

JOESandbox Cloud BASIC



**ID:** 708237

**Sample Name:**

qOiBFerq7X.exe

**Cookbook:** default.jbs

**Time:** 07:54:20

**Date:** 23/09/2022

**Version:** 36.0.0 Rainbow Opal

# Table of Contents

Table of Contents	2
Windows Analysis Report qOiBFerq7X.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Sigma Signatures	3
Snort Signatures	3
Joe Sandbox Signatures	4
AV Detection	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
World Map of Contacted IPs	7
Public IPs	7
General Information	7
Warnings	8
Simulations	8
Behavior and APIs	8
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASNs	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	9
Static PE Info	9
General	9
Entrypoint Preview	9
Data Directories	11
Sections	11
Resources	13
Imports	13
Possible Origin	13
Network Behavior	14
TCP Packets	14
Statistics	14
Behavior	14
System Behavior	14
Analysis Process: qOiBFerq7X.exePID: 2512, Parent PID: 5692	14
General	14
File Activities	14
Analysis Process: conhost.exePID: 5384, Parent PID: 2512	15
General	15
Disassembly	15

# Windows Analysis Report

qOiBFerq7X.exe

## Overview

### General Information

Sample Name:	qOiBFerq7X.exe
Analysis ID:	708237
MD5:	e350cbab3b64e8..
SHA1:	719c508f86b5e0..
SHA256:	b25478bd070ab2..
Tags:	185-25-204-244Servereasy... exe Morpheus
Infos:	

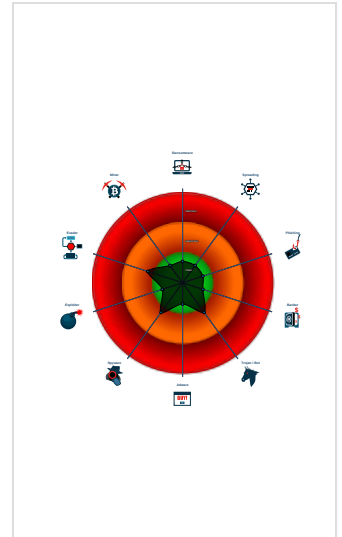
### Detection

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
- qOiBFerq7X.exe (PID: 2512 cmdline: "C:\Users\user\Desktop\qOiBFerq7X.exe" MD5: E350CBAB3B64E8F7E523619721392D21)
  - conhost.exe (PID: 5384 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

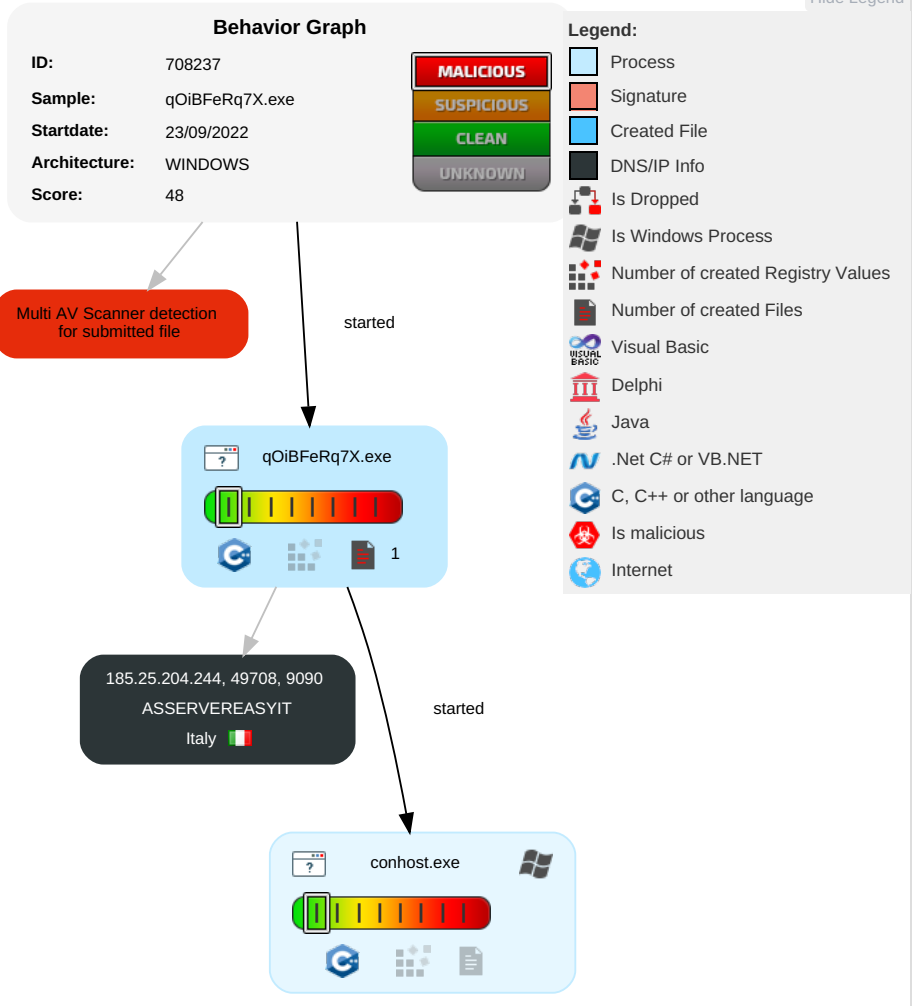


Multi AV Scanner detection for submitted file

## 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

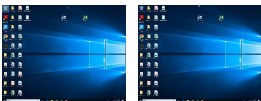
## Behavior Graph



## 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
qOiBFerq7X.exe	0%	ReversingLabs		
qOiBFerq7X.exe	7%	Virustotal		<a href="#">Browse</a>


### Dropped Files

 No Antivirus matches


### Unpacked PE Files

 No Antivirus matches

### Domains

 No Antivirus matches

### URLs

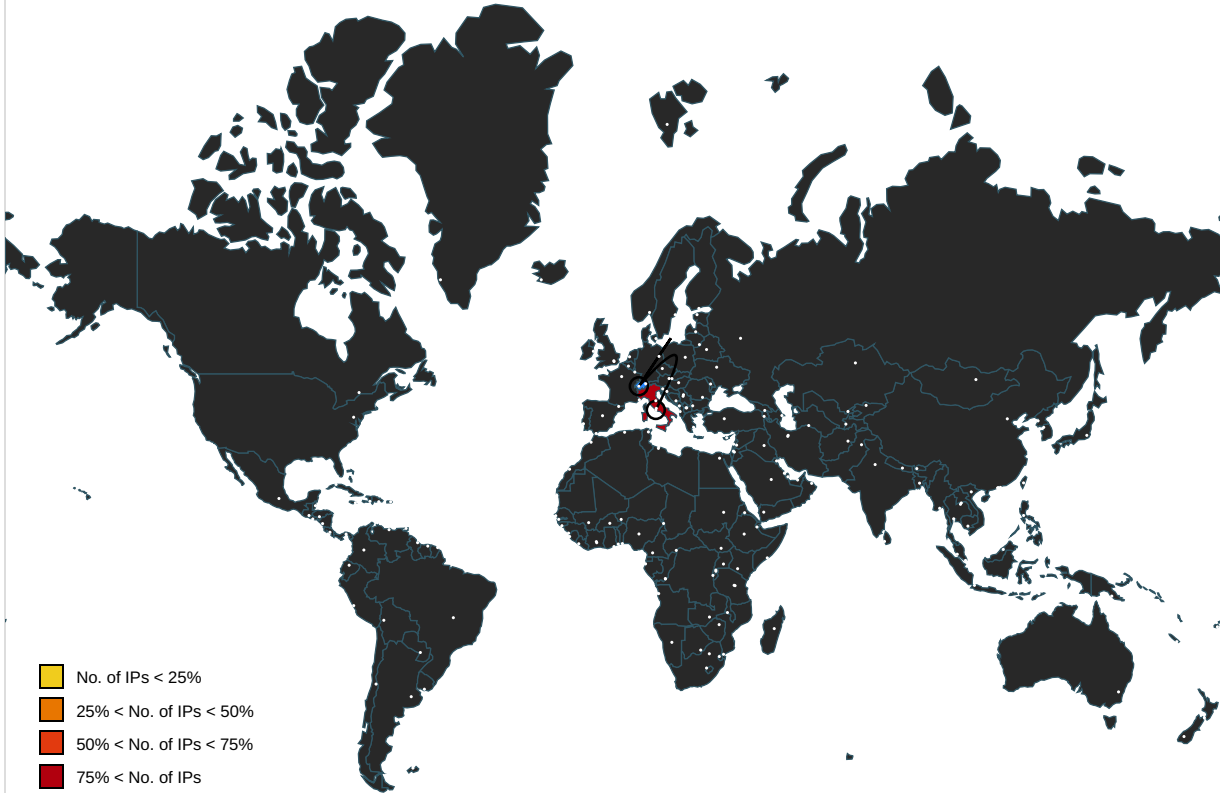
 No Antivirus matches

## 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:	708237
Start date and time:	2022-09-23 07:54:20 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qOIBFeRq7X.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:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>


Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.winEXE@2/0@0/1
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"> <li>• Successful, ratio: 100% (good quality ratio 100%)</li> <li>• Quality average: 75.8%</li> <li>• Quality standard deviation: 24.4%</li> </ul>
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none"> <li>• Found application associated with file extension: .exe</li> <li>• Stop behavior analysis, all processes terminated</li> </ul>

## Warnings

- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Execution Graph export aborted for target qOIBFeRq7X.exe, PID 2512 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





Instruction
int3
int3
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

Instruction
jne 00007F7424AEC0FEh
dec eax
mov eax, 00000000h
jmp 00007F7424AEC175h
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	0x3dd000	0x47c	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x415000	0x42560	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3de000	0x55a8	.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	0x264180	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	0x12f2ad	0x12f400	False	0.44155438478977743	data	6.134186837146027	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x131000	0x132548	0x132600	False	0.40453513871889024	data	5.359995809128577	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x264000	0x777c8	0x1ba00	False	0.37967512726244346	data	4.447089029507736	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
/4	0x2dc000	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	0x2dd000	0x36838	0x36a00	False	0.9957361985125858	data	7.994836896991751	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES , IMAGE_SCN_ALIGN_64BYTES , IMAGE_SCN_ALIGN_256BYT ES, IMAGE_SCN_ALIGN_1024BYT ES, IMAGE_SCN_ALIGN_4096BYT ES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARD ABLE, IMAGE_SCN_MEM_READ
/32	0x314000	0xafee	0xb000	False	0.9980690696022727	data	7.939302201607372	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES , IMAGE_SCN_ALIGN_64BYTES , IMAGE_SCN_ALIGN_256BYT ES, IMAGE_SCN_ALIGN_1024BYT ES, IMAGE_SCN_ALIGN_4096BYT ES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARD ABLE, IMAGE_SCN_MEM_READ
/46	0x31f000	0x30	0x200	False	0.103515625	data	0.8556848540171443	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES , IMAGE_SCN_ALIGN_64BYTES , IMAGE_SCN_ALIGN_256BYT ES, IMAGE_SCN_ALIGN_1024BYT ES, IMAGE_SCN_ALIGN_4096BYT ES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARD ABLE, IMAGE_SCN_MEM_READ
/65	0x320000	0x665c7	0x66600	False	0.9984093597374848	data	7.997091496748059	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES , IMAGE_SCN_ALIGN_64BYTES , IMAGE_SCN_ALIGN_256BYT ES, IMAGE_SCN_ALIGN_1024BYT ES, IMAGE_SCN_ALIGN_4096BYT ES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARD ABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/78	0x387000	0x42e51	0x43000	False	0.9844478777985075	data	7.992917864787682	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	0x3ca000	0x122d6	0x12400	False	0.974703017979452	data	7.801272414782094	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	0x3dd000	0x47c	0x600	False	0.3333333333333333	data	3.569267435002183	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x3de000	0x55a8	0x5600	False	0.32639898255813954	data	5.435661439949003	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.symtab	0x3e4000	0x30cee	0x30e00	False	0.2462735773657289	data	5.299414661215501	IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x415000	0x42560	0x42600	False	0.03361508356873823	data	1.4857977616407179	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ


## Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4150e8	0x42028	data		
RT_GROUP_ICON	0x457110	0x14	data		
RT_MANIFEST	0x457128	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 07:55:19.176639080 CEST	49708	9090	192.168.2.6	185.25.204.244
Sep 23, 2022 07:55:19.202127934 CEST	9090	49708	185.25.204.244	192.168.2.6
Sep 23, 2022 07:55:19.708651066 CEST	49708	9090	192.168.2.6	185.25.204.244
Sep 23, 2022 07:55:19.734209061 CEST	9090	49708	185.25.204.244	192.168.2.6
Sep 23, 2022 07:55:20.240000963 CEST	49708	9090	192.168.2.6	185.25.204.244
Sep 23, 2022 07:55:20.265697956 CEST	9090	49708	185.25.204.244	192.168.2.6

## Statistics

### Behavior

● qOIBFeRq7X.exe  
● conhost.exe

 Click to jump to process

## System Behavior

**Analysis Process: qOIBFeRq7X.exe** PID: 2512, Parent PID: 5692

### General

Target ID:	0
Start time:	07:55:17
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\qOIBFeRq7X.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\qOIBFeRq7X.exe"
Imagebase:	0xf20000
File size:	4145664 bytes
MD5 hash:	E350CBAB3B64E8F7E523619721392D21
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: 5384, Parent PID: 2512

#### General

Target ID:	1
Start time:	07:55:18
Start date:	23/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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