.exe C:\Users\user\Desktop\c3.dll,@Nooncry@4 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"iZ+yu73sQgHWIoKVZvTBVFftBRzgg84Wo8cRK1WKzlYIyRSwRES+5puIFDGj4t/PJdO/J+rFd8Puk9xQXkAk5gtRJ+EiBjQZEhIJII9S4j9MojvldfnQXG4MCZq2vijykYOVQ/oipgSqNw946zszs4wFVrWAoZclk2bk1tyqtgqxkkj0
TTwIXY2VfInsWFxD/3rDCluhcm6BGxwpQenf9WcO9HcjXScxWCVoj1xEKoz2EWs5Yz+47bMOX0XSfQdNTrhQDAWX7nAEEA6/oHUm46QdJTg5UtCf5yxbjwIgAf3SZboeJUyNSK7Q1WQQUlETGFBqUZa4n/YRWCQVzi42QoGrPxpP3LrDh
lEYnFm7fQM=",
  "c2_domain": [
    "app10.laptok.at",
    "apt.feel500.at",
    "init.in100k.at"
  ],
  "botnet": "3500",
  "server": "580",
  "serpent_key": "GfG96RIHgUj8PvPF",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000003.527385053.0000000002960000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000005.00000003.556982674.0000000002DC0000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000004.00000003.545943062.0000000004230000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000003.528290372.0000000002C00000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000000.00000002.878420774.0000000003119000.00000004.00000040.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.6f250000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.31194a0.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.3.rundll32.exe.4238d07.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.2968d07.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.3.rundll32.exe.2dc8d07.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

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

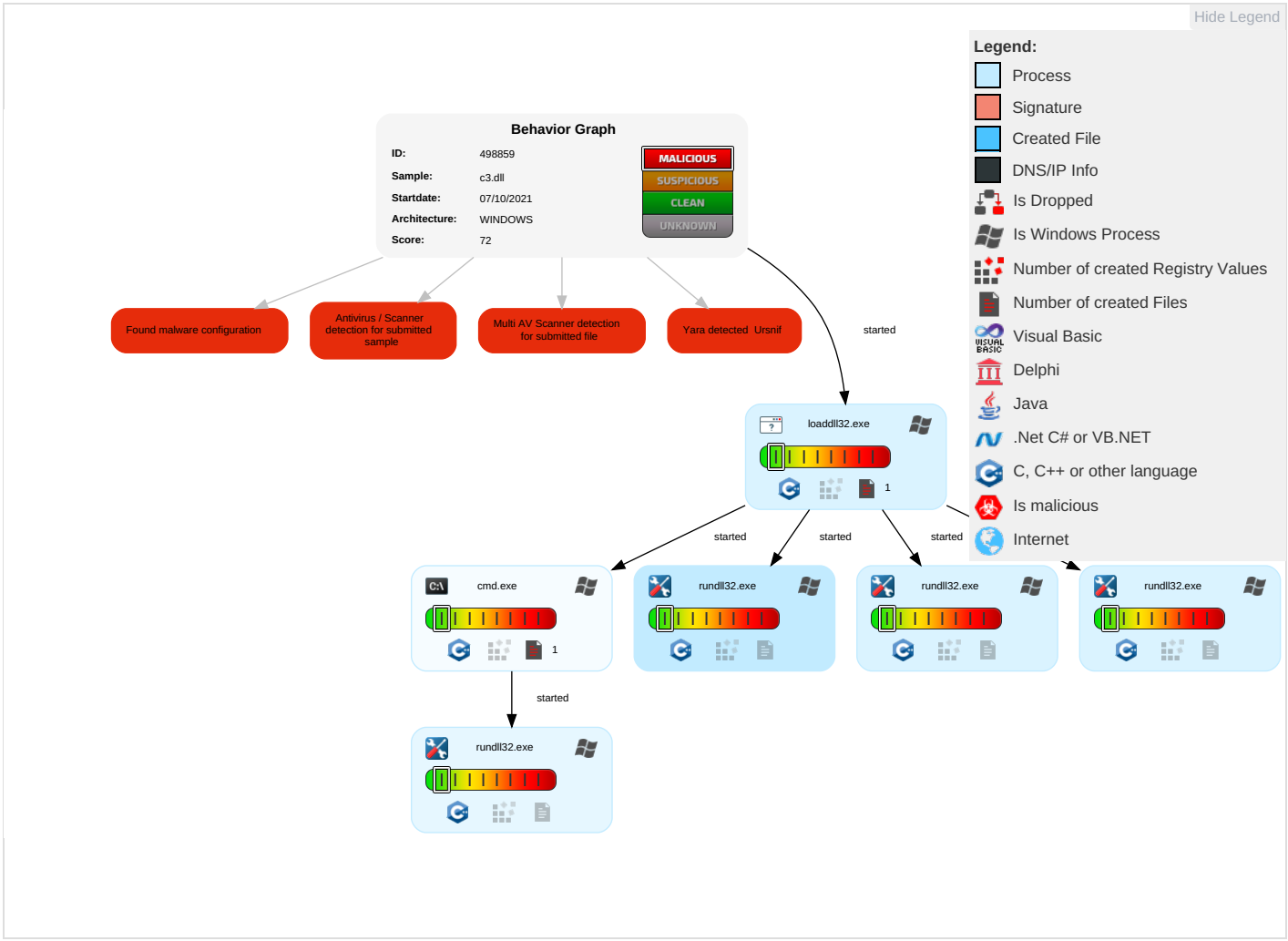
Remote Access Functionality:

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	Remote Service Effects	Imp
Valid Accounts	Native API 1	Path Interception	Process Injection 1 2	Rundll32 1	OS Credential Dumping	System Time 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	Mod Sys Par
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing 2	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Dev Loc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Del Dev Dat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Car Billi Fra

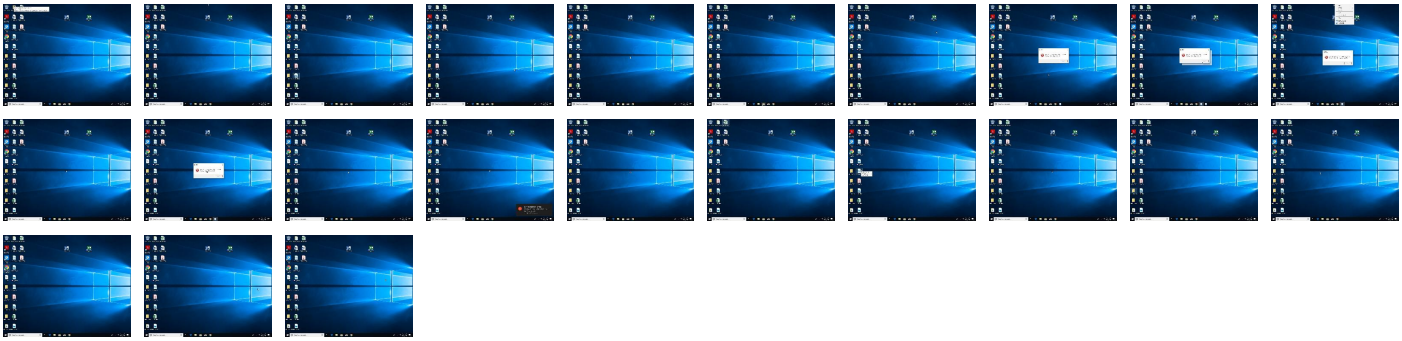
Behavior Graph



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
c3.dll	59%	Virustotal		Browse
c3.dll	11%	Metadefender		Browse
c3.dll	66%	ReversingLabs	Win32.Trojan.Wacatac	

Source	Detection	Scanner	Label	Link
c3.dll	100%	Avira	TR/AD.UrsnifDropper.mlwbg	

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:	33.0.0 White Diamond
Analysis ID:	498859
Start date:	07.10.2021
Start time:	15:53:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	c3.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:	25
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:	mal72.troj.winDLL@11/0@0/0
EGA Information:	Failed

HDC Information:	• Successful, ratio: 17.2% (good quality ratio 16.2%) • Quality average: 79.2% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 53% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32
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):	6.470808656519418
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%

General

File name:	c3.dll
File size:	188928
MD5:	c309ec3264c7bf7c771cca5703e841fe
SHA1:	2af04c50d324bc6f42fe9714ea89cf300471c169
SHA256:	616255c7f0697542e2a3e5e6b4834fffa5e56e7ede26612454674a9937d32a19
SHA512:	d8777b8436b00dbf0e6fc3c222ca63cc4b034886262a2950aed129b198280495e55c9ef107dff033f52c72109b28a90d28bd6ab362d98bb4037570f118d2f8ba
SSDEEP:	3072:qrvdO1LblP9WNrgFFxA9cHv3UgmvXIyLOM9LPm/wKrD3SzGamTdHJyrVoNXO47:qZgi8FTAuHPUl5SeTSnZuoN+4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>.p.z...z...z.....y.....k...<...j...<...j...z.....<.....<...n.....{.....{.....{...Richz.....PE..L..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1001a61
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:	0x56F56CBB [Fri Mar 25 16:52:11 2016 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:	41b0070c0a9513aca3e2dec57678f6a0

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1ccc6	0x1ce00	False	0.706642316017	data	6.80010328322	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1e000	0xcc9e	0xce00	False	0.591607251214	COM executable for DOS	5.46383270408	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2b000	0x13744	0x2400	False	0.444227430556	data	4.46433641721	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x3f000	0x114	0x200	False	0.29296875	data	1.47141497128	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x40000	0x4e8	0x600	False	0.388671875	data	3.65070908006	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x41000	0x1524	0x1600	False	0.776278409091	data	6.55572681018	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

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

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6364 Parent PID: 1228

General

Start time:	15:54:28
Start date:	07/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\c3.dll'
Imagebase:	0x390000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.878420774.0000000003119000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.560938842.0000000001080000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 6376 Parent PID: 6364

General

Start time:	15:54:29
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\c3.dll',#1
Imagebase:	0x2a0000
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: 6384 Parent PID: 6364

General

Start time:	15:54:29
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\c3.dll,@Againkind@0
Imagebase:	0x2d0000
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_1, Description: Yara detected Ursnif, Source: 00000002.00000003.527385053.0000000002960000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6396 Parent PID: 6376

General

Start time:	15:54:29
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe 'C:\Users\user\Desktop\c3.dll',#1
Imagebase:	0x2d0000
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_1, Description: Yara detected Ursnif, Source: 00000003.00000003.528290372.0000000002C00000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6436 Parent PID: 6364

General

Start time:	15:54:34
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\c3.dll,@Consonanttime@8
Imagebase:	0x2d0000
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_1, Description: Yara detected Ursnif, Source: 00000004.00000003.545943062.0000000004230000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 6456 Parent PID: 6364

General

Start time:	15:54:40
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\c3.dll,@Nooncry@4
Imagebase:	0x2d0000
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_1, Description: Yara detected Ursnif, Source: 00000005.00000003.556982674.0000000002DC0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Disassembly

Code Analysis

Code Analysis