



ID: 403761
Sample Name: 206bfb50000.dll
Cookbook: default.jbs
Time: 11:44:34
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report 206bfb50000.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
Hooking and other Techniques for Hiding and Protection: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
File Icon 10
Static PE Info 10
General 10
Entrypoint Preview 10
Data Directories 12
Sections 12
Network Behavior 12
Code Manipulations 12
Statistics 12
Behavior 12

Copyright Joe Security LLC 2021

System Behavior 13
Analysis Process: loaddll64.exe PID: 4992 Parent PID: 5700 13
General 13
File Activities 13
Analysis Process: cmd.exe PID: 204 Parent PID: 4992 13
General 13
File Activities 14
Analysis Process: rundll32.exe PID: 4896 Parent PID: 4992 14
General 14
File Activities 14
Analysis Process: rundll32.exe PID: 5412 Parent PID: 204 14
General 14
File Activities 14
Disassembly 14
Code Analysis 14

Copyright Joe Security LLC 2021

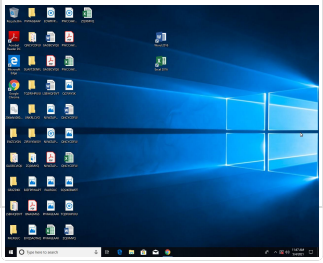
Analysis Report 206bfb50000.dll

Overview

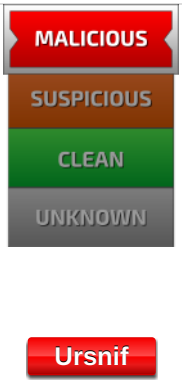
General Information

Sample Name:	206bfb50000.dll
Analysis ID:	403761
MD5:	34f21bceaca8327..
SHA1:	c2d38256cd16f2d..
SHA256:	f2b3f79ade40513..
Tags:	Gozi
Infos:	

Most interesting Screenshot:



Detection

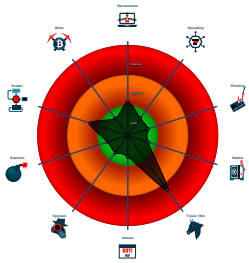


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Machine Learning detection for samp…
- Checks if the current process is bein…
- Creates a process in suspended mo…
- PE file does not import any functions
- Program does not show much activi…
- Tries to load missing DLLs

Classification



Startup

- **System is w10x64**
- loaddll64.exe (PID: 4992 cmdline: loaddll64.exe 'C:\Users\user\Desktop\206bfb50000.dll' MD5: A84133CCB118CF35D49A423CD836D0EF)
  - cmd.exe (PID: 204 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\206bfb50000.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5412 cmdline: rundll32.exe 'C:\Users\user\Desktop\206bfb50000.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4896 cmdline: rundll32.exe C:\Users\user\Desktop\206bfb50000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

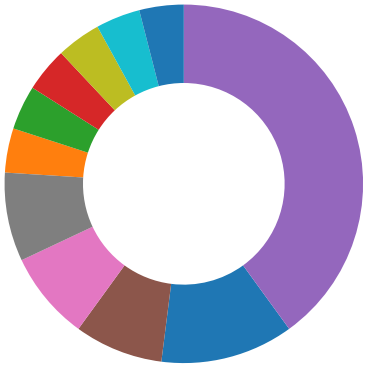
Source	Rule	Description	Author	Strings
206bfb50000.dll	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



- AV Detection
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for 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

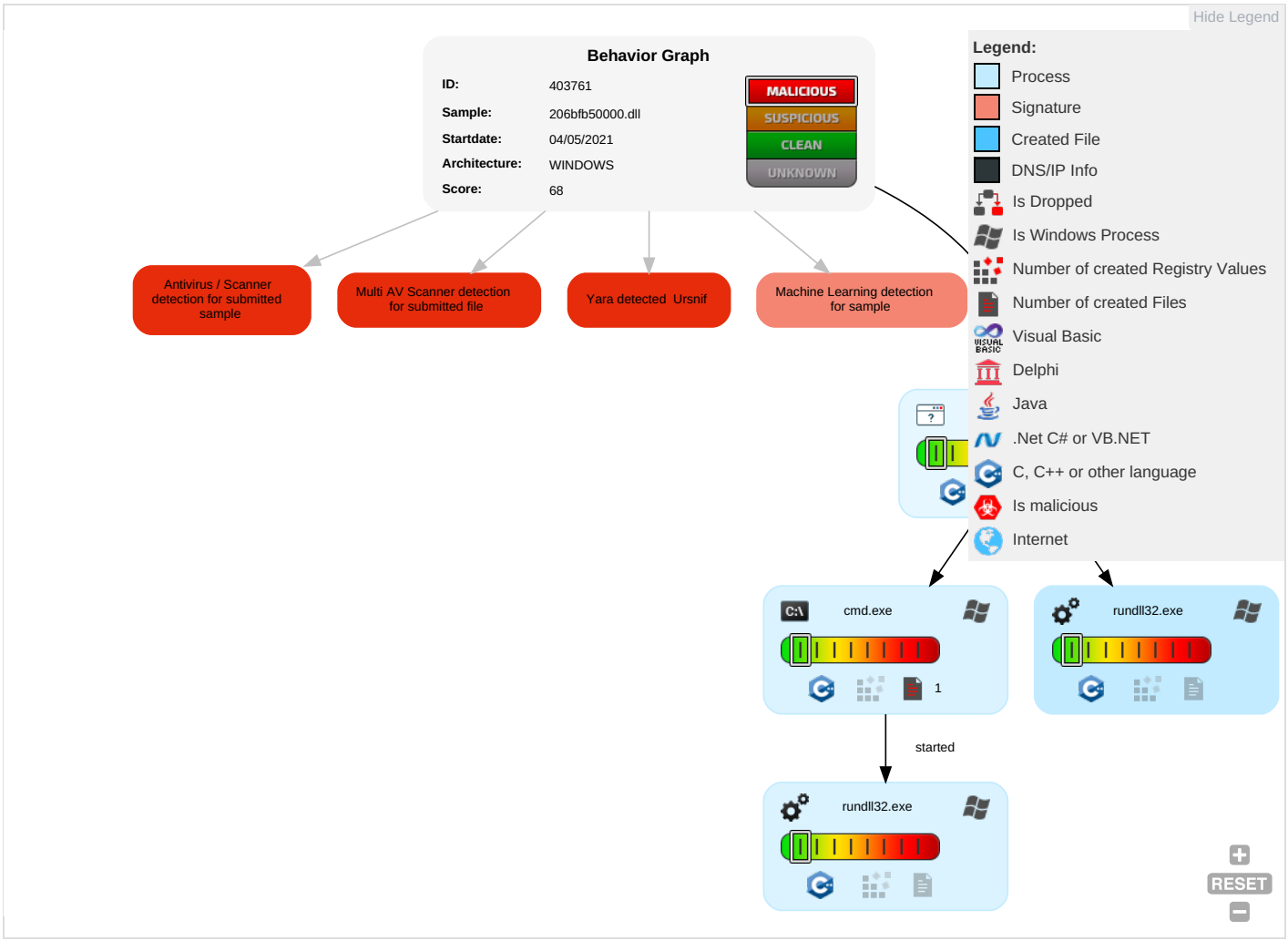
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Rundll32 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Network Configuration Discovery	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
206bfb50000.dll	30%	ReversingLabs	Win64.Infostealer.Convagent	
206bfb50000.dll	100%	Avira	HEUR/AGEN.1108168	
206bfb50000.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://file://USER.ID%lu.exe/upd	206bfb50000.dll	false	• Avira URL Cloud: safe	low
http://constitution.org/usdeclar.txt	206bfb50000.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://constitution.org/usdeclar.txtC:	206bfb50000.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403761
Start date:	04.05.2021
Start time:	11:44:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	206bfb50000.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:	34
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:	mal68.troj.winDLL@7/0@0/0
EGA Information:	Failed
HDC Information:	Failed

Copyright Joe Security LLC 2021

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
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • VT rate limit hit for: /opt/package/joesandbox/database/analysis/403761/sample/206bfb50000.dll

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:	MS-DOS executable
Entropy (8bit):	6.331080654014987

General

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:	206bfb50000.dll
File size:	223744
MD5:	34f21bceaca8327c54d59c0fa103540d
SHA1:	c2d38256cd16f2d6a2f9fdd4128d14378fd125ac
SHA256:	f2b3f79ade40513d7a6c736864b524c885eeb24934b3fd1ee71c38e666b45f18
SHA512:	97333a6a2b6240ca020cbc99529ac8baa1057a73c6a6b6e872642dfb73f026c3152048aa0f0183a310116097fd2ae746c96630b6eb6aeb0e6588f625efbef8e2
SSDEEP:	3072:fWLHqJ4VtWYQUVpsPHQqdPFQ6l7Bz9DHzcUvNfxYPr9fGWg+Bm5kf7DLm:4qO/rsPHN7Q6l7Bz9zhvNJYPrg1+L
File Content Preview:	MZ..... ....PE..d..

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1800080e4
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	
Time Stamp:	0x60804A27 [Wed Apr 21 15:52:07 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 00007F9010934536h
cmp edx, ebx
jne 00007F9010934541h
mov eax, ebx
lock xadd dword ptr [0002B8AFh], eax
add eax, ebx
cmp eax, ebx
jne 00007F9010934531h

Instruction
dec ecx
mov edx, eax
call 00007F90109472E2h
test eax, eax
je 00007F9010934525h
xor ebx, ebx
jmp 00007F9010934521h
lock add dword ptr [0002B891h], FFFFFFFFh
jne 00007F9010934517h
call 00007F90109463A3h
mov eax, ebx
dec eax
add esp, 20h
pop ebx
ret
int3
int3
dec eax
mov dword ptr [esp+08h], ebx
dec eax
mov dword ptr [esp+10h], ebp
dec eax
mov dword ptr [esp+18h], esi
push edi
dec eax
sub esp, 20h
cmp dword ptr [0002BE31h], 00000000h
inc ecx
mov ebx, ecx
dec ecx
mov esi, eax
dec eax
mov eax, edx
je 00007F90109345B3h
xor edx, edx
dec eax
mov ecx, eax
call 00007F901092EB35h
dec eax
mov ecx, dword ptr [0002B83Dh]
dec esp
lea eax, dword ptr [ebx+01h]
xor edx, edx
dec eax
mov ebp, eax
call dword ptr [00024F26h]
dec eax
test eax, eax
dec eax
mov edi, eax
je 00007F9010934587h
dec esp
mov eax, ebx
dec eax
mov edx, esi
dec eax
mov ecx, eax
call 00007F901094BA2Bh
dec eax
lea ecx, dword ptr [0002BDB9h]
mov byte ptr [ebx+edi], 00000000h
call dword ptr [0002504Fh]
lock add dword ptr [0002BDCFh], 01h
dec eax

Instruction
lea ecx, dword ptr [00000000h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x31b10	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x30a20	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x34000	0x17ac	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x39000	0x344	.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	0x2d000	0x530	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x2eda4	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	0x2ba46	0x2bc00	False	0.568303571429	data	6.33861296477	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2d000	0x4b48	0x4c00	False	0.403114720395	data	5.25264814147	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x32000	0x1f88	0x1a00	False	0.307992788462	lif file	3.7353523401	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x34000	0x17ac	0x1800	False	0.53857421875	data	5.30366145469	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x36000	0x2148	0x2200	False	0.427504595588	data	4.96451183531	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x39000	0x1000	0xa00	False	0.458984375	data	4.2959680462	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

- loaddll64.exe
- cmd.exe
- rundll32.exe

● rundll32.exe

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 4992 Parent PID: 5700

General

Start time:	11:45:28
Start date:	04/05/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\206bfb50000.dll'
Imagebase:	0x7ff621dc0000
File size:	140288 bytes
MD5 hash:	A84133CCB118CF35D49A423CD836D0EF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 204 Parent PID: 4992

General

Start time:	11:45:28
Start date:	04/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\206bfb50000.dll',#1
Imagebase:	0x7ff7bf140000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 4896 Parent PID: 4992

General

Start time:	11:45:29
Start date:	04/05/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\206bfb50000.dll,#1
Imagebase:	0x7ff68ef20000
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5412 Parent PID: 204

General

Start time:	11:45:29
Start date:	04/05/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\206bfb50000.dll',#1
Imagebase:	0x7ff68ef20000
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis