



ID: 632396
Sample Name: 5300000.dll
Cookbook: default.jbs
Time: 16:40:38
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 5300000.dll 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Threatname: Ursnif 3
Yara Signatures 3
Initial Sample 4
Sigma Signatures 4
Snort Signatures 4
Joe Sandbox Signatures 4
AV Detection 4
Key, Mouse, Clipboard, Microphone and Screen Capturing 4
E-Banking Fraud 4
Hooking and other Techniques for Hiding and Protection 4
Stealing of Sensitive Information 4
Remote Access Functionality 4
Mitre Att&ck Matrix 4
Behavior Graph 5
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 7
Contacted Domains 7
World Map of Contacted IPs 7
General Information 7
Warnings 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASNs 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
Static File Info 8
General 8
File Icon 9
Static PE Info 9
General 9
Entrypoint Preview 9
Rich Headers 11
Data Directories 11
Sections 11
Network Behavior 11
Statistics 12
Behavior 12
System Behavior 12
Analysis Process: loaddll32.exePID: 6412, Parent PID: 4468 12
General 12
File Activities 12
Analysis Process: cmd.exePID: 6420, Parent PID: 6412 12
General 12
File Activities 13
Analysis Process: rundll32.exePID: 6448, Parent PID: 6420 13
General 13
File Activities 13
Disassembly 13

Copyright Joe Security LLC 2022

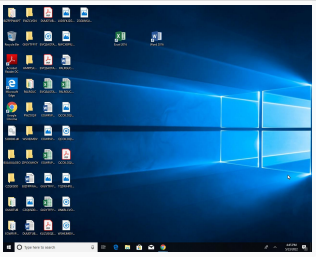
Windows Analysis Report

5300000.dll

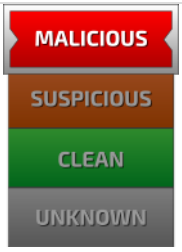
Overview

General Information

Sample Name:	5300000.dll
Analysis ID:	632396
MD5:	67f12b772561c1..
SHA1:	39a3c933a2fe4e..
SHA256:	9af5351d4a0384..
Tags:	dll
Infos:	



Detection



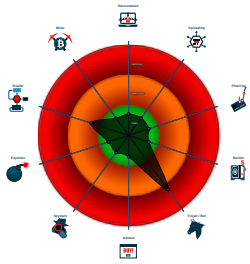
Ursnif

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
- PE file does not import any functions
- Tries to load missing DLLs
- Program does not show much activi…
- Creates a process in suspended mo…
- Checks if the current process is bei…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6412 cmdline: loaddll32.exe "C:\Users\user\Desktop\5300000.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6420 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\5300000.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6448 cmdline: rundll32.exe "C:\Users\user\Desktop\5300000.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"aVn5cc4yxmeeaLO1GhSDa9E9i9AhiobBqld00ioGlWOx7yX95FcGN3HicG7Ma8K4OSypooZMeS/Q9RHBbebiZB0htVqQfpLIdb7MhjDHDEBHCtTQeeoA8LfDaJAEQ2IdhSWjXZZqcMncDfNRXuwiAWQdEo+PTa9HSuW2G4AqVIhs9hBL
2BAZZa8Egh74wCmZjW5gvEmkB+aIKoafUXWf9rJ70sGHrX3U1JPn9tSGnbML+e9g5HE/xe2QT/jXivxkLmTVQv5cQZbQWCQmVvKyQzH4ZmE8FDdAahhD8LLQyis0qatiz93QdIa9WeAg8/W3ijW7qgygdKBu/PDPFWkBFjL9Ourt+q4fq
ApYM+hMcvc=",
  "c2_domain": [
    "agenziaent.top",
    "agenziaentr.top",
    "statusline.ru",
    "statuslines.ru"
  ],
  "botnet": "7631",
  "server": "50",
  "serpent_key": "xlmWrvhFyvbUdepr",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
5300000.dll	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

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

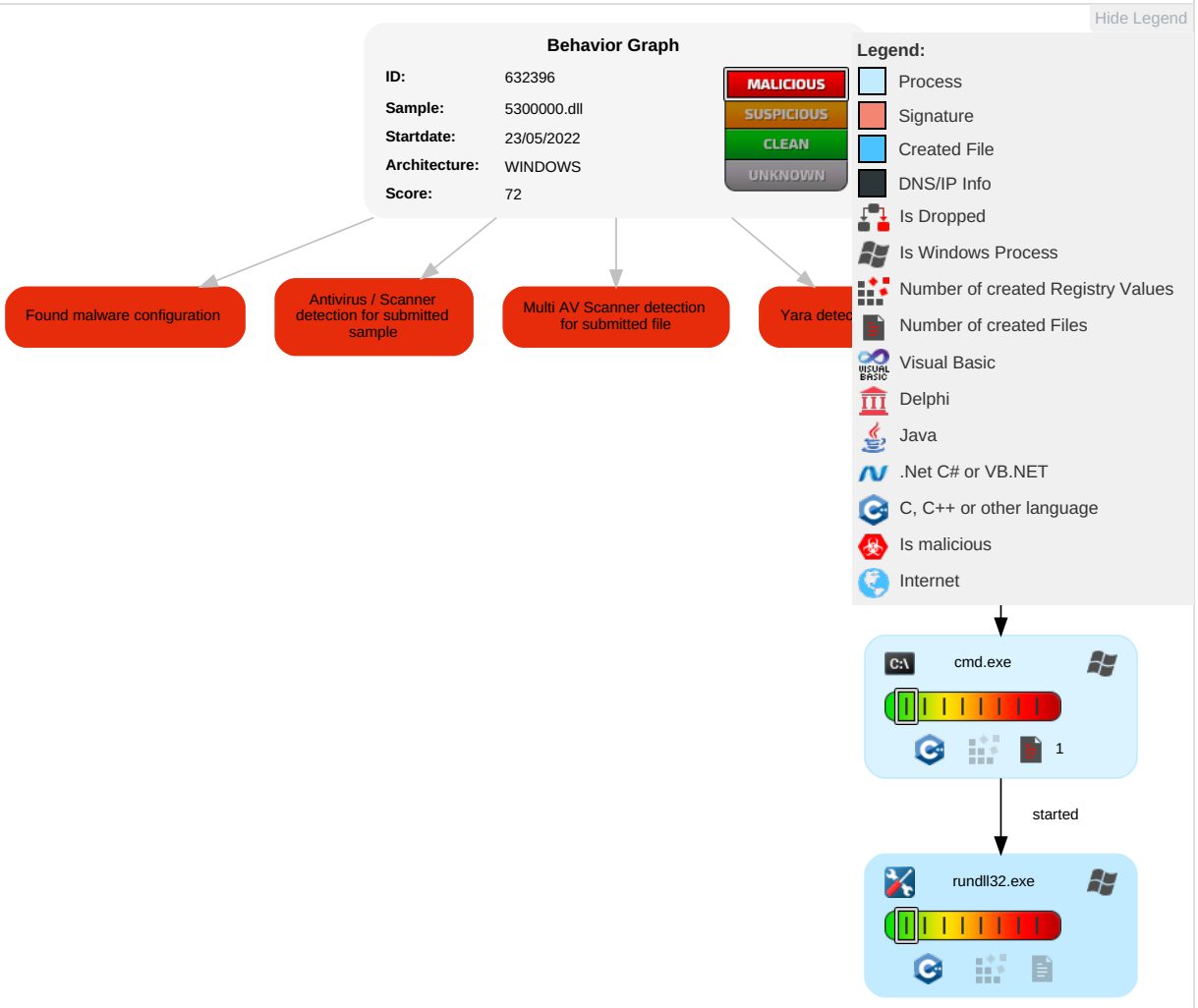
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 1 Process Injection	1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Rundll32	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 DLL Side-Loading	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Behavior Graph

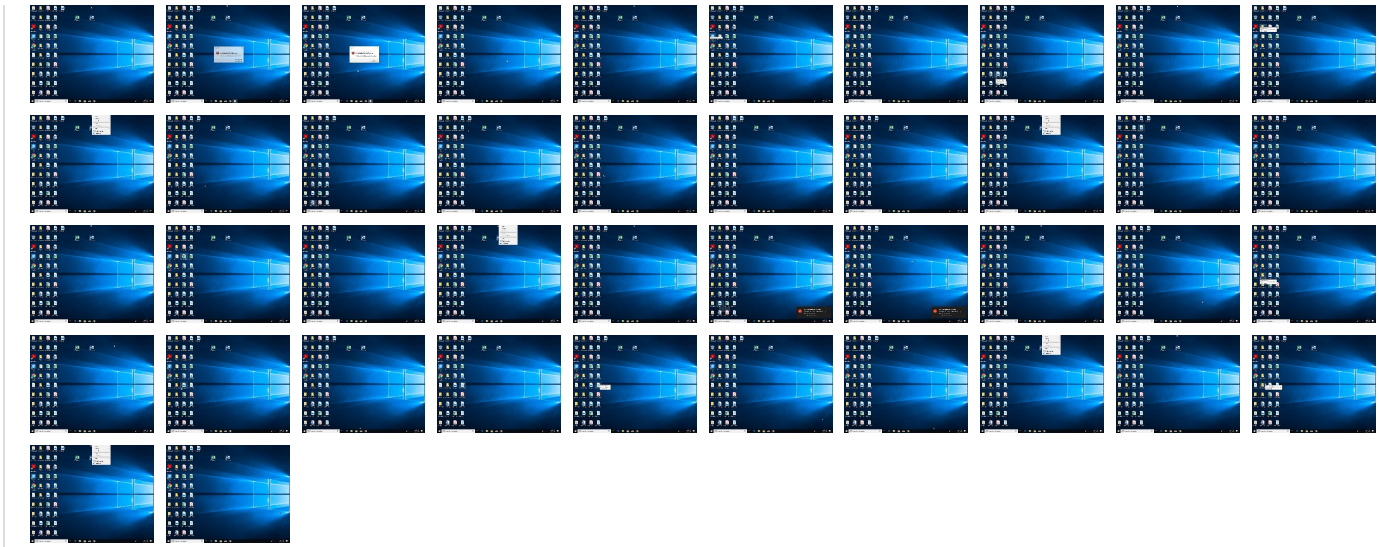


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Copyright Joe Security LLC 2022





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
5300000.dll	51%	ReversingLabs	Win32.Trojan.Razy	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
5300000.dll	100%	Avira	HEUR/AGEN.1245293	

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

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632396
Start date and time: 23/05/202216:40:38	2022-05-23 16:40:38 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5300000.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:	28
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@5/0@0/0
EGA Information:	Failed
HDC Information:	Failed

Copyright Joe Security LLC 2022

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: 5300000.dll

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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):	6.648453671897272

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:	5300000.dll
File size:	44544
MD5:	67f12b772561c13041ada1de17bff6c1
SHA1:	39a3c933a2fe4e0d373da3bbf556c4a58d051732
SHA256:	9af5351d4a0384db5af18c90007cc7aacd856b701c6a8d8da49bdaa4e9c2a3a7
SHA512:	75dd963ff30de23e581a2eb6fecf90d69111d613960e48c9508c756dfca2374280145cbb6f9f1ea840e433b39ecd5bd538dcf3e36489037ec59a349841b037a8
SSDEEP:	768:65pad4LOyeTJRRtpg6DBpLuS7rmWucAh1gRhOEOQJMkhe0gspoEs/P:Mpapy6JRRY6D3LPrM0RhOEJJMk1VjaP
TLSH:	38138D02F6F90CF2D3A39E746610FBF867FA863112786094E72399CA59A4953E53D307
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p.....i.....i.....H...:.....:.....:.....i.....i.....i.....Rich.....PE..L.....b...

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1000586c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x6213BE96 [Mon Feb 21 16:32:22 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Instruction
mov eax, dword ptr [esp+08h]
push esi
xor esi, esi
inc esi
sub eax, 00000000h
je 00007F80909BEA45h
dec eax
jne 00007F80909BEA56h
push 1000A2DCh
call dword ptr [1000900Ch]
cmp eax, esi
jne 00007F80909BEA47h
push dword ptr [esp+08h]
call 00007F80909BE9A4h
test eax, eax
je 00007F80909BEA3Ah
xor esi, esi

Instruction
jmp 00007F80909BEA36h
push 1000A2DCh
call dword ptr [10009010h]
test eax, eax
jne 00007F80909BEA27h
call 00007F80909BB267h
mov eax, esi
pop esi
retn 000Ch
push ebp
mov ebp, esp
push ecx
xor eax, eax
inc eax
cmp dword ptr [ebp+08h], 00000000h
mov dword ptr [ebp-04h], eax
je 00007F80909BEA35h
push eax
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007F80909BDD23h
test eax, eax
je 00007F80909BEA3Ah
push 00000004h
lea eax, dword ptr [ebp-04h]
push eax
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push 00000004h
push 80000001h
call 00007F80909BE18Bh
leave
retn 000Ch
push ebp
mov ebp, esp
sub esp, 58h
push ebx
push esi
push edi
mov esi, eax
xor eax, eax
mov word ptr [ebp-44h], ax
lea edi, dword ptr [ebp-42h]
stosd
stosd
stosd
stosw
xor eax, eax
mov word ptr [ebp-34h], ax
lea edi, dword ptr [ebp-32h]
stosd
stosd
stosd
stosw
xor eax, eax
mov word ptr [ebp-24h], ax
lea edi, dword ptr [ebp-22h]
stosd

Copyright Joe Security LLC 2022

Instruction
stosd
push 00000008h
pop ebx
push dword ptr [ebp+08h]
stosd
stosw
call dword ptr [000090D0h]

Rich Headers

Programming Language:	• [ASM] VS2008 SP1 build 30729 • [LNK] VS2008 SP1 build 30729 • [C++] VS2005 build 50727 • [IMP] VS2008 SP1 build 30729 • [EXP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x9f10	0x32	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x98d4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc000	0x744	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x9000	0x12c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x92a4	0xe0	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

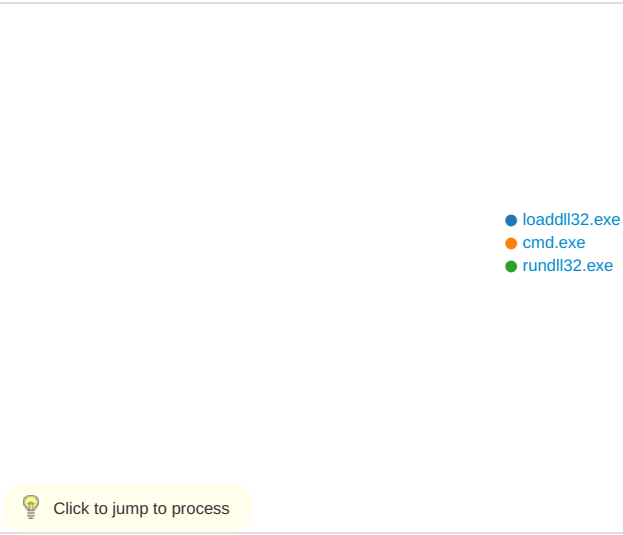
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x7663	0x7800	False	0.621875	data	6.52907311562	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x9000	0xf42	0x1000	False	0.4609375	data	4.70307546866	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x3e8	0x200	False	0.572265625	ARJ archive data, v29, original name: , os: MS-DOS	3.67785998014	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0xb000	0xeae	0x1000	False	0.901123046875	data	7.52389912782	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xc000	0x1000	0x1000	False	0.610107421875	data	5.4947263917	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6412, Parent PID: 4468

General

Target ID:	0
Start time:	16:41:49
Start date:	23/05/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\5300000.dll"
Imagebase:	0x840000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6420, Parent PID: 6412

General

Target ID:	1
Start time:	16:41:50
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\5300000.dll",#1
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D

Copyright Joe Security LLC 2022

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **6448**, Parent PID: **6420**

General

Target ID:	2
Start time:	16:41:50
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\5300000.dll",#1
Imagebase:	0x100000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly