ID: 780207
Sample Name: 8082-svc-x86.exe
Cookbook: default.jbs
Time: 16:02:38
Date: 08/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

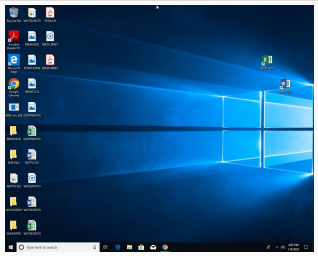
Windows Analysis Report

8082-svc-x86.exe

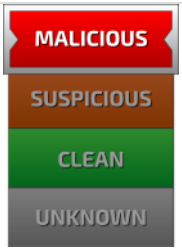
Overview

General Information

Sample Name:	8082-svc-x86.exe
Analysis ID:	780207
MD5:	8fc088eec229a6…
SHA1:	0043b6ba9f8edfd.
SHA256:	deeb89a16aa2b7.
Tags:	45139105143 exe opendir
Infos:	



Detection



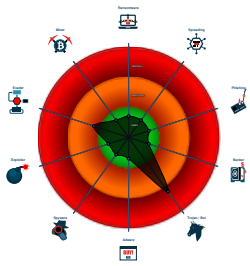
CobaltStrike

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…
- Uses 32bit PE files
- Yara signature match
- Antivirus or Machine Learning detec…
- Contains functionality to dynamicall…
- Found large amount of non-executed…
- Program does not show much activi…

Classification



Process Tree

- **System is w10x64**
- 8082-svc-x86.exe (PID: 3396 cmdline: C:\Users\user\Desktop\8082-svc-x86.exe MD5: 8FC088EEC229A693F2D754C67A2E506A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
8082-svc-x86.exe	CobaltStrike_Resources_Artifact32_v3_14_to_v4_x	Cobalt Strike\'s resources/artifact32{.dll,.exe,big.exe,big.dll,bigsvc.exe} signature for versions 3.14 to 4.x and resources/artifact32svc.exe for 3.14 to 4.x and resources/artifact32uac.dll for v3.14 and v4.0	gssincla@google.com	• 0xe07:$pushFmtStr: C7 44 24 28 5C 00 00 00 C7 44 24 24 65 00 00 00 C7 44 24 20 70 00 00 00 C7 44 24 1C 69 00 00 00 C7 44 24 18 70 00 00 00 F7 F1 C7 44 24 14 5C 00 00 00 C7 44 24 10 2E 00 00 00 C7 44 24 0C 5C 00 ... • 0x44a68:$fmtStr: %c%c%c%c%c%c%c%cMSSE-%d-server

Source	Rule	Description	Author	Strings
8082-svc-x86.exe	CobaltStrike_Resources_Artifact32svc_Exe_v3_1_v3_2_v3_14_and_v4_x	Cobalt Strike\'s resources/artifact32svc(big).exe signature for versions 3.1 and 3.2 (with overlap with v3.14 through v4.x)	gssincla@google.com	• 0xbc2:$decoderFunc: 89 C8 BF 04 00 00 00 99 F7 FF 8B 7D E0 8A 04 17 30
8082-svc-x86.exe	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.296319172.0000000000401000.00000020.00000001.01000000.00000003.sdmp	CobaltStrike_Resources_Artifact32svc_Exe_v3_1_v3_2_v3_14_and_v4_x	Cobalt Strike\'s resources/artifact32svc(big).exe signature for versions 3.1 and 3.2 (with overlap with v3.14 through v4.x)	gssincla@google.com	• 0x7c2:$decoderFunc: 89 C8 BF 04 00 00 00 99 F7 FF 8B 7D E0 8A 04 17 30
00000000.00000000.295977191.0000000000401000.00000020.00000001.01000000.00000003.sdmp	CobaltStrike_Resources_Artifact32svc_Exe_v3_1_v3_2_v3_14_and_v4_x	Cobalt Strike\'s resources/artifact32svc(big).exe signature for versions 3.1 and 3.2 (with overlap with v3.14 through v4.x)	gssincla@google.com	• 0x7c2:$decoderFunc: 89 C8 BF 04 00 00 00 99 F7 FF 8B 7D E0 8A 04 17 30

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.8082-svc-x86.exe.400000.0.unpack	CobaltStrike_Resources_Artifact32_v3_14_to_v4_x	Cobalt Strike\'s resources/artifact32{.dll,.exe,big.exe,big.dll,bigsvc.exe} signature for versions 3.14 to 4.x and resources/artifact32svc.exe for 3.14 to 4.x and resources/artifact32uac.dll for v3.14 and v4.0	gssincla@google.com	• 0xe07:$pushFmtStr: C7 44 24 28 5C 00 00 00 C7 44 24 24 65 00 00 00 C7 44 24 20 70 00 00 00 C7 44 24 1C 69 00 00 00 C7 44 24 18 70 00 00 00 F7 F1 C7 44 24 14 5C 00 00 00 C7 44 24 10 2E 00 00 00 C7 44 24 0C 5C 00 ... • 0x44a68:$fmtStr: %c%c%c%c%c%c%c%cMSSE-%d-server
0.2.8082-svc-x86.exe.400000.0.unpack	CobaltStrike_Resources_Artifact32svc_Exe_v3_1_v3_2_v3_14_and_v4_x	Cobalt Strike\'s resources/artifact32svc(big).exe signature for versions 3.1 and 3.2 (with overlap with v3.14 through v4.x)	gssincla@google.com	• 0xbc2:$decoderFunc: 89 C8 BF 04 00 00 00 99 F7 FF 8B 7D E0 8A 04 17 30
0.2.8082-svc-x86.exe.400000.0.unpack	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	Joe Security	
0.0.8082-svc-x86.exe.400000.0.unpack	CobaltStrike_Resources_Artifact32_v3_14_to_v4_x	Cobalt Strike\'s resources/artifact32{.dll,.exe,big.exe,big.dll,bigsvc.exe} signature for versions 3.14 to 4.x and resources/artifact32svc.exe for 3.14 to 4.x and resources/artifact32uac.dll for v3.14 and v4.0	gssincla@google.com	• 0xe07:$pushFmtStr: C7 44 24 28 5C 00 00 00 C7 44 24 24 65 00 00 00 C7 44 24 20 70 00 00 00 C7 44 24 1C 69 00 00 00 C7 44 24 18 70 00 00 00 F7 F1 C7 44 24 14 5C 00 00 00 C7 44 24 10 2E 00 00 00 C7 44 24 0C 5C 00 ... • 0x44a68:$fmtStr: %c%c%c%c%c%c%c%cMSSE-%d-server
0.0.8082-svc-x86.exe.400000.0.unpack	CobaltStrike_Resources_Artifact32svc_Exe_v3_1_v3_2_v3_14_and_v4_x	Cobalt Strike\'s resources/artifact32svc(big).exe signature for versions 3.1 and 3.2 (with overlap with v3.14 through v4.x)	gssincla@google.com	• 0xbc2:$decoderFunc: 89 C8 BF 04 00 00 00 99 F7 FF 8B 7D E0 8A 04 17 30

Click to see the 1 entries

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

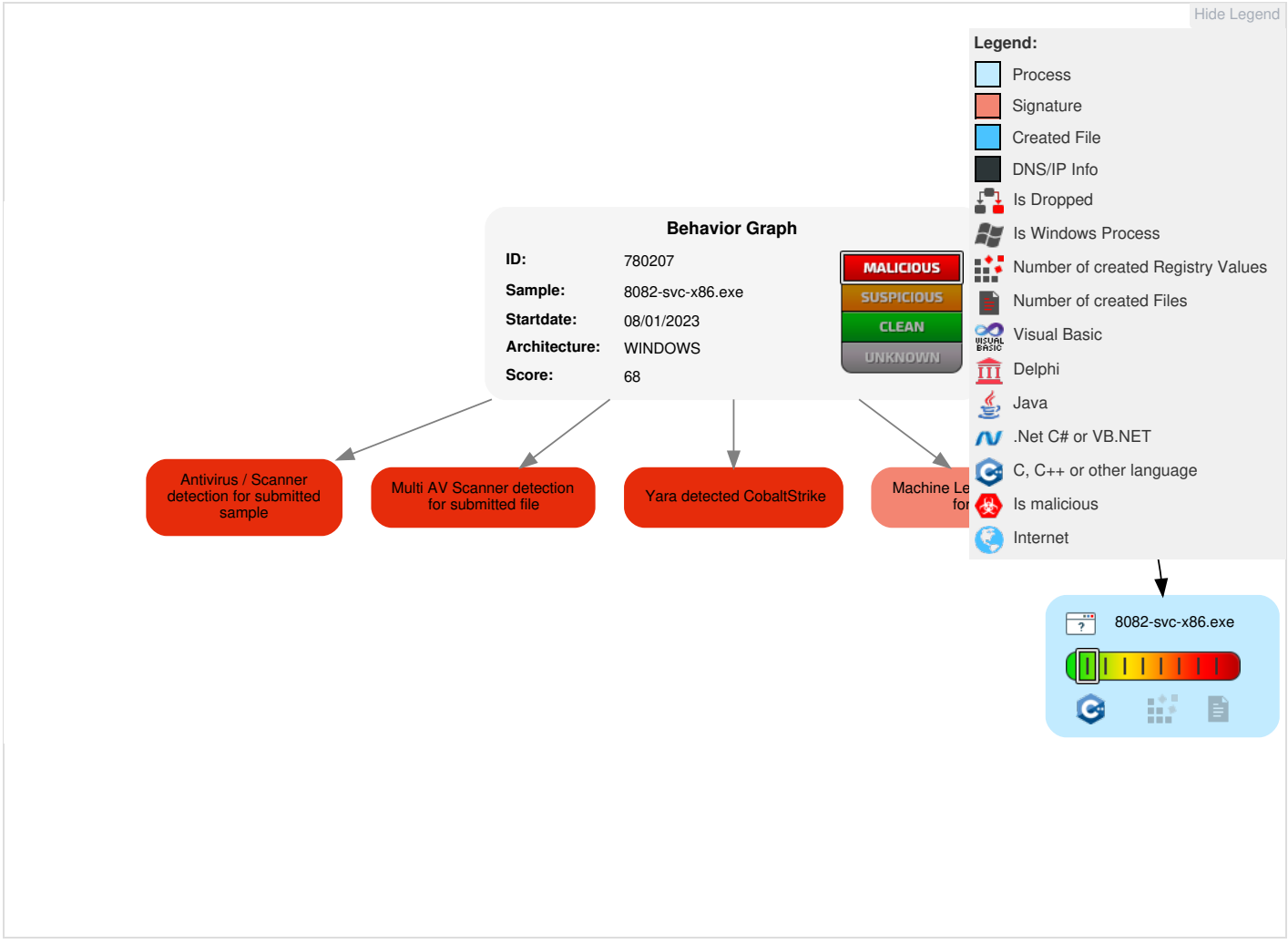
Remote Access Functionality

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	2 Service Execution	3 Windows Service	3 Windows Service	1 Software Packing	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	1 Native API	Boot or Logon Initialization Scripts	1 Process Injection	1 Process Injection	LSASS Memory	2 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

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-x86.exe	93%	ReversingLabs	Win32.Trojan.CobaltStrike	
8082-svc-x86.exe	100%	Avira	TR/Crypt.XPACK.Gen	
8082-svc-x86.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.8082-svc-x86.exe.400000.0.unpack	100%	Avira	TR/Hijacker.Gen		Download File
0.2.8082-svc-x86.exe.400000.0.unpack	100%	Avira	TR/Hijacker.Gen		Download File

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:	780207
Start date and time:	2023-01-08 16:02:38 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8082-svc-x86.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:	mal68.troj.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 41.8%) • Quality average: 28.8% • Quality standard deviation: 39.3%
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

Warnings

- VT rate limit hit for: 8082-svc-x86.exe

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) Intel 80386 (stripped to external PDB), for MS Windows
Entropy (8bit):	6.668168868781468
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	8082-svc-x86.exe
File size:	285696
MD5:	8fc088eec229a693f2d754c67a2e506a
SHA1:	0043b6ba9f8edfd83d00bbce364797d4c65b3b75
SHA256:	deeb89a16aa2b7b63504602de422f508c196b8be3289e57f3b9d74337d585425
SHA512:	8108f5d1e8dceea2276c89b5bf964e463fe466f25e115f80bb798f83e7619e7c4b40321e695b41570cc5136bc63b2fba90f1a34e4d05949d87ccf309a9d90ee8
SSDEEP:	6144:uQJAy6O5fo59McMv/0pWHV77hLB5FPfPfPfP8DRDNpGxnT:uQN6O5w8/XVXhLB5FPfPfPfP8D9NpgnT
TLSH:	D154CF87C75D0CA2F06A3A389EE77D676A19EBE1E30E0D4ED2BB27A50D06797441C701
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^..... ...X.....0....@.....g..... .....

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, 32BIT_MACHINE, DEBUG_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5EDED50D [Tue Jun 9 00:17:17 2020 UTC]
TLS Callbacks:	0x401bd0, 0x401b80
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:	de77f3139eaf74f1b255ab7be0b6605f

Entrypoint Preview

Instruction
sub esp, 0Ch
mov dword ptr [00447040h], 00000001h
call 00007F50D8FB4E23h
add esp, 0Ch
jmp 00007F50D8FB350Bh
lea esi, dword ptr [esi+00000000h]
sub esp, 0Ch
mov dword ptr [00447040h], 00000000h
call 00007F50D8FB4E03h
add esp, 0Ch
jmp 00007F50D8FB34EBh
nop
nop
nop
nop
nop
nop
push ebp
mov ebp, esp
sub esp, 18h
mov eax, dword ptr [00445420h]
test eax, eax
je 00007F50D8FB388Eh
mov dword ptr [esp], 00446020h
call dword ptr [004481CCh]
mov edx, 00000000h
sub esp, 04h
test eax, eax
je 00007F50D8FB3868h
mov dword ptr [esp+04h], 0044602Eh
mov dword ptr [esp], eax
call dword ptr [004481D0h]
sub esp, 08h
mov edx, eax
test edx, edx
je 00007F50D8FB385Bh
mov dword ptr [esp], 00445420h

Instruction
call edx
leave
ret
lea esi, dword ptr [esi+00h]
push ebp
mov ebp, esp
pop ebp
ret
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
push ebp
mov ebp, esp
sub esp, 10h
mov edx, dword ptr [0040300Ch]
mov eax, dword ptr [ebp+08h]
test edx, edx
jle 00007F50D8FB3872h
cmp dword ptr [00403010h], 00000000h
jle 00007F50D8FB3869h
mov ecx, dword ptr [004481CCh]
mov dword ptr [eax+edx], ecx
mov edx, dword ptr [000000D0h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x48000	0x8a0	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
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	0x4a000	0x18	.tls
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x48180	0x130	.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1fd4	0x2000	False	0.563720703125	data	5.933774570860191	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	0x42424	0x42600	False	0.5399489465630886	data	6.670005359968773	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
.rdata	0x46000	0x324	0x400	False	0.4970703125	data	4.535472821564213	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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.bss	0x47000	0x47c	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
.idata	0x48000	0x8a0	0xa00	False	0.373046875	data	4.745754334582236	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	0x49000	0x34	0x200	False	0.068359375	Matlab v4 mat-file (little endian) \`\035@, numeric, rows 4198416, columns 0	0.2655385886073115	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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.tls	0x4a000	0x20	0x200	False	0.05078125	data	0.22482003450968063	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

Imports

DLL	Import
ADVAPI32.dll	RegisterServiceCtrlHandlerA, SetServiceStatus, StartServiceCtrlDispatcherA
KERNEL32.dll	CloseHandle, ConnectNamedPipe, CreateFileA, CreateNamedPipeA, CreateProcessA, CreateThread, DeleteCriticalSection, EnterCriticalSection, ExitProcess, FreeLibrary, GetCurrentProcess, GetCurrentProcessId, GetCurrentThreadId, GetEnvironmentVariableA, GetLastError, GetModuleHandleA, GetProcAddress, GetStartupInfoA, GetSystemTimeAsFileTime, GetThreadContext, GetTickCount, InitializeCriticalSection, LeaveCriticalSection, LoadLibraryA, LoadLibraryW, QueryPerformanceCounter, ReadFile, ResumeThread, SetThreadContext, SetUnhandledExceptionFilter, Sleep, TerminateProcess, TlsGetValue, UnhandledExceptionFilter, VirtualAllocEx, VirtualProtect, VirtualProtectEx, VirtualQuery, WriteFile, WriteProcessMemory
msvcrt.dll	__dllonexit, __getmainargs, __initenv, __lconv_init, __set_app_type, __setusermatherr, _acmdln, _amsg_exit, _cexit, _fmode, _initterm, _iob, _lock, _onexit, _snprintf, _unlock, _winmajor, 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-x86.exe PID: **3396**, Parent PID: **3324**

General

Target ID:	0
Start time:	16:03:33
Start date:	08/01/2023
Path:	C:\Users\user\Desktop\8082-svc-x86.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\8082-svc-x86.exe
Imagebase:	0x400000
File size:	285696 bytes

MD5 hash:	8FC088EEC229A693F2D754C67A2E506A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: CobaltStrike_Resources_Artifact32svc_Exe_v3_1_v3_2_v3_14_and_v4_x, Description: Cobalt Strike\'s resources/artifact32svc(big).exe signature for versions 3.1 and 3.2 (with overlap with v3.14 through v4.x), Source: 00000000.00000002.296319172.0000000000401000.00000020.00000001.01000000.00000003.sdmp, Author: gssincla@google.com • Rule: CobaltStrike_Resources_Artifact32svc_Exe_v3_1_v3_2_v3_14_and_v4_x, Description: Cobalt Strike\'s resources/artifact32svc(big).exe signature for versions 3.1 and 3.2 (with overlap with v3.14 through v4.x), Source: 00000000.00000000.295977191.0000000000401000.00000020.00000001.01000000.00000003.sdmp, Author: gssincla@google.com
Reputation:	low

Disassembly

No disassembly