ID: 651262
Sample Name: wlbsctrl.dll
Cookbook: default.jbs
Time: 18:03:50
Date: 23/06/2022
Version: 35.0.0 Citrine

Table of Contents

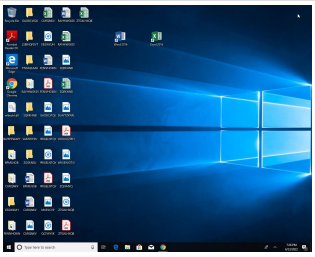
Windows Analysis Report

wlbsctrl.dll

Overview

General Information

Sample Name:	wlbsctrl.dll
Analysis ID:	651262
MD5:	8b2356cc4b0a38..
SHA1:	ffb6a64c9996aa9..
SHA256:	1e57baa7d7c987..
Infos:	



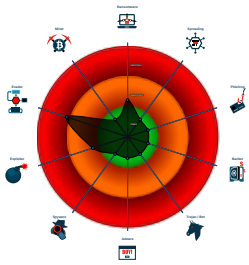
Detection

Score:	26
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Contains functionality to detect slee…
- Found inlined nop instructions (likely…
- Sample file is different than original …
- Contains functionality to check if a d…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Detected potential crypto function
- Contains functionality to call native …
- Contains functionality to detect sand…
- May check if the current machine is…
- Program does not show much activi…

Classification



Analysis Advice

Sample monitors window changes (e.g. starting applications), analyze the sample with the 'Simulates keyboard and window changes' cookbook

Sample may be VM or Sandbox-aware, try analysis on a native machine

Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 5068 cmdline: loaddll64.exe "C:\Users\user\Desktop\wlbsctrl.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 3352 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\wlbsctrl.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5828 cmdline: rundll32.exe "C:\Users\user\Desktop\wlbsctrl.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

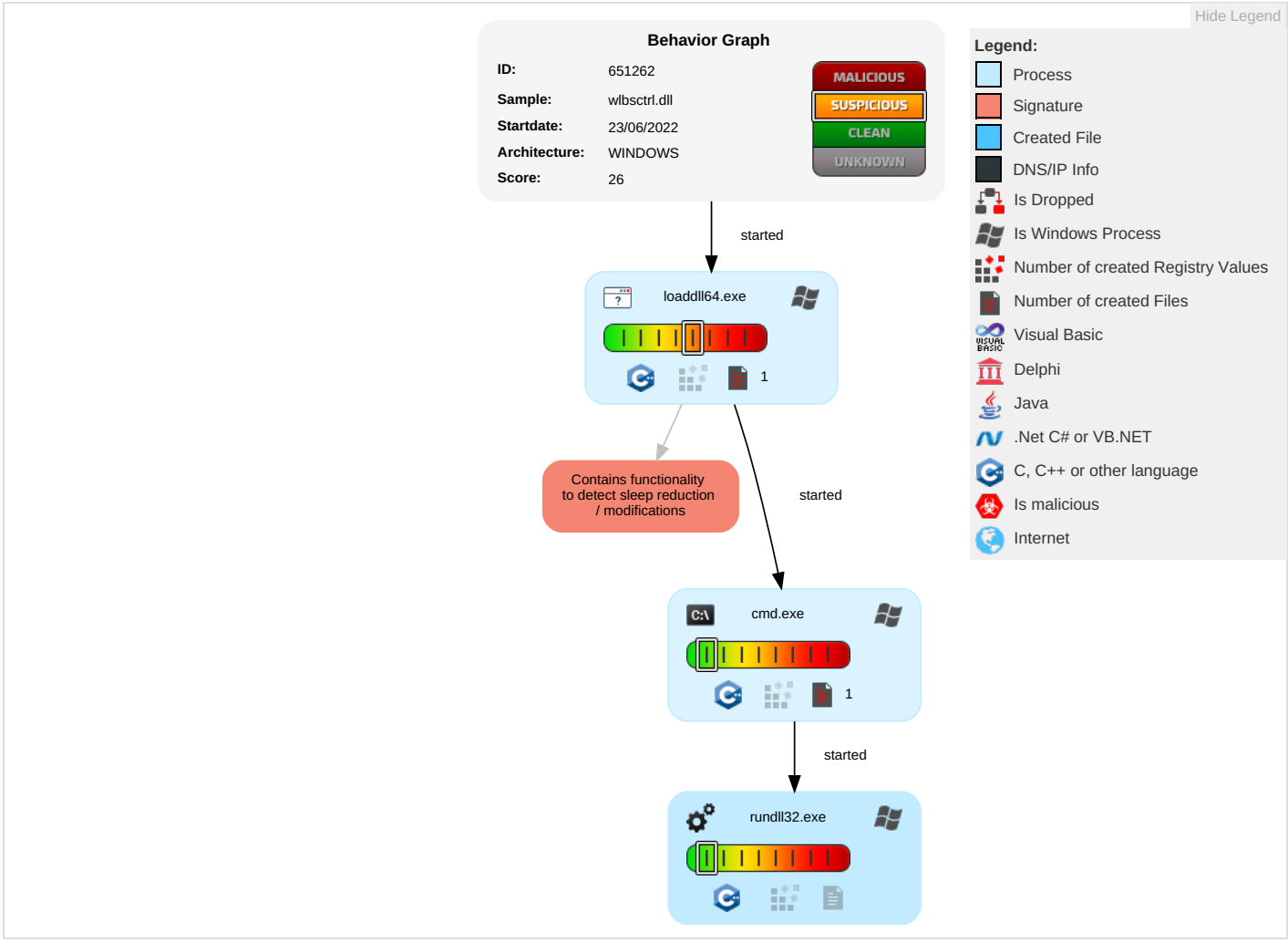
Malware Analysis System Evasion

Contains functionality to detect sleep reduction / modifications

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	Path Interception	1 1 Process Injection	1 Rundll32	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 2 Virtualization/Sandbox Evasion	LSASS Memory	1 3 Security Software Discovery	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 Process 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)	2 Obfuscated Files or Information	NTDS	1 2 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

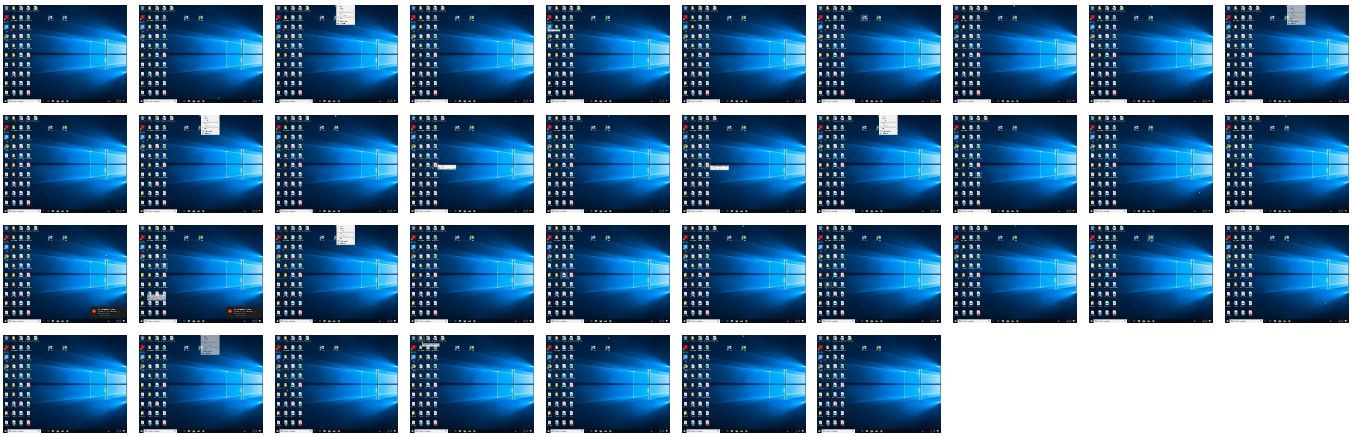
Behavior Graph



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

No Antivirus matches

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:	35.0.0 Citrine
Analysis ID:	651262
Start date and time: 23/06/202218:03:50	2022-06-23 18:03:50 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wlbsctrl.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:	32
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:	SUS
Classification:	sus26.evad.winDLL@5/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 19.6% (good quality ratio 3.5%) • Quality average: 13.8% • Quality standard deviation: 31.9%
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, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, time.windows.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:05:07	API Interceptor	1x Sleep call for process: loaddll64.exe modified

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) x86-64, for MS Windows
Entropy (8bit):	2.301165268606333
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	wlbsctrl.dll
File size:	775168
MD5:	8b2356cc4b0a382e79dcd4a844839e91
SHA1:	ffb6a64c9996aa9e14ab69791f610babf98784c5
SHA256:	1e57baa7d7c987aebd09b43788e9388c89a1cb9e89b4cbad24a8662e606d62f2
SHA512:	273c11f50ce23d01108c7edf484f10fc7d318cd89fcc51baf7f2721f1655340b0167214498f5e08a9e7fdae9e656f6f516a7eff7a25e7151e1f0ea5fc5d71ba0
SSDEEP:	12288:FjwnXutNmopfRYxaKHFiPTLJsaVHct37frld/ibWccccccccI6gRThD:
TLSH:	59F4B75A0823D211D8244C3196377AC66F1672E9776C27D3F6A92FA2C1390C1AD77F3A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{Fv.(Fv.(Fv.(O.k(Bv.(...)Dv.(R..)Cv.(Fv.(pv.(...)Jv.(...)Nv.(...)Bv.(...)Gv.(...(Gv.(Fvo(Gv.(...)Gv.(RichFv.(.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x18000100a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x62ACC1D8 [Fri Jun 17 18:03:04 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	05dcd6eab6e64f86dc1e816425be7b14

Entrypoint Preview

Instruction
jmp 00007F7328B01BB2h
jmp 00007F7328B02099h
jmp 00007F7328B00C2Ch
jmp 00007F7328B02107h
jmp 00007F7328B00DF2h
jmp 00007F7328B02925h
jmp 00007F7328B02B44h
jmp 00007F7328AFFA93h
jmp 00007F7328B02342h
jmp 00007F7328B020EDh
jmp 00007F7328B05F64h
jmp 00007F7328B02B23h
jmp 00007F7328B02B32h
jmp 00007F7328B00B35h
jmp 00007F7328B05F30h
jmp 00007F7328B03D6Bh
jmp 00007F7328B01122h
jmp 00007F7328B05FA1h
jmp 00007F7328B0169Ch
jmp 00007F7328B028BBh
jmp 00007F7328B02B02h
jmp 00007F7328B0220Dh
jmp 00007F7328B03D28h
jmp 00007F7328B015F3h
jmp 00007F7328B02AE6h
jmp 00007F7328B05FD9h
jmp 00007F7328B00F1Ch
jmp 00007F7328B014D7h
jmp 00007F7328B05E8Ah
jmp 00007F7328B023F9h
jmp 00007F7328B02AD4h
jmp 00007F7328B02007h
jmp 00007F7328B05E26h
jmp 00007F7328B01FF9h
jmp 00007F7328B0225Ch

Instruction
jmp 00007F7328B00467h
jmp 00007F7328B05FC2h
jmp 00007F7328B02069h
jmp 00007F7328B00C6Ch
jmp 00007F7328AFF7A3h

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbe3b0	0x78	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc1000	0x890	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0xbd000	0x420	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc2000	0x40	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xab64	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xb0a0	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xaba0	0x138	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xbe000	0x3b0	.idata
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	0x89b5	0x8a00	False	0.24363111413043478	data	3.5100227973693183	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xa000	0x1f62	0x2000	False	0.1304931640625	data	1.5044615193257005	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc000	0xb0539	0xafe00	False	0.1482459355010661	data	2.016608344146886	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0xbd000	0x5ac	0x600	False	0.3919270833333333	data	3.213440260810703	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.idata	0xbe000	0xe3d	0x1000	False	0.23828125	data	3.0459227597586005	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tls	0xbf000	0x309	0x400	False	0.021484375	data	0.011173818721219527	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.00cfg	0xc0000	0x151	0x200	False	0.0546875	data	0.330964730370671	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc1000	0x890	0xa00	False	0.2640625	data	2.6030848233720585	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc2000	0x1f1	0x200	False	0.14453125	data	0.7368777605793444	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc11c0	0x354	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0xc1518	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	CreateFileA, GetDiskFreeSpaceExA, CloseHandle, Sleep, GetCurrentProcess, GetTickCount, GetModuleHandleA, GetProcAddress, CreateFileMappingA, K32EnumProcesses, K32GetModuleInformation, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, SetEvent, ResetEvent, WaitForSingleObjectEx, CreateEventW, GetModuleHandleW, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, IsProcessorFeaturePresent, TerminateProcess, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead
USER32.dll	GetCursorPos
VCRUNTIME140.dll	memset, __C_specific_handler, __current_exception, __current_exception_context, __std_type_info_destroy_list
api-ms-win-crt-stdio-l1-1-0.dll	__acrt_iob_func, __stdio_common_vfprintf
api-ms-win-crt-runtime-l1-1-0.dll	terminate, _initterm_e, _seh_filter_dll, _configure_narrow_argv, _initialize_narrow_environment, _initialize_onexit_table, _register_onexit_function, _execute_onexit_table, _crt_atexit, _crt_at_quick_exit, _cexit, _initterm

Possible Origin

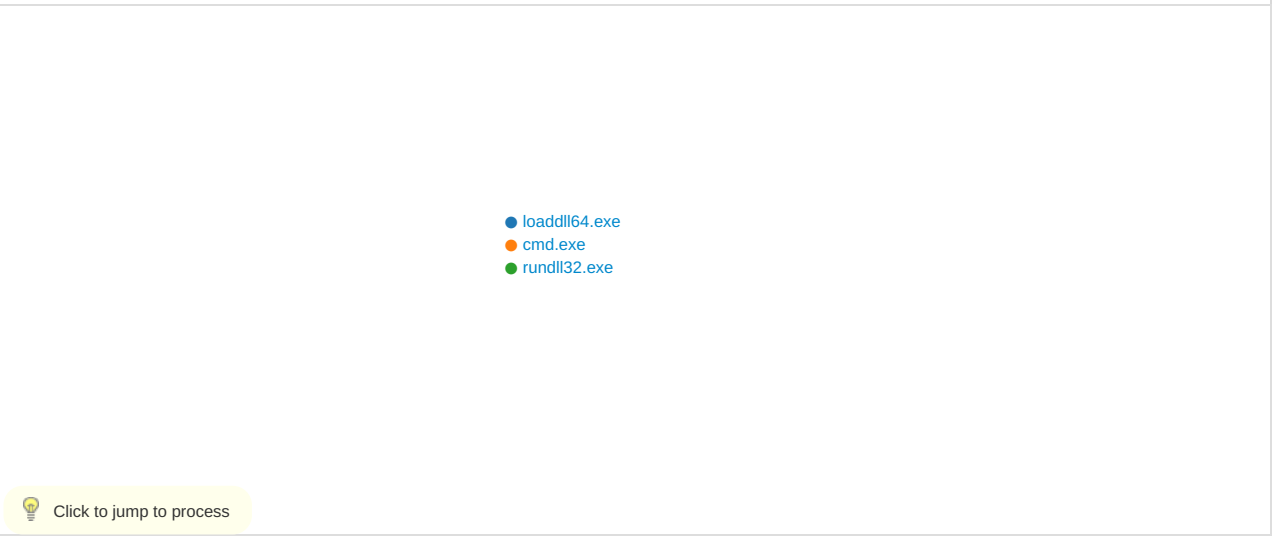
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **5068**, Parent PID: **3892**

General

Target ID:	1
Start time:	18:04:53
Start date:	23/06/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\wlbsctrl.dll"
Imagebase:	0x7ff7eaf20000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **3352**, Parent PID: **5068**

General

Target ID:	3
Start time:	18:04:53
Start date:	23/06/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\wlbsctrl.dll",#1
Imagebase:	0x7ff7bb450000
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: **5828**, Parent PID: **3352**

General

Target ID:	4
Start time:	18:04:54
Start date:	23/06/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\wlbsctrl.dll",#1
Imagebase:	0x7ff745220000
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