ID: 780203
Sample Name: 8082-x64.dll.exe
Cookbook: default.jbs
Time: 16:01:00
Date: 08/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 8082-x64.dll.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Initial Sample 4
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 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 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
World Map of Contacted IPs 8
General Information 8
Warnings 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 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 11
Sections 11
Imports 15
Exports 15
Network Behavior 16
Statistics 16
Behavior 16
System Behavior 16
Analysis Process: loaddll64.exePID: 3420, Parent PID: 3452 16
General 16
File Activities 16
Analysis Process: conhost.exePID: 3384, Parent PID: 3420 16
General 16
Analysis Process: cmd.exePID: 5260, Parent PID: 3420 17
General 17
File Activities 17
Analysis Process: regsvr32.exePID: 6136, Parent PID: 3420 17
General 17
Analysis Process: rundll32.exePID: 5160, Parent PID: 5260 17
General 17
Analysis Process: rundll32.exePID: 5204, Parent PID: 3420 18
General 18
Analysis Process: rundll32.exePID: 1408, Parent PID: 3420 18
General 18
Analysis Process: rundll32.exePID: 4952, Parent PID: 3420 18
General 18
Disassembly 19

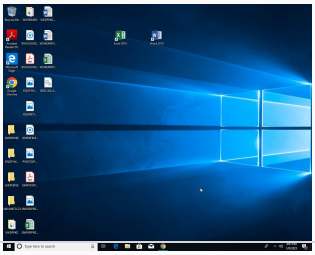
Windows Analysis Report

8082-x64.dll.exe

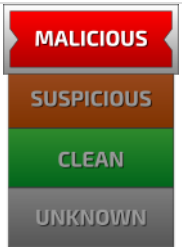
Overview

General Information

Sample Name:	8082-x64.dll.exe (renamed file extension from exe to dll)
Analysis ID:	780203
MD5:	43616639411a59.
SHA1:	416932059dc348..
SHA256:	6a289f491c8d5d..
Tags:	45139105143 exe opendir
Infos:	YARA



Detection



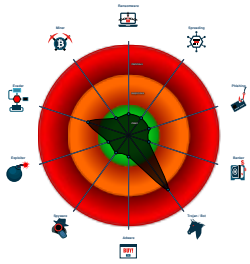
CobaltStrike

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

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected CobaltStrike
- Multi AV Scanner detection for subm…
- Machine Learning detection for sam…
- Registers a DLL
- Sample execution stops while proce…
- PE file contains more sections than…
- Yara signature match
- Tries to load missing DLLs
- May sleep (evasive loops) to hinder…
- Program does not show much activi…
- Creates a process in suspended mo…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 3420 cmdline: loaddll64.exe "C:\Users\user\Desktop\8082-x64.dll.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 3384 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5260 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\8082-x64.dll.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5160 cmdline: rundll32.exe "C:\Users\user\Desktop\8082-x64.dll.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 6136 cmdline: regsvr32.exe /s C:\Users\user\Desktop\8082-x64.dll.dll MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 5204 cmdline: rundll32.exe C:\Users\user\Desktop\8082-x64.dll.dll,DllGetClassObject MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 1408 cmdline: rundll32.exe C:\Users\user\Desktop\8082-x64.dll.dll,DllMain MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4952 cmdline: rundll32.exe C:\Users\user\Desktop\8082-x64.dll.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
8082-x64.dll.dll	CobaltStrike_Resources_Artifact64_v3_14_to_v4_x	Cobalt Strike\'s resources/artifact64{.exe,.dll,svc.exe,svcbig.exe,big.exe,big.dll,.x64.dll,big.x64.dll} and resource/artifactuac(alt)64.exe signature for versions v3.14 through v4.x	gssincla@google.com	• 0xa25:$fmtBuilder: 41 B8 5C 00 00 00 C7 44 24 50 5C 00 00 00 C7 44 24 48 65 00 00 00 C7 44 24 40 70 00 00 00 C7 44 24 38 69 00 00 00 C7 44 24 30 70 00 00 00 C7 44 24 28 5C 00 00 00 C7 44 24 20 2E 00 00 00 89 54 ... • 0x44a00:$fmtString: %c%c%c%c%c%c%c%cMSSE-%d-server
8082-x64.dll.dll	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	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

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Remote Access Functionality

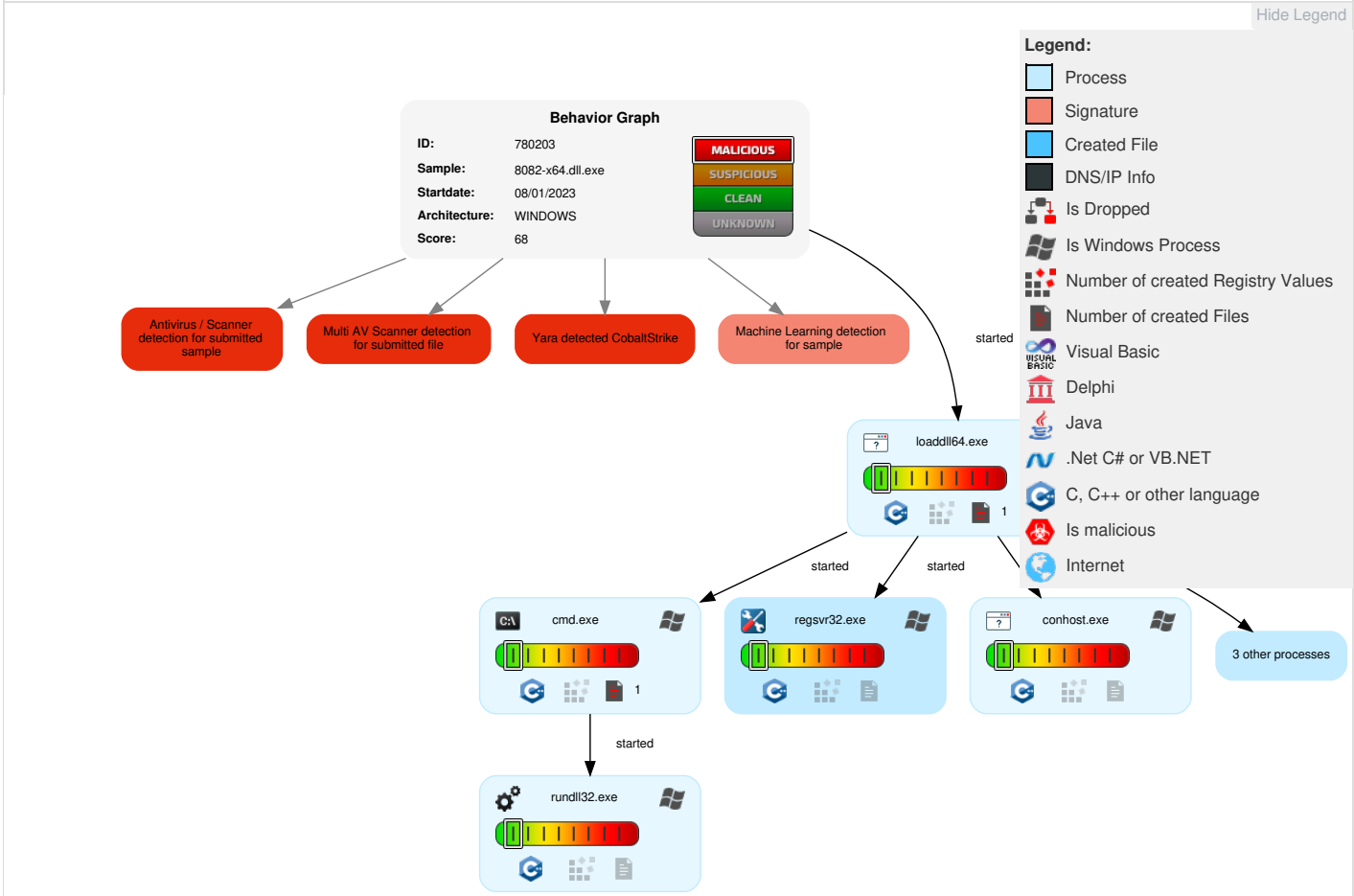
Yara detected CobaltStrike

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 Regsvr32	OS Credential Dumping	1 1 Virtualization/Sandbox Evasion	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 System Information 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 Virtualization/Sandbox Evasion	Security Account Manager	Query Registry	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	System Network Configuration Discovery	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	1 DLL Side-Loading	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

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
8082-x64.dll.dll	78%	ReversingLabs	Win64.Backdoor.CobaltStrike	
8082-x64.dll.dll	63%	Virustotal		Browse
8082-x64.dll.dll	100%	Avira	HEUR/AGEN.1235510	
8082-x64.dll.dll	100%	Joe Sandbox ML		

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:	780203
Start date and time:	2023-01-08 16:01:00 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8082-x64.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:	22
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@14/0@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:	• Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
16:02:08	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) (console) x86-64 (stripped to external PDB), for MS Windows
Entropy (8bit):	7.250454733634642
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.41% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • VXD Driver (31/22) 0.03%
File name:	8082-x64.dll.dll
File size:	287744
MD5:	43616639411a590f022505998a6f567e
SHA1:	416932059dc3488000b171beeac258fc792d4c71
SHA256:	6a289f491c8d5d789e31e89c73ba06ef6fc075458a1106b7213b29da798f6c03
SHA512:	9989fc8ee3a07db0a9f9a98395e75178507f20e9189f15c9b9dc51f55efe23c324388edc0032ded78db392f69ae9560505a979e165661a0fe46ca7c73c41139a
SSDEEP:	6144:49TczeYIVeH21LD3rMPwjEMSUEufxTUhYohcnxK7xERM5jy45yrjz:weAP3QPKEeEuShYohcnx+xEsUT
TLSH:	9954ADC0D6EEE60CEA36C5B72B9762679030F344FAD62BB124660B0696D647DD0D027F

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....^....."..... ...`.....k..... .....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x6bac13f0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x6bac0000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED, DLL
DLL Characteristics:	
Time Stamp:	0x5EDED517 [Tue Jun 9 00:17:27 2020 UTC]
TLS Callbacks:	0x6bac1910
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:	f73cb1b8999c7e79c50459b8e1f144f0

Entrypoint Preview

Instruction
dec eax
sub esp, 48h
mov dword ptr [00047C22h], 00000000h
cmp edx, 01h
je 00007F19909F547Fh
dec eax
add esp, 48h
jmp 00007F19909F52F9h
nop dword ptr [eax+00h]
mov dword ptr [esp+30h], edx
dec eax
mov dword ptr [esp+38h], ecx
dec esp
mov dword ptr [esp+28h], eax
call 00007F19909F6092h
call 00007F19909F63FDh
dec esp
mov eax, dword ptr [esp+28h]
dec eax
mov ecx, dword ptr [esp+38h]
mov edx, dword ptr [esp+30h]
dec eax
add esp, 48h
jmp 00007F19909F52C6h
nop
push ebp
push edi
push esi

Instruction
push ebx
dec eax
sub esp, 58h
inc ebp
xor eax, eax
inc ecx
mov ecx, 00000001h
dec eax
mov edi, ecx
mov esi, edx
mov dword ptr [esp+4Ch], 00000000h
dec eax
mov dword ptr [esp+38h], 00000000h
mov dword ptr [esp+30h], 00000000h
mov edx, 00000002h
mov dword ptr [esp+28h], 00000000h
mov dword ptr [esp+20h], 00000000h
dec eax
lea ecx, dword ptr [00048475h]
call dword ptr [00049D6Bh]
dec eax
mov ebx, eax
dec eax
lea eax, dword ptr [eax-01h]
dec eax
cmp eax, FFFFFFFDh
jnbe 00007F19909F54C0h
xor edx, edx
dec eax
mov ecx, ebx
call dword ptr [00049D43h]
test eax, eax
dec eax
mov ebp, dword ptr [00049E32h]
jne 00007F19909F549Ch
jmp 00007F19909F54A8h
dec eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x4a000	0xb0	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4b000	0x7bc	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x47000	0x27c	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x4e000	0x2c4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x4d000	0x28	.tls
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x4b1e4	0x1a8	.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	0x1f10	0x2000	False	0.5732421875	data	6.021842385150596	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x3000	0x42470	0x42600	False	0.5997381120527306	data	7.257802920028994	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x46000	0x170	0x200	False	0.416015625	data	3.5502048501802737	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.pdata	0x47000	0x27c	0x400	False	0.3515625	data	2.9537206983747	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.xdata	0x48000	0x200	0x200	False	0.380859375	locale data table	3.772885986330123	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.bss	0x49000	0x990	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.edata	0x4a000	0xb0	0x200	False	0.271484375	data	1.9824304709536775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.idata	0x4b000	0x7bc	0x800	False	0.357421875	data	4.239308826637131	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x4c000	0x58	0x200	False	0.0546875	data	0.20153937813451883	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.tls	0x4d000	0x48	0x200	False	0.0546875	data	0.29046607431271465	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x4e000	0x2c4	0x400	False	0.626953125	GLS_BINARY_LSB_FIRST	4.699885638394994	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	CloseHandle, ConnectNamedPipe, CreateFileA, CreateNamedPipeA, CreateThread, DeleteCriticalSection, EnterCriticalSection, GetCurrentProcess, GetCurrentProcessId, GetCurrentThreadId, GetLastError, GetModuleHandleA, GetProcAddress, GetSystemTimeAsFileTime, GetTickCount, InitializeCriticalSection, LeaveCriticalSection, LoadLibraryW, QueryPerformanceCounter, ReadFile, RtlAddFunctionTable, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, SetUnhandledExceptionFilter, Sleep, TerminateProcess, TlsGetValue, UnhandledExceptionFilter, VirtualAlloc, VirtualProtect, VirtualQuery, WriteFile
msvcrt.dll	__dllonexit, __iob_func, _amsg_exit, _initterm, _lock, _onexit, _unlock, abort, calloc, free, fwrite, malloc, memcpy, signal, sprintf, strlen, strncmp, vfprintf

Exports

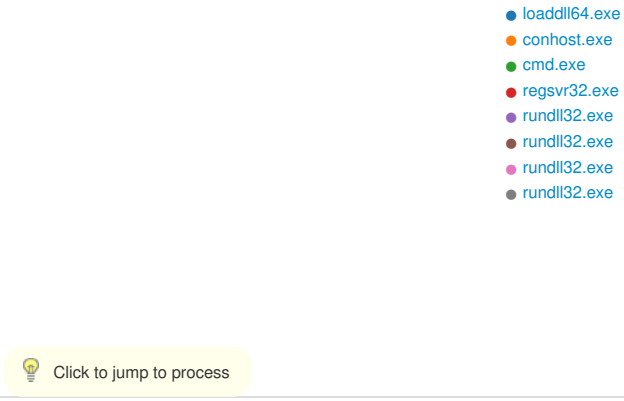
Name	Ordinal	Address
DllGetClassObject	1	0x6bac170b
DllMain	2	0x6bac16c7
DllRegisterServer	3	0x6bac1705
DllUnregisterServer	4	0x6bac1708
StartW	5	0x6bac1714

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 3420, Parent PID: 3452

General

Target ID:	0
Start time:	16:01:58
Start date:	08/01/2023
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\8082-x64.dll.dll"
Imagebase:	0x7ff6569f0000
File size:	139776 bytes
MD5 hash:	C676FC0263EDD17D4CE7D644B8F3FCD6
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: conhost.exe PID: 3384, Parent PID: 3420

General

Target ID:	1
Start time:	16:01:58

Start date:	08/01/2023
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: **5260**, Parent PID: **3420**

General

Target ID:	2
Start time:	16:01:58
Start date:	08/01/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\8082-x64.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: regsvr32.exe PID: **6136**, Parent PID: **3420**

General

Target ID:	3
Start time:	16:01:58
Start date:	08/01/2023
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\8082-x64.dll.dll
Imagebase:	0x7ff7fcfe0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **5160**, Parent PID: **5260**

General

Target ID:	4
Start time:	16:01:58

Start date:	08/01/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\8082-x64.dll.dll",#1
Imagebase:	0x7ff6aa9a0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **5204**, Parent PID: **3420**

General

Target ID:	5
Start time:	16:01:58
Start date:	08/01/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\8082-x64.dll.dll,DllGetClassObject
Imagebase:	0x7ff6aa9a0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **1408**, Parent PID: **3420**

General

Target ID:	6
Start time:	16:02:02
Start date:	08/01/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\8082-x64.dll.dll,DllMain
Imagebase:	0x7ff6aa9a0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **4952**, Parent PID: **3420**

General

Target ID:	7
Start time:	16:02:05
Start date:	08/01/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\8082-x64.dll.dll,DllRegisterServer
Imagebase:	0x7ff6aa9a0000

File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly