ID: 708236
Sample Name: AIO.exe
Cookbook: default.jbs
Time: 07:54:04
Date: 23/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

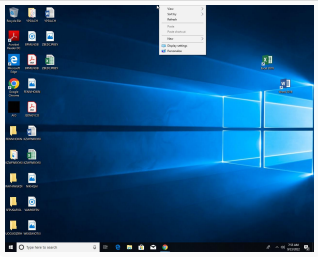
Windows Analysis Report

AIO.exe

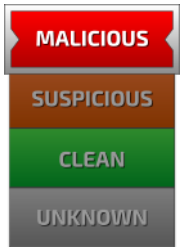
Overview

General Information

Sample Name:	AIO.exe
Analysis ID:	708236
MD5:	9c1181704c48d6..
SHA1:	ada9921624f322..
SHA256:	44ea8ae385d7d9.
Tags:	dropped exe morpheus
Infos:	



Detection

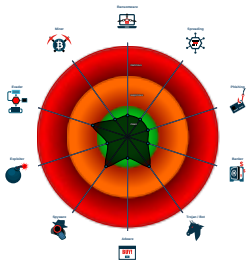


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- PE file contains more sections than…
- Potential time zone aware malware
- Installs a raw input device (often for…
- Program does not show much activi…
- Detected TCP or UDP traffic on non…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- AIO.exe (PID: 4572 cmdline: "C:\Users\user\Desktop\AIO.exe" MD5: 9C1181704C48D62DE14C5F682C4F5D5E)
  - conhost.exe (PID: 4536 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **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

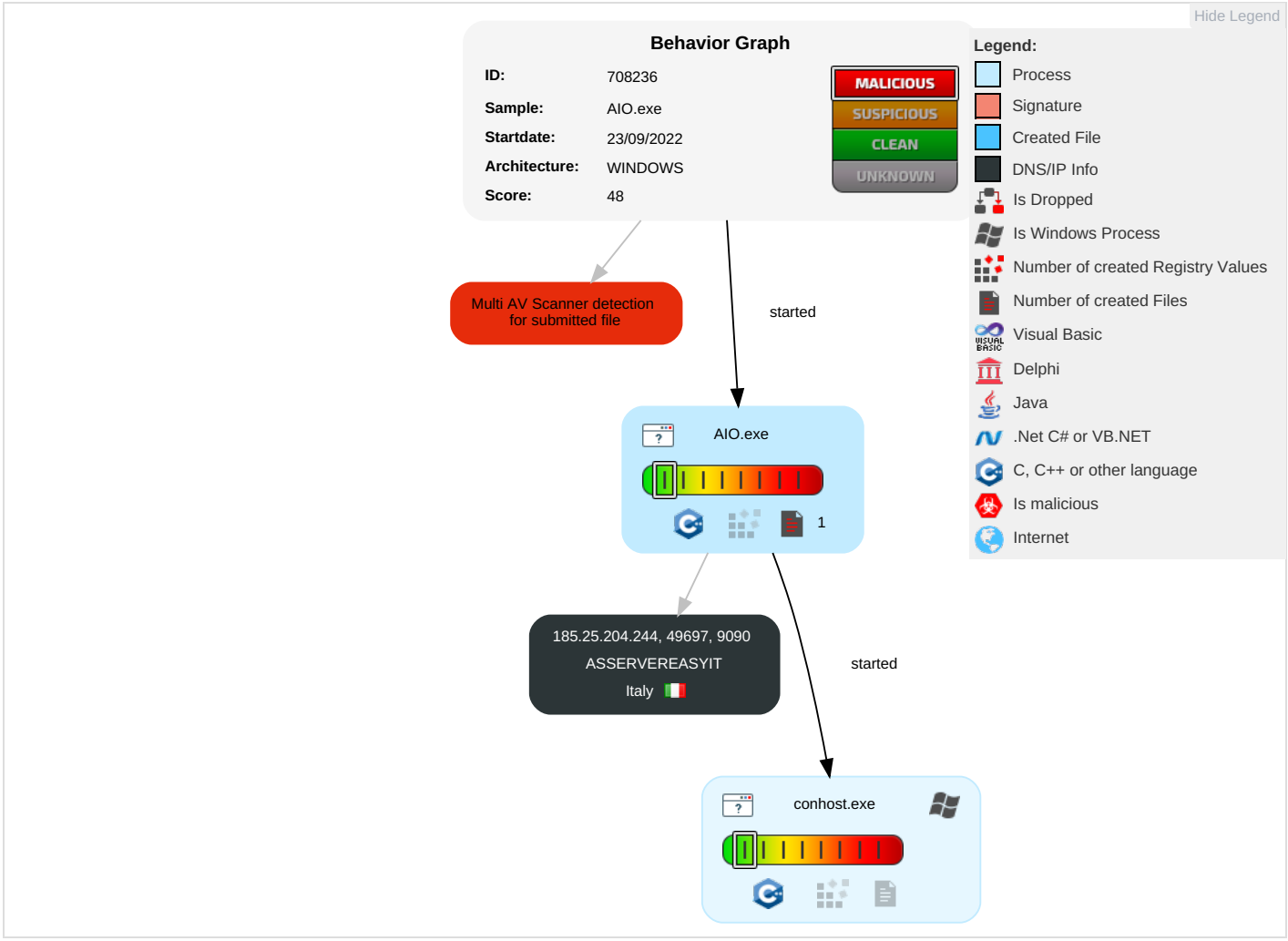
AV Detection

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	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	1 Process Injection	1 Software Packing	1 1 Input Capture	1 System Time Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Non-Standard Port	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 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 System Information 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

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
AIO.exe	0%	ReversingLabs		
AIO.exe	7%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

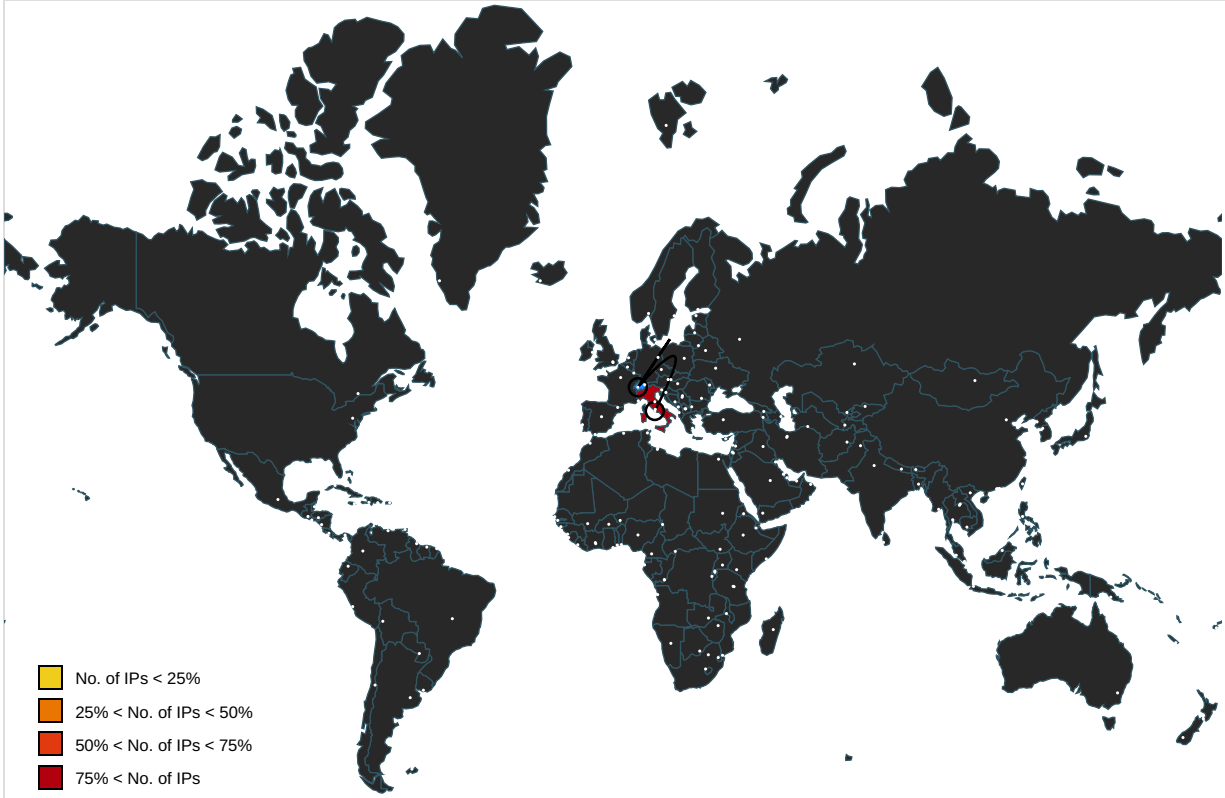
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.25.204.244	unknown	Italy		60798	ASSERVEREASYIT	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	708236
Start date and time:	2022-09-23 07:54:04 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AIO.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:	2
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:	mal48.winEXE@2/0@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 100%) • Quality average: 75.8% • Quality standard deviation: 24.4%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Execution Graph export aborted for target AIO.exe, PID 4572 because there are no executed function
- Not all processes where analyzed, report is missing behavior information

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 (console) x86-64 (stripped to external PDB), for MS Windows

Entropy (8bit):	6.745466282178942
TrID:	• Win64 Executable (generic) (12005/4) 74.95% • Generic Win/DOS Executable (2004/3) 12.51% • DOS Executable Generic (2002/1) 12.50% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.04%
File name:	AIO.exe
File size:	4077056
MD5:	9c1181704c48d62de14c5f682c4f5d5e
SHA1:	ada9921624f3225054745643b0d4504939efd1aa
SHA256:	44ea8ae385d7d95d4f0b9c6969c0d0ca55acfd996e97236c0ae04eb2b4b2d623
SHA512:	42756ad205c3e99b3a9c0eda1dbaa80923b714ab56e9ab987917e6a41b52571f6965254ee9dc486c2e444d080554956ad4059ca5695d36de53d92201583e4f05
SSDEEP:	49152:g8CBJF3V3kt1rb/TLvO90d7HjmAFd4A64nsfJr3J66/XUg/UljSVZgxxkq1QarAU:U3WeIAnba7tKtzQ
TLSH:	45164C03784758A4C4B993BD8565C2D576337B84EB3227D32A20A6799A72FC34E3E3D4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....7.....".....Y.....@.....D.....`... .....

File Icon

Icon Hash:	20000a0021000480

Static PE Info

General

Entrypoint:	0x465900
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	1
File Version Major:	6
File Version Minor:	1
Subsystem Version Major:	6
Subsystem Version Minor:	1
Import Hash:	9cbefe68f395e67356e2a5d8d1b285c0

Entrypoint Preview

Instruction
jmp 00007F4E18D1BB00h
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
pushfd
cld
dec eax
sub esp, 000000E0h
dec eax
mov dword ptr [esp], edi
dec eax
mov dword ptr [esp+08h], esi
dec eax
mov dword ptr [esp+10h], ebp
dec eax
mov dword ptr [esp+18h], ebx
dec esp
mov dword ptr [esp+20h], esp
dec esp
mov dword ptr [esp+28h], ebp
dec esp
mov dword ptr [esp+30h], esi
dec esp
mov dword ptr [esp+38h], edi
movups dqword ptr [esp+40h], xmm6
movups dqword ptr [esp+50h], xmm7
inc esp
movups dqword ptr [esp+60h], xmm0
inc esp
movups dqword ptr [esp+70h], xmm1
inc esp
movups dqword ptr [esp+00000080h], xmm2
inc esp
movups dqword ptr [esp+00000090h], xmm3
inc esp
movups dqword ptr [esp+000000A0h], xmm4
inc esp
movups dqword ptr [esp+000000B0h], xmm5
inc esp
movups dqword ptr [esp+000000C0h], xmm6
inc esp
movups dqword ptr [esp+000000D0h], xmm7
dec eax
sub esp, 30h
dec ecx
mov edi, eax
dec eax
mov edx, dword ptr [00000028h]
dec eax
cmp edx, 00000000h
jne 00007F4E18D1F80Eh

Instruction
dec eax
mov eax, 00000000h
jmp 00007F4E18D1F885h
dec eax
mov edx, dword ptr [edx+00000000h]
dec eax
cmp edx, 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3dc000	0x47c	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x414000	0x33170	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3dd000	0x5580	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x262180	0x140	.data
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	0x12e80d	0x12ea00	False	0.44155953118546054	data	6.13492107696467	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x130000	0x131988	0x131a00	False	0.40479933537832313	data	5.362616895297891	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x262000	0x777c8	0x1ba00	False	0.37963093891402716	data	4.4437373554282775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
/4	0x2da000	0x127	0x200	False	0.6171875	data	5.097874074212899	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/19	0x2db000	0x36747	0x36800	False	0.9970344753440367	data	7.994232193058085	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/32	0x312000	0xafd1	0xb000	False	0.9973810369318182	data	7.939671694657932	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/46	0x31d000	0x30	0x200	False	0.103515625	data	0.8556848540171443	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/65	0x31e000	0x663f5	0x66400	False	0.9984575565403423	data	7.996921212792595	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/78	0x385000	0x43014	0x43200	False	0.9842695239757915	data	7.992613233207576	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/90	0x3c9000	0x122ad	0x12400	False	0.9734321489726028	data	7.801216600325401	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.idata	0x3dc000	0x47c	0x600	False	0.333984375	data	3.572216214307509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x3dd000	0x5580	0x5600	False	0.32562681686046513	data	5.4368326520791035	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.symtab	0x3e3000	0x30c15	0x30e00	False	0.24586397058823528	data	5.2949299515861545	IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x414000	0x33170	0x33200	False	0.029206143031784843	data	2.383138623744508	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4140e8	0x32c38	data		
RT_GROUP_ICON	0x446d20	0x14	data		
RT_MANIFEST	0x446d38	0x434	XML 1.0 document, ASCII text	English	United States

Imports

DLL	Import
kernel32.dll	WriteFile, WriteConsoleW, WaitForMultipleObjects, WaitForSingleObject, VirtualQuery, VirtualFree, VirtualAlloc, SwitchToThread, SuspendThread, SetWaitableTimer, SetUnhandledExceptionFilter, SetProcessPriorityBoost, SetEvent, SetErrorMode, SetConsoleCtrlHandler, ResumeThread, PostQueuedCompletionStatus, LoadLibraryA, LoadLibraryW, SetThreadContext, GetThreadContext, GetSystemInfo, GetSystemDirectoryA, GetStdHandle, GetQueuedCompletionStatusEx, GetProcessAffinityMask, GetProcAddress, GetEnvironmentStringsW, GetConsoleMode, FreeEnvironmentStringsW, ExitProcess, DuplicateHandle, CreateWaitableTimerExW, CreateThread, CreateIoCompletionPort, CreateFileA, CreateEventA, CloseHandle, AddVectoredExceptionHandler

Possible Origin

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

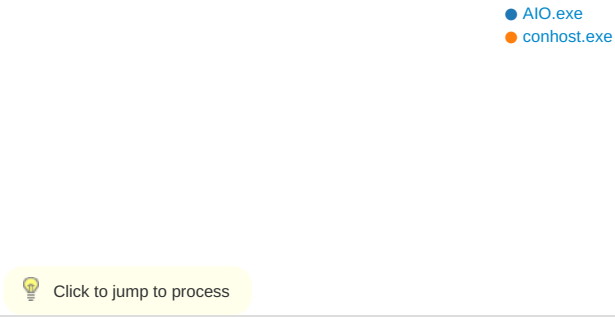
Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 07:55:03.822855949 CEST	49697	9090	192.168.2.5	185.25.204.244
Sep 23, 2022 07:55:03.848623037 CEST	9090	49697	185.25.204.244	192.168.2.5
Sep 23, 2022 07:55:04.354446888 CEST	49697	9090	192.168.2.5	185.25.204.244
Sep 23, 2022 07:55:04.380914927 CEST	9090	49697	185.25.204.244	192.168.2.5
Sep 23, 2022 07:55:04.885790110 CEST	49697	9090	192.168.2.5	185.25.204.244
Sep 23, 2022 07:55:04.911514044 CEST	9090	49697	185.25.204.244	192.168.2.5

Statistics

Behavior



System Behavior

Analysis Process: AIO.exe PID: **4572**, Parent PID: **5856**

General

Target ID:	0
Start time:	07:55:02
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\AIO.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\AIO.exe"
Imagebase:	0x1a0000
File size:	4077056 bytes
MD5 hash:	9C1181704C48D62DE14C5F682C4F5D5E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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: **4536**, Parent PID: **4572**

General

Target ID:	1
Start time:	07:55:03
Start date:	23/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly