ID: 324360
Sample Name: JbVn44CzFw
Cookbook: default.jbs
Time: 16:32:05
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Copyright null 2020

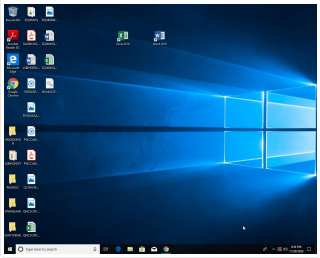
Analysis Report JbVn44CzFw

Overview

General Information

Sample Name:	JbVn44CzFw (renamed file extension from none to dll)
Analysis ID:	324360
MD5:	ac716ad4ce2461..
SHA1:	bf3a28737bb643e.
SHA256:	1c2d38dda5eb14..

Most interesting Screenshot:



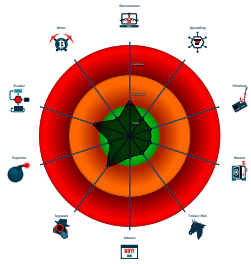
Detection

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

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Creates a DirectInput object (often fo…
- May sleep (evasive loops) to hinder …
- PE file contains strange resources
- Program does not show much activi…
- Sample file is different than original …
- Tries to load missing DLLs

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5740 cmdline: loaddll32.exe 'C:\Users\user\Desktop\JbVn44CzFw.dll' MD5: 76E2251D0E9772B9DA90208AD741A205)
  - rundll32.exe (PID: 5912 cmdline: rundll32.exe C:\Users\user\Desktop\JbVn44CzFw.dll,Continentmark MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2148 cmdline: rundll32.exe C:\Users\user\Desktop\JbVn44CzFw.dll,Thankclaim MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

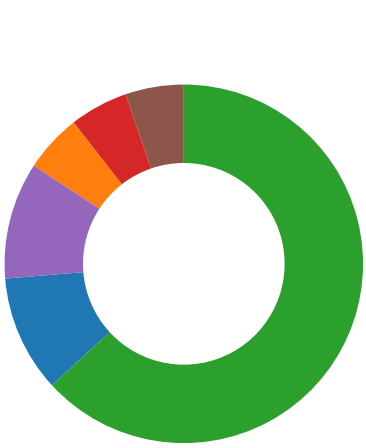
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

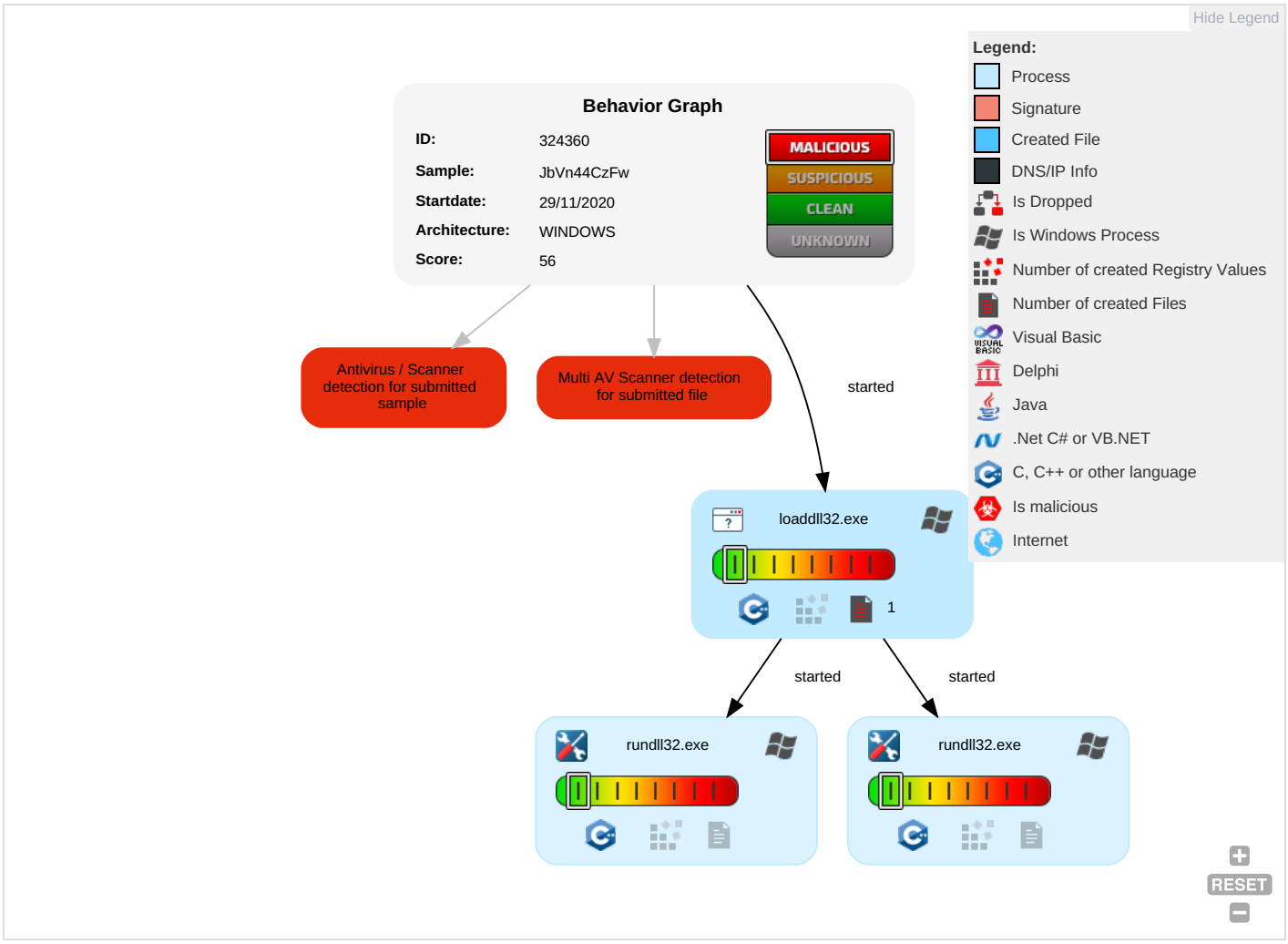
Multi AV Scanner detection for submitted file

Mitre Att&ck Matrix

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

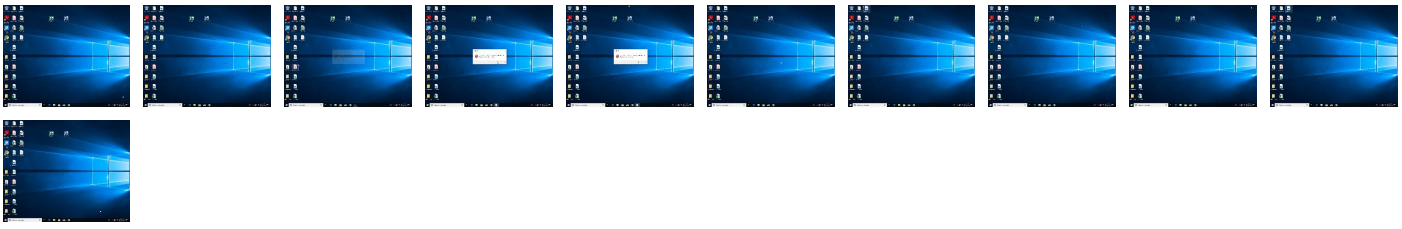
Copyright null 2020



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
JbVn44CzFw.dll	65%	Virustotal		Browse
JbVn44CzFw.dll	67%	ReversingLabs	Win32.Trojan.Kryptik	
JbVn44CzFw.dll	100%	Avira	TR/AD.Dridex.cpgs	

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:	31.0.0 Red Diamond
Analysis ID:	324360
Start date:	29.11.2020
Start time:	16:32:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JbVn44CzFw (renamed file extension from none to 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:	23
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.winDLL@5/0@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
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe

Simulations

Behavior and APIs

Time	Type	Description
16:33:01	API Interceptor	2x Sleep call for process: loaddll32.exe modified
16:33:13	API Interceptor	2x Sleep call for process: rundll32.exe modified

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):	6.299075820327542
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:	JbVn44CzFw.dll
File size:	491008
MD5:	ac716ad4ce2461246e783bda05ba40a4
SHA1:	bf3a28737bb643e478021b279aec7213e5216666
SHA256:	1c2d38dda5eb14c8870b4ef6a95f054f30a88dda3474712b956094c65d063103
SHA512:	b6366b6813e88c43b58f5217629b9f485d92b0baa294913f007fa6a7d87e0091cbb385e5c119579ff766f3611dad61439335b0b032719702a0f2ccf954afbdf7
SSDEEP:	6144:bBtHoA+cBYUrraE4Cx/chlPmXYDWhPsmZWGOYnKw0JKYflkBTKilaC0u:U0aFCqTPmXYDWdsmZWGOLw0btCui
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ...s...s...s..2s...s..1s...s.. s...s..'s4..s..7s...s...s...s...s...s..6s...s..0s...s..5s...sRich...s.....PE..L..

File Icon

Icon Hash:	f0f0ccccccecc68

Static PE Info

General

Entrypoint:	0x420090
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x5DD16C15 [Sun Nov 17 15:49:41 2019 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:	7f464f31966f9c77555f8117da4c066c

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F089446C377h
call 00007F089447B0E5h
mov eax, dword ptr [ebp+10h]
push eax
mov ecx, dword ptr [ebp+0Ch]
push ecx
mov edx, dword ptr [ebp+08h]
push edx
call 00007F089446C384h
add esp, 0Ch
pop ebp
retn 000Ch
int3
int3
int3
int3
int3
int3
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push FFFFFFFEh
push 00463B70h
push 0042B470h
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFFE8h
push ebx
push esi
push edi
mov eax, dword ptr [0046673Ch]
xor dword ptr [ebp-08h], eax
xor eax, ebp
push eax

Instruction
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
mov dword ptr [ebp-18h], esp
mov dword ptr [ebp-1Ch], 00000001h
cmp dword ptr [ebp+0Ch], 00000000h
jne 00007F089446C382h
cmp dword ptr [0046B4E4h], 00000000h
jne 00007F089446C379h
xor eax, eax
jmp 00007F089446C4C3h
mov dword ptr [ebp-04h], 00000000h
cmp dword ptr [ebp+0Ch], 01h
je 00007F089446C378h
cmp dword ptr [ebp+0Ch], 02h
jne 00007F089446C3C6h
cmp dword ptr [00449318h], 00000000h
je 00007F089446C387h
mov eax, dword ptr [ebp+10h]
push eax
mov ecx, dword ptr [ebp+0Ch]
push ecx
mov edx, dword ptr [ebp+08h]
push edx
call dword ptr [00449318h]
mov dword ptr [ebp-1Ch], eax
cmp dword ptr [ebp-1Ch], 00000000h
je 00007F089446C386h
mov eax, dword ptr [ebp+10h]
push eax
mov ecx, dword ptr [ebp+0Ch]
push ecx
mov edx, dword ptr [ebp+08h]
push edx
call 00007F089447C0DBh

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [ASM] VS2008 build 21022 • [LNK] VS2008 SP1 build 30729 • [EXP] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [C++] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x655b0	0x5e	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x64b6c	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x977000	0x4928	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x97c000	0x2af4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x48250	0x1c	.rdata
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	0x48000	0x1c8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
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	0x46081	0x46200	False	0.57083124443	data	6.54741114063	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x48000	0x1d60e	0x1d800	False	0.606652211335	data	5.973702872	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x66000	0x9101c8	0x5200	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x977000	0x4928	0x4a00	False	0.490023226351	data	5.47494215962	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x97c000	0xa2b6	0xa400	False	0.215653582317	data	2.52515301313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x9774a8	0x25a8	data	English	United States
RT_ICON	0x979a50	0x10a8	data	English	United States
RT_ICON	0x97aaf8	0x988	data	English	United States
RT_ICON	0x97b480	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_GROUP_ICON	0x97b8e8	0x3e	data	English	United States
RT_VERSION	0x977180	0x328	data	English	United States

Imports

DLL	Import
KERNEL32.dll	CreateFileA, HeapAlloc, QueryPerformanceCounter, WaitForSingleObject, SetEvent, GetProcessHeap, GetDateFormatA, OpenProcess, GetVolumeInformationA, Sleep, GetFileAttributesA, CreateProcessA, VirtualProtectEx, LoadLibraryA, GetSystemInfo, GetModuleFileNameA, GetModuleHandleA, GetCurrentDirectoryA, GetVersionExA, GetSystemTime, GetConsoleOutputCP, WriteConsoleA, SetStdHandle, GetLocaleInfoW, InitializeCriticalSectionAndSpinCount, GetUserDefaultLCID, EnumSystemLocalesA, IsValidLocale, GetLocaleInfoA, WideCharToMultiByte, InterlockedIncrement, InterlockedDecrement, MultiByteToWideChar, InterlockedExchange, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetModuleFileNameW, GetCurrentThreadId, GetCommandLineA, GetCPInfo, HeapValidate, IsBadReadPtr, RaiseException, RtlUnwind, LCMapStringA, GetLastError, LCMapStringW, GetProcAddress, TlsGetValue, GetModuleHandleW, TlsAlloc, TlsSetValue, TlsFree, SetLastError, DebugBreak, GetStdHandle, WriteFile, OutputDebugStringA, WriteConsoleW, GetFileType, OutputDebugStringW, ExitProcess, LoadLibraryW, SetHandleCount, GetStartupInfoA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, HeapDestroy, HeapCreate, HeapFree, VirtualFree, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, GetStringTypeA, GetStringTypeW, FlushFileBuffers, GetConsoleCP, GetConsoleMode, HeapSize, HeapReAlloc, VirtualAlloc, GetACP, GetOEMCP, IsValidCodePage, ReadFile, SetFilePointer, CloseHandle
ole32.dll	OleCreate, CoInitialize, StgCreateDocfile, OleUninitialize, CoSuspendClassObjects, OleInitialize, CoUninitialize
UxTheme.dll	GetThemeTextExtent, GetThemeFont, CloseThemeData
MPR.dll	WNetGetConnectionA, WNetGetUserA, WNetGetUniversalNameA

Exports

Name	Ordinal	Address
Continentmark	1	0x4165f0
Thankclaim	2	0x416650

Version Infos

Description	Data
LegalCopyright	2007. All rights reserved. condition.
InternalName	play1.dll
FileVersion	1.1.4756.2976
CompanyName	GovernThese Solver Least
ProductName	LawThey Whole Wire
ProductVersion	1.1.4756.2976
FileDescription	LawThey Whole Wire
OriginalFilename	play1.dll
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
English	United States	

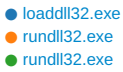
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5740 Parent PID: 5644

General

Start time:	16:32:51
Start date:	29/11/2020
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\JbVn44CzFw.dll'
Imagebase:	0x8e0000
File size:	119808 bytes
MD5 hash:	76E2251D0E9772B9DA90208AD741A205
Has elevated privileges:	true

Copyright null 2020

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: rundll32.exe PID: 5912 Parent PID: 5740

General

Start time:	16:33:01
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\JbVn44CzFw.dll,Continentmark
Imagebase:	0x110000
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2148 Parent PID: 5740

General

Start time:	16:33:04
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\JbVn44CzFw.dll,Thankclaim
Imagebase:	0x110000
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis

Copyright null 2020