ID: 725156
Sample Name: d610000.dll.exe
Cookbook: default.jbs
Time: 10:00:16
Date: 18/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

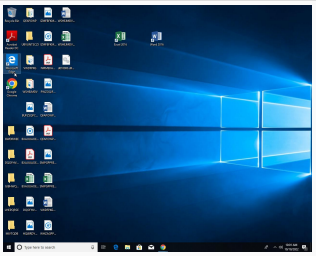
Windows Analysis Report

d610000.dll.exe

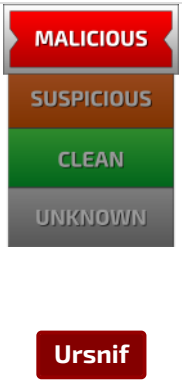
Overview

General Information

Sample Name:	d610000.dll.exe (renamed file extension from exe to dll)
Analysis ID:	725156
MD5:	c5280e5552a8fb..
SHA1:	8ea200f303f42df..
SHA256:	f9641b26c887ef0..
Tags:	exe gozi
Infos:	YARA



Detection



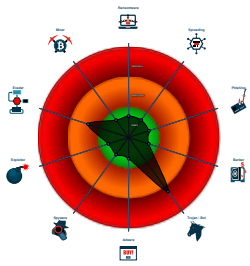
Ursnif

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

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Ursnif
- Sample execution stops while proce…
- 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: 5052 cmdline: loaddll64.exe "C:\Users\user\Desktop\d610000.dll.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 4952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5932 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\d610000.dll.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5944 cmdline: rundll32.exe "C:\Users\user\Desktop\d610000.dll.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5784 cmdline: rundll32.exe C:\Users\user\Desktop\d610000.dll.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"GE4Kf3pbrel1zpiOoLCHqOkVEoQCjXZcwDJgnKKashzu0ThAOIAJ/NQb3zKPQODOcEFRZfugbCviR+t+viu5jwjNVxTXEO+9Oq9MXvnhL3atJQPuJlCCvGC4jxqOl1+k9/pwik62mMuWd8AoXgZ/WmjcnNaQRQszlbtuRbQoHZr3ItTr
Vv9BHP0eOyDB8QSDHjb8UnRBZMZZaqAL2uRE2sPmEgdRIm6Wuju2n1FVZtl1kxpF/++L23MifEqV2vCG4veI+iRsyoDo+5dNzy/SoNvG0JmlelPoFeRD0XGBrM85vXLHSpsv4AWDYzOs7NLBs/ynxrCVGuIVfCRpyyhS7Zc5Z5ky0QHC4
pY+36zr4yQ=",
  "c2_domain": [
    "trackingg-protectioon.cdn1.mozilla.net",
    "siwdmfkshsgw.com",
    "trackingg-protectioon.cdn1.mozilla.net",
    "188.127.224.114",
    "weiqeqwns.com",
    "weiqeqwens.com",
    "weiqewqwns.com",
    "iujdhsndjfks.com",
    "ijduwhsbvk.com"
  ],
  "ip_check_url": [
    "http://ipinfo.io/ip",
    "http://curlmyip.net"
  ],
  "serpent_key": "YFVenkBsAbUmuHYi",
  "tor32_dll": "file://c:\\test\\test32.dll",
  "tor64_dll": "file://c:\\test\\tor64.dll",
  "movie_capture": "30, 8, *terminal* *wallet* *bank* *banco*",
  "server": "50",
  "sleep_time": "1",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "60",
  "time_value": "60",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "60",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "60",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "10103",
  "SetWaitableTimer_value": "1"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
d610000.dll.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

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

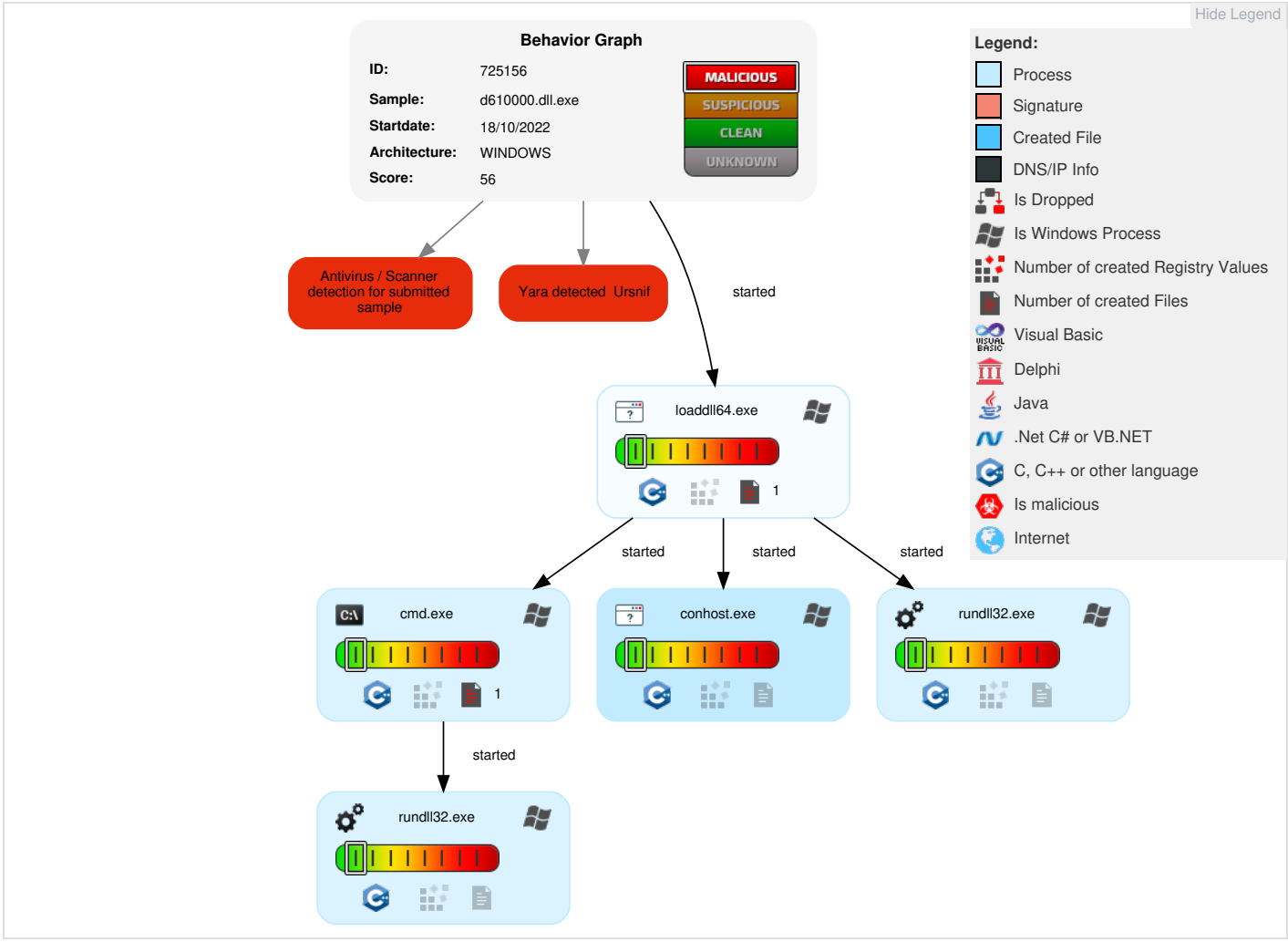
Remote Access Functionality

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
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

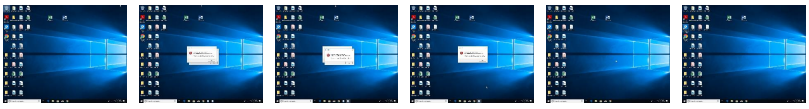
Behavior Graph



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
d610000.dll.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:	36.0.0 Rainbow Opal
Analysis ID:	725156
Start date and time:	2022-10-18 10:00:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	d610000.dll.exe (renamed file extension from exe to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
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@8/0@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:	• Stop behavior analysis, all processes terminated

Warnings

- Excluded domains from analysis (whitelisted): fs.microsoft.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 PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.42546882759388
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 84.94% • Win64 Executable (generic) (12005/4) 10.00% • DOS Executable Borland Pascal 7.0x (2037/25) 1.70% • Generic Win/DOS Executable (2004/3) 1.67% • DOS Executable Generic (2002/1) 1.67%
File name:	d610000.dll.dll
File size:	232960
MD5:	c5280e5552a8fb5066f56616df777bcc
SHA1:	8ea200f303f42df4e6a18286bd92c18c1c61a92e
SHA256:	f9641b26c887ef0abd66f0e0b614b6599b339b424c671bd83dddb2e59d91bbb1
SHA512:	2a533b45452b3fd6f8be4f1deae9fa537b1762b6511d12d0502f0c7d7678a56d291b813b9d15ee32dee7cf6af775d33bfb9132ad8a7f73b39a3745fa8914ddce
SSDEEP:	3072:rlfGqwJTeTEom3IlkR2SCD6q9KgyItk78mV0dfgxT/cqAYw5VgCK5hcjkyxJFoc:rlDosEPR66q9KgyIlnd6oqAYD5SnFoc
TLSH:	97346E6AA3E50995ED6BD5B5C953D217EBF334092B64C30F53B0CAA66F17722B21C302
File Content Preview:	MZ.....PE..d.....%c...

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x18000ada0
Entrypoint Section:	.text
Digitally signed:	false

Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	
Time Stamp:	0x632596F2 [Sat Sep 17 09:44:18 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	

Entrypoint Preview

Instruction
inc eax
push ebx
dec eax
sub esp, 20h
mov ebx, 00000001h
test edx, edx
je 00007FE6E0D9A4F6h
cmp edx, ebx
jne 00007FE6E0D9A501h
mov eax, ebx
lock xadd dword ptr [0002ACB3h], eax
add eax, ebx
cmp eax, ebx
jne 00007FE6E0D9A4F1h
dec ecx
mov edx, eax
call 00007FE6E0DACDFAh
test eax, eax
je 00007FE6E0D9A4E5h
xor ebx, ebx
jmp 00007FE6E0D9A4E1h
lock add dword ptr [0002AC95h], FFFFFFFFh
jne 00007FE6E0D9A4D7h
call 00007FE6E0DA7F27h
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, 20h
dec eax
mov ebx, ecx
dec eax
mov ecx, dword ptr [ecx+08h]
call dword ptr [ebx]
dec eax
lea edx, dword ptr [ebx+10h]

Instruction
cmp byte ptr [edx], 00000000h
mov edi, eax
je 00007FE6E0D9A4EBh
dec eax
mov ecx, dword ptr [0002AE4Fh]
dec eax
lea eax, dword ptr [0002F01Bh]
inc esp
mov eax, edi
dec eax
add ecx, eax
call 00007FE6E0D9A54Ah
dec eax
mov ecx, dword ptr [0002AC3Eh]
dec esp
mov eax, ebx
xor edx, edx
call dword ptr [00023263h]
lock add dword ptr [0002AE03h], FFFFFFFFh
mov ecx, edi
call dword ptr [00023263h]
int3
int3
int3
inc esp
mov ebx, ecx
xor eax, eax
inc ebp
xor ecx, ecx
inc esp
xor ebx, dword ptr [0002AE01h]
dec esp
mov edx, edx
dec eax
test edx, edx
je 00007FE6E0D9A509h
dec esp
lea eax, dword ptr [edx+10h]
inc ebp
cmp ecx, dword ptr [edx]
jnc 00007FE6E0D9A500h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x337e0	0x36	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x32738	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x37000	0x18d8	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3c000	0x340	.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	0x2e000	0x520	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x309ac	0x1e0	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2cc32	0x2ce00	False	0.5784133443593314	data	6.355705596590523	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x2e000	0x5816	0x5a00	False	0.36796875	data	5.2743155509814015	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x34000	0x2040	0x1a00	False	0.3288762019230769	lif file "", version 0, LIF identifier 0, directory start address 0 length 0	3.978657207829179	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x37000	0x18d8	0x1a00	False	0.5178786057692307	data	5.20244289599206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x39000	0x2020	0x2200	False	0.9345128676470589	data	7.791653023995373	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x3c000	0x1000	0xc00	False	0.5865885416666666	data	5.354640768558997	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Statistics

Behavior

System Behavior

Analysis Process: loaddll64.exe PID: 5052, Parent PID: 3452

General

Target ID:	0
Start time:	10:01:12

Start date:	18/10/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\d610000.dll.dll"
Imagebase:	0x7ff67dee0000
File size:	139776 bytes
MD5 hash:	C676FC0263EDD17D4CE7D644B8F3FCD6
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: conhost.exe PID: 4952, Parent PID: 5052

General

Target ID:	1
Start time:	10:01:12
Start date:	18/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: 5932, Parent PID: 5052

General

Target ID:	2
Start time:	10:01:13
Start date:	18/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\d610000.dll.dll",#1
Imagebase:	0x7ff707bb0000
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: **5784**, Parent PID: **5052**

General

Target ID:	3
Start time:	10:01:13
Start date:	18/10/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\d610000.dll.dll,#1
Imagebase:	0x7ff6b5800000
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: **5944**, Parent PID: **5932**

General

Target ID:	4
Start time:	10:01:13
Start date:	18/10/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\d610000.dll.dll",#1
Imagebase:	0x7ff6b5800000
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