ID: 780212
Sample Name: 8082-svc-x64.exe
Cookbook: default.jbs
Time: 16:08:04
Date: 08/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

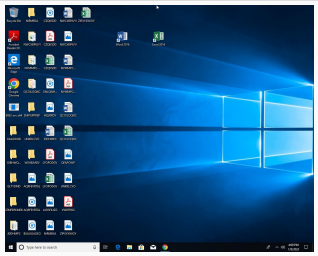
Windows Analysis Report

8082-svc-x64.exe

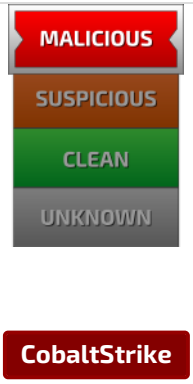
Overview

General Information

Sample Name:	8082-svc-x64.exe
Analysis ID:	780212
MD5:	89be3be20ca0dc..
SHA1:	4f92b6f168ee853.
SHA256:	37e828da01820a.
Tags:	45139105143 exe opendir
Infos:	



Detection



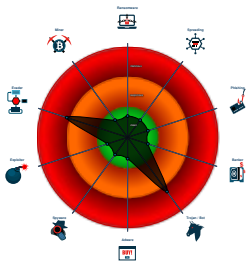
CobaltStrike

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected CobaltStrike
- Multi AV Scanner detection for subm…
- Found API chain indicative of debug…
- Machine Learning detection for sam…
- Yara signature match
- Found large amount of non-executed…
- Program does not show much activi…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- 8082-svc-x64.exe (PID: 6108 cmdline: C:\Users\user\Desktop\8082-svc-x64.exe MD5: 89BE3BE20CA0DCE73C12A5A015BCB9A5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
8082-svc-x64.exe	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	• 0xd75:$fmtBuilder: 41 B8 5C 00 00 00 C7 44 24 50 5C 00 00 00 C7 44 24 48 65 00 00 00 C7 44 24 40 70 00 00 00 C7 44 24 38 69 00 00 00 C7 44 24 30 70 00 00 00 C7 44 24 28 5C 00 00 00 C7 44 24 20 2E 00 00 00 89 54 ... • 0x44e50:$fmtString: %c%c%c%c%c%c%c%cMSSE-%d-server
8082-svc-x64.exe	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.8082-svc-x64.exe.400000.0.unpack	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	• 0xd75:$fmtBuilder: 41 B8 5C 00 00 00 C7 44 24 50 5C 00 00 00 C7 44 24 48 65 00 00 00 C7 44 24 40 70 00 00 00 C7 44 24 38 69 00 00 00 C7 44 24 30 70 00 00 00 C7 44 24 28 5C 00 00 00 C7 44 24 20 2E 00 00 00 89 54 ... • 0x44e50:$fmtString: %c%c%c%c%c%c%c%cMSSE-%d-server
0.2.8082-svc-x64.exe.400000.0.unpack	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	Joe Security	
0.0.8082-svc-x64.exe.400000.0.unpack	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	• 0xd75:$fmtBuilder: 41 B8 5C 00 00 00 C7 44 24 50 5C 00 00 00 C7 44 24 48 65 00 00 00 C7 44 24 40 70 00 00 00 C7 44 24 38 69 00 00 00 C7 44 24 30 70 00 00 00 C7 44 24 28 5C 00 00 00 C7 44 24 20 2E 00 00 00 89 54 ... • 0x44e50:$fmtString: %c%c%c%c%c%c%c%cMSSE-%d-server
0.0.8082-svc-x64.exe.400000.0.unpack	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

Anti Debugging

Found API chain indicative of debugger detection

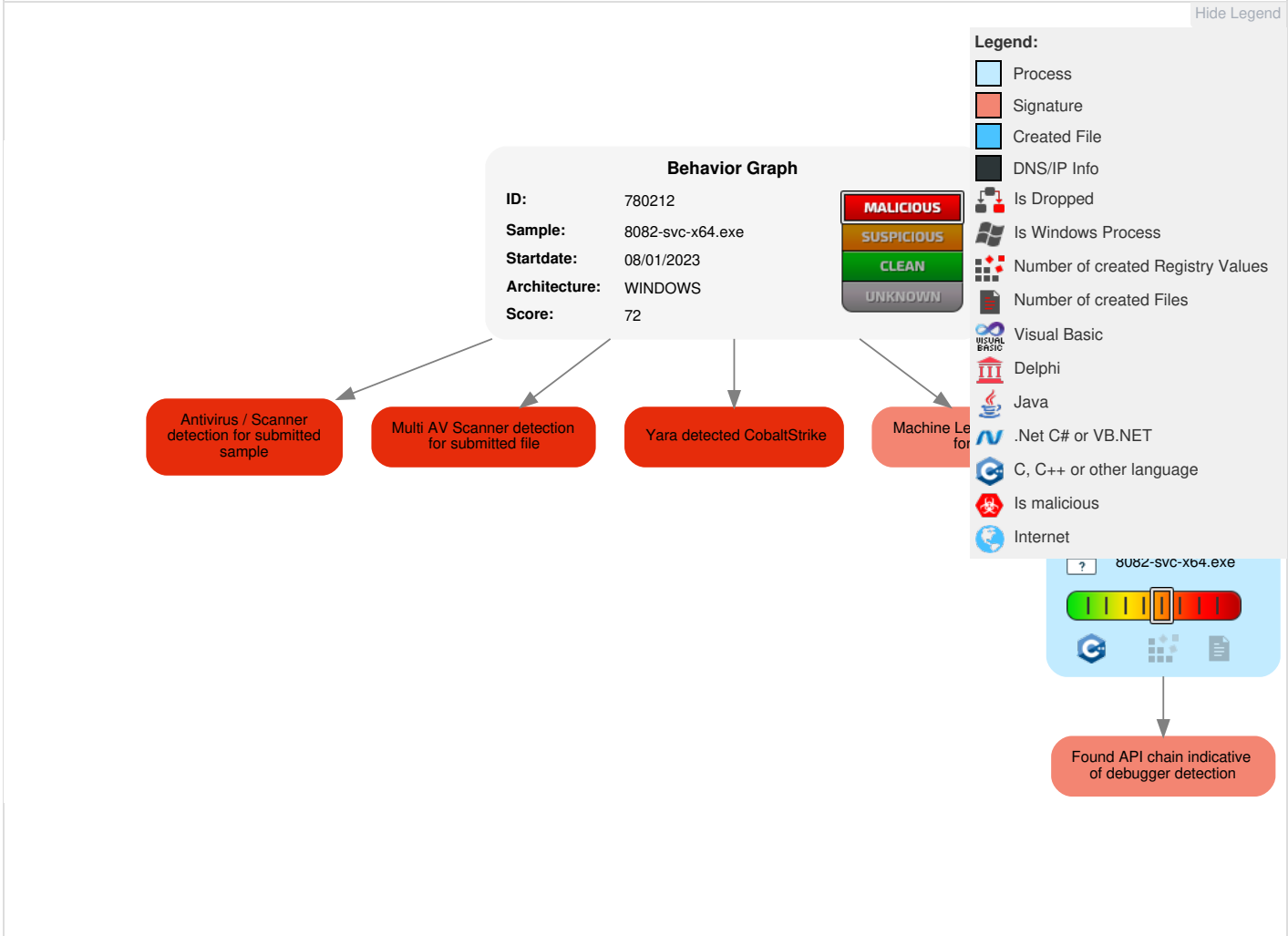
Remote Access Functionality

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	2 Service Execution	3 Windows Service	3 Windows Service	1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 System Time 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 Process Injection	1 Process Injection	LSASS Memory	1 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)	Obfuscated Files or Information	Security Account Manager	1 Virtualization/Sandbox Evasion	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)	Binary Padding	NTDS	2 System Information 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
8082-svc-x64.exe	80%	ReversingLabs	Win64.Backdoor.CobaltStrike	
8082-svc-x64.exe	68%	Virustotal		Browse
8082-svc-x64.exe	100%	Avira	HEUR/AGEN.1202022	
8082-svc-x64.exe	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:	780212
Start date and time:	2023-01-08 16:08:04 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8082-svc-x64.exe
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:	1
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:	mal72.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 95.8% (good quality ratio 59.2%) • Quality average: 48% • Quality standard deviation: 42.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

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:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Entropy (8bit):	7.355879244825435
TrID:	• Win64 Executable (generic) (12005/4) 74.80% • Generic Win/DOS Executable (2004/3) 12.49% • DOS Executable Generic (2002/1) 12.47% • VXD Driver (31/22) 0.19% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.04%
File name:	8082-svc-x64.exe
File size:	289280
MD5:	89be3be20ca0dce73c12a5a015bcb9a5
SHA1:	4f92b6f168ee8536278fa58a6df5c9b368421030
SHA256:	37e828da01820aad58414d0b73c935a0e408c274cdd872cbbae25f9cbcba0b08
SHA512:	d8490691ad53b026586dad57bb8bc59c8c3c7c9433305d317ad9aa203d9998b4fcf0e514cc562285565a1763dca7f96cfc0c62336a98cea62026dc114908b8a7
SSDEEP:	6144:6p2TnO+/tCo4wsn5PO/ziUZmUhS6b2m+7HUDnivKMpurzC37gmdqDqq7rvxAiS7Y:6onVGia9dqD5uO6lW
TLSH:	4654BF0AE855E917CB4DE07857630F7A27FB9FFEC42519A6313944236F9BA3B98C5200
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....^...../.....$...B.....@.....:..... .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4014b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5EDED518 [Tue Jun 9 00:17:28 2020 UTC]
TLS Callbacks:	0x401af0
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:	bed5688a4a2b5ea6984115b458755e90

Entrypoint Preview

Instruction
dec eax
sub esp, 28h
mov dword ptr [00048BB2h], 00000001h
call 00007FF6849E9B02h
call 00007FF6849E7F7Dh
nop
nop
dec eax
add esp, 28h
ret
nop
dec eax
sub esp, 28h
mov dword ptr [00048B92h], 00000000h
call 00007FF6849E9AE2h
call 00007FF6849E7F5Dh
nop
nop
dec eax
add esp, 28h
ret
nop
dec eax
sub esp, 18h
mov eax, dword ptr [00002B12h]
test eax, eax
jle 00007FF6849E82EAh
cmp dword ptr [00002B0Bh], 00000000h
jle 00007FF6849E82E1h
dec eax
mov edx, dword ptr [00049E42h]
dec eax
cwde
dec eax

Instruction
mov dword ptr [ecx+eax], edx
dec eax
arpl word ptr [00002AF5h], ax
dec eax
mov edx, dword ptr [00049E36h]
dec eax
mov dword ptr [ecx+eax], edx
dec eax
add esp, 18h
ret
push ebx
dec eax
sub esp, 00000500h
dec eax
mov ebx, dword ptr [edx+08h]
mov dword ptr [esp+60h], 00100002h
dec esp
mov dword ptr [esp+28h], eax
dec eax
lea edx, dword ptr [esp+30h]
dec eax
mov ecx, ebx
call dword ptr [00049E1Eh]
test eax, eax
dec esp
mov eax, dword ptr [esp+28h]
je 00007FF6849E82E6h
dec esp
mov dword ptr [esp+000000B0h], eax
dec eax
lea edx, dword ptr [esp+30h]
dec eax
mov ecx, ebx
call dword ptr [00049E5Fh]
test eax, eax
je 00007FF6849E82CCh
dec eax
mov ecx, ebx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4b000	0xb74	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x48000	0x2ac	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x4b2c0	0x270	.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	0x2400	0x2400	False	0.5936414930555556	data	6.129764070813093	IMAGE_SCN_CNT_CODE, 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	0x4000	0x42490	0x42600	False	0.6019781367702448	data	7.3657766804633775	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	0x47000	0x310	0x400	False	0.4541015625	data	4.1965610649629825	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	0x48000	0x2ac	0x400	False	0.3740234375	data	3.1610117624320244	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	0x49000	0x268	0x400	False	0.2587890625	data	2.847508632820401	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	0x4a000	0xa60	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
.idata	0x4b000	0xb74	0xc00	False	0.3372395833333333	data	4.3479190304641575	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	0x68	0x200	False	0.0703125	data	0.2694448386073115	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
.tls	0x4d000	0x48	0x200	False	0.052734375	data	0.21776995545804623	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

Imports

DLL	Import
ADVAPI32.dll	RegisterServiceCtrlHandlerA, SetServiceStatus, StartServiceCtrlDispatcherA
KERNEL32.dll	CloseHandle, ConnectNamedPipe, CreateFileA, CreateNamedPipeA, CreateProcessA, CreateThread, DeleteCriticalSection, EnterCriticalSection, ExitProcess, GetCurrentProcess, GetCurrentProcessId, GetCurrentThreadId, GetEnvironmentVariableA, GetLastError, GetModuleHandleA, GetProcAddress, GetStartupInfoA, GetSystemTimeAsFileTime, GetThreadContext, GetTickCount, InitializeCriticalSection, LeaveCriticalSection, LoadLibraryW, QueryPerformanceCounter, ReadFile, ResumeThread, RtlAddFunctionTable, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, SetThreadContext, SetUnhandledExceptionFilter, Sleep, TerminateProcess, TlsGetValue, UnhandledExceptionFilter, VirtualAllocEx, VirtualProtect, VirtualProtectEx, VirtualQuery, WriteFile, WriteProcessMemory
msvcrt.dll	__C_specific_handler, __dllonexit, __getmainargs, __initenv, __iob_func, __lconv_init, __set_app_type, __setusermatherr, _acmdln, _amsg_exit, _cexit, _fmode, _initterm, _lock, _onexit, _snprintf, _unlock, abort, calloc, exit, fprintf, free, fwrite, malloc, memcpy, signal, sprintf, strlen, strncmp, vfprintf

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: 8082-svc-x64.exe PID: 6108, Parent PID: 3528

General	
Target ID:	0
Start time:	16:08:59
Start date:	08/01/2023
Path:	C:\Users\user\Desktop\8082-svc-x64.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\8082-svc-x64.exe
Imagebase:	0x400000
File size:	289280 bytes
MD5 hash:	89BE3BE20CA0DCE73C12A5A015BCB9A5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly