ID: 556768
Sample Name: 24ff7d60000.dll
Cookbook: default.jbs
Time: 12:51:22
Date: 20/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

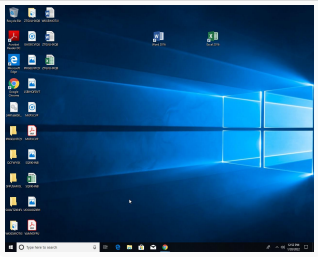
Windows Analysis Report

24ff7d60000.dll

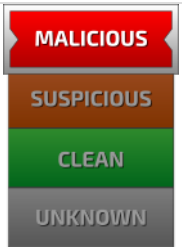
Overview

General Information

Sample Name:	24ff7d60000.dll
Analysis ID:	556768
MD5:	7dfb20c4318a10..
SHA1:	e85b218a1ee6ec..
SHA256:	f8090b2dea0188..
Tags:	exe Gozi
Infos:	YARA SIGMA



Detection



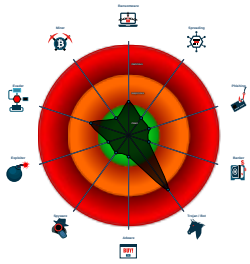
Ursnif

Score:	76
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
- Sigma detected: Suspicious Call by…
- 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**
- loaddll64.exe (PID: 7028 cmdline: loaddll64.exe "C:\Users\user\Desktop\24ff7d60000.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 7036 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\24ff7d60000.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 7056 cmdline: rundll32.exe "C:\Users\user\Desktop\24ff7d60000.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7044 cmdline: rundll32.exe C:\Users\user\Desktop\24ff7d60000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"1ez6ZX9GBMHuzrxYcEvmkX0k1/y/WRE5hgthXVQ4P44VmZDRyl+qzgB3X8mQxx9hX87voxwb+7CbnJcCZ4hp/XwNIs0rUcJj4wwNctiIvZb8gIPsgWrAjjXLGMBCWjpmhIdWmYD7oSqxAb7ciAuhtWabiveV3OFwUuMRDbNtONTWpz/J
4JVtQJ3XBbp99SutX5vbOPhgKBI3aszrv+0c1EkjrakCFHlOqMs8bjEjNDxrhaBWjOM1EU17zvHVkK7hxDkKQ5buzWmjrzDZEEWnvM3aa5uVRR1v44XnbolU0ltUakCZT4sH963oonk1uijxExj7eWoI4x+donYvsc/nFxNyfe6c/mfSK
b7U2RhPG4g=",
  "c2_domain": [
    "art.microsoftsofymicrosoftsoft.at",
    "r23cirt55ysvtdvl.onion",
    "poi.redhatbabby.at",
    "fgx.dangerboy.at",
    "pop.biopiof.at",
    "l46t3vgvmtx5wxe6.onion",
    "apr.intoolkom.at"
  ],
  "ip_check_url": [
    "curlmyip.net"
  ],
  "serpent_key": "KCVH9K5GZjoxwK5f",
  "server": "580",
  "sleep_time": "10",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "600",
  "time_value": "600",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "300",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "505050",
  "SetWaitableTimer_value": "60"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
24ff7d60000.dll	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	

Sigma Overview

System Summary

Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

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

System Summary

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Stealing of Sensitive Information

Yara detected Ursnif

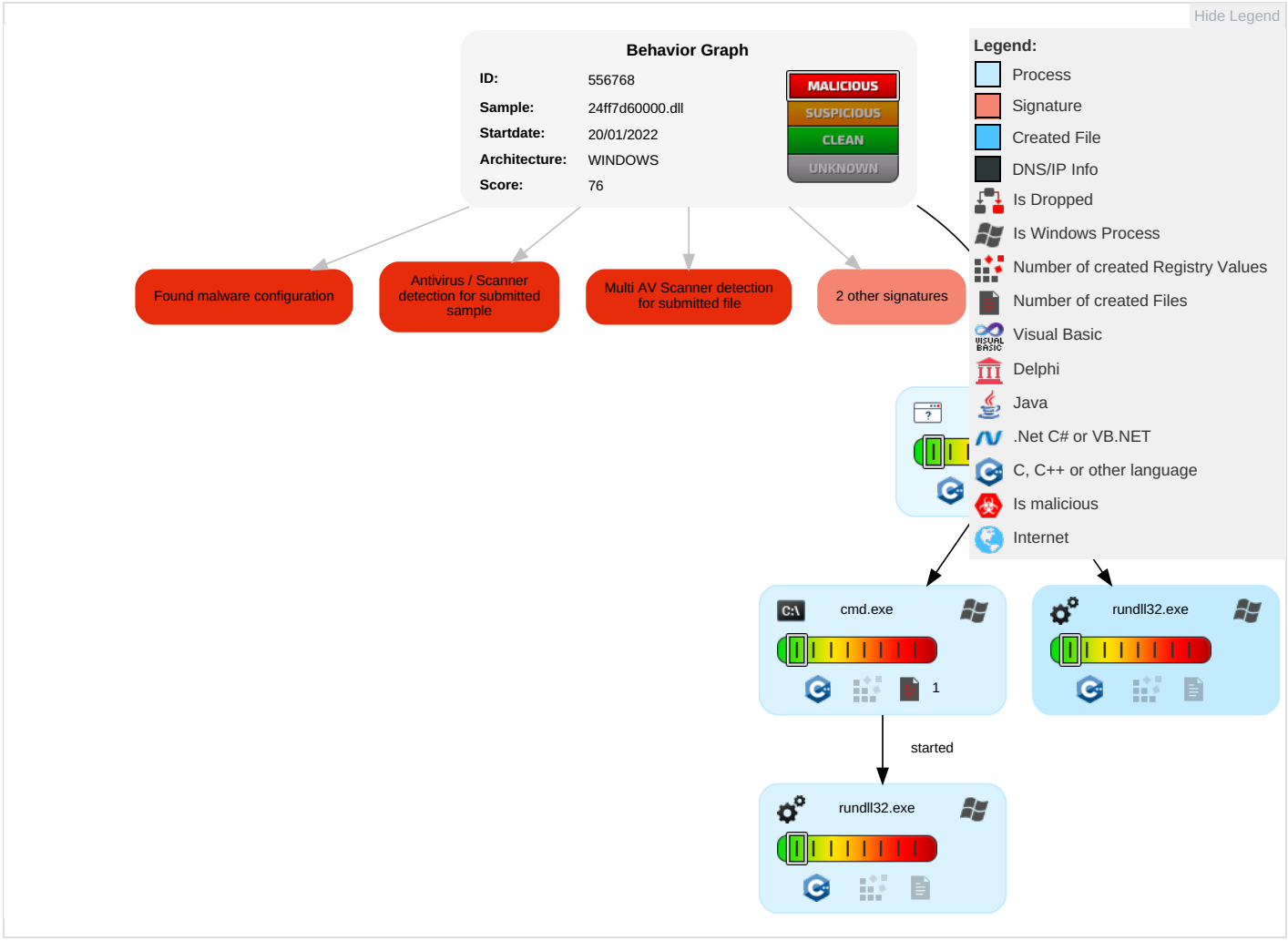
Remote Access Functionality

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
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.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
24ff7d60000.dll	42%	ReversingLabs	Win64.Trojan.Ursnif	
24ff7d60000.dll	100%	Avira	HEUR/AGEN.1212258	

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:	556768
Start date:	20.01.2022
Start time:	12:51:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	24ff7d60000.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:	8
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:	mal76.troj.winDLL@7/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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 • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 20.82.209.183
- Excluded domains from analysis (whitelisted): www.bing.com, dual-a-0001.dc-msedge.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

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:	MS-DOS executable
Entropy (8bit):	6.442221882725178
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 84.88% • Win64 Executable (generic) (12005/4) 9.99% • DOS Executable Borland Pascal 7.0x (2037/25) 1.69% • Generic Win/DOS Executable (2004/3) 1.67% • DOS Executable Generic (2002/1) 1.67%
File name:	24ff7d60000.dll
File size:	248320
MD5:	7dfb20c4318a1045a3745e8ca507ce78
SHA1:	e85b218a1ee6ec3be0ec69eaccd62671766561ea
SHA256:	f8090b2dea01886cdf4b8c69e924e6f92717d3d19e1927aba61fda5b5b80898a
SHA512:	23b74d28a190c14be5a5164b92ca43d8a98a09925edbdd6e6810fc580e87af03598426a5a25e78c73d5e0dff54f0eddb79b4bd5f1f9e3777236e2cf49200c051
SSDEEP:	6144:HPMtglXNWOg0SbrhI8exPofnrWWJE4RX:HP1hI02rO8exgvrWWJh
File Content Preview:	MZ.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x18000527c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	
Time Stamp:	0x61B67F6F [Sun Dec 12 23:02:07 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:	

Entrypoint Preview

Instruction
inc eax
push ebx
dec eax
sub esp, 20h
test edx, edx
mov ebx, 00000001h
je 00007FB72471DDB6h
cmp edx, ebx
jne 00007FB72471DDC1h
mov eax, ebx
lock xadd dword ptr [00034717h], eax
add eax, ebx
cmp eax, ebx
jne 00007FB72471DDB1h
dec ecx
mov edx, eax
call 00007FB724738D16h
test eax, eax
je 00007FB72471DDA5h
xor ebx, ebx
jmp 00007FB72471DDA1h
lock add dword ptr [000346F9h], FFFFFFFFh
jne 00007FB72471DD97h
call 00007FB72471F97Fh
mov eax, ebx
dec eax
add esp, 20h
pop ebx
ret
int3
int3
dec eax
mov dword ptr [esp+08h], ebx
push edi
dec eax
sub esp, 60h
lock add dword ptr [000348CAh], 01h

Instruction
inc esp
mov edx, dword ptr [esp+000000A0h]
mov eax, dword ptr [000348ECh]
inc ecx
or edx, 04h
cmp al, 06h
jnbe 00007FB72471DDF6h
jne 00007FB72471DD9Bh
cmp byte ptr [000348DCh], 00000000h
jnbe 00007FB72471DDEBh
dec eax
mov eax, dword ptr [esp+000000B8h]
dec eax
mov edi, dword ptr [esp+000000C0h]
dec eax
mov dword ptr [esp+50h], edi
dec eax
mov dword ptr [esp+48h], eax
dec eax
mov eax, dword ptr [esp+000000B0h]
dec eax
mov dword ptr [esp+40h], eax
dec eax
mov eax, dword ptr [esp+000000A8h]
dec eax
mov dword ptr [esp+38h], eax
mov eax, dword ptr [esp+00000098h]
inc esp
mov dword ptr [esp+30h], edx
mov dword ptr [esp+28h], eax
dec eax
mov eax, dword ptr [esp+00000090h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x37800	0x37	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x367f8	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x3a000	0x18f0	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3e000	0x32c	.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	0x31000	0x4f0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x34e9c	0x1e0	.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	0x2fdec	0x2fe00	False	0.579277496736	zlib compressed data	6.39992554242	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x31000	0x6837	0x6a00	False	0.372346698113	data	5.26021941188	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

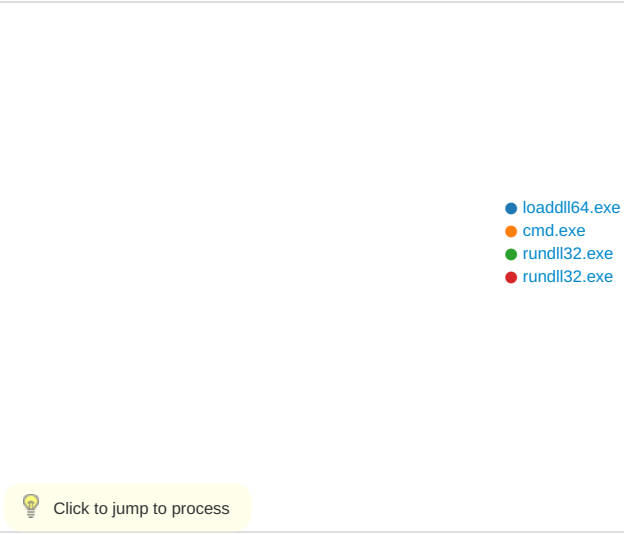
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x38000	0x1e40	0x1800	False	0.31640625	lif file	3.696189142	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x3a000	0x18f0	0x1a00	False	0.528094951923	data	5.32861522181	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x3c000	0x1f80	0x2000	False	0.970458984375	data	7.90682667928	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x3e000	0x1000	0xc00	False	0.513346354167	data	4.74473762141	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **7028**, Parent PID: **5096**

General

Start time:	12:52:21
Start date:	20/01/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\24ff7d60000.dll"
Imagebase:	0x7ff6aeda0000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	moderate

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: 7036, Parent PID: 7028

General

Start time:	12:52:21
Start date:	20/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\24ff7d60000.dll",#1
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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: 7044, Parent PID: 7028

General

Start time:	12:52:21
Start date:	20/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\24ff7d60000.dll,#1
Imagebase:	0x7ff779fd0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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

Analysis Process: rundll32.exe PID: 7056, Parent PID: 7036

General

Start time:	12:52:22
Start date:	20/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false

Commandline:	rundll32.exe "C:\Users\user\Desktop\24ff7d60000.dll",#1
Imagebase:	0x7ff779fd0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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