
**ID:** 708239
**Sample Name:** 67AzzNNioP.exe
**Cookbook:** default.jbs
**Time:** 07:55:46
**Date:** 23/09/2022
**Version:** 36.0.0 Rainbow Opal

# Table of Contents

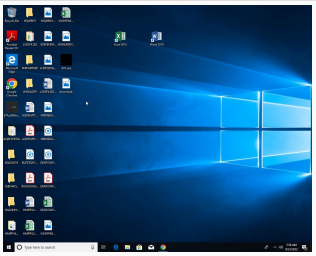
# Windows Analysis Report

## 67AzzNNioP.exe

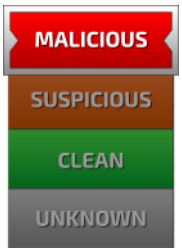
## Overview

### General Information

| | |
|---|---|
| Sample Name: | 67AzzNNioP.exe |
| Analysis ID: | 708239 |
| MD5: | f44d0bd72d1433.. |
| SHA1: | dbe17733409126. |
| SHA256: | 8f8cb5930100e8.. |
| Tags: | 185-25-204-244Servereasy… exe morpheus |
| Infos: | |



### Detection

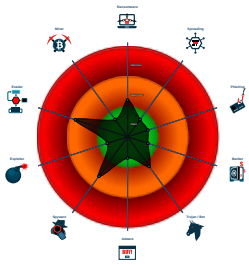



| | |
|---|---|
| Score: | 56 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Multi AV Scanner detection for subm…
- Multi AV Scanner detection for drop…
- Uses 32bit PE files
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query local…
- Uses code obfuscation techniques (…
- Found evasive API chain (date chec…
- PE file contains sections with non-s…
- Detected potential crypto function
- Contains functionality to query CPU…
- Found potential string decryption / a…

### Classification



## Process Tree

- **System is w10x64**
- 67AzzNNioP.exe (PID: 3932 cmdline: "C:\Users\user\Desktop\67AzzNNioP.exe" MD5: F44D0BD72D14338B655A6D4457419493)
  - AIO.exe (PID: 5576 cmdline: "C:\Users\user\Desktop\AIO.exe" MD5: 9C1181704C48D62DE14C5F682C4F5D5E)
    - conhost.exe (PID: 3776 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

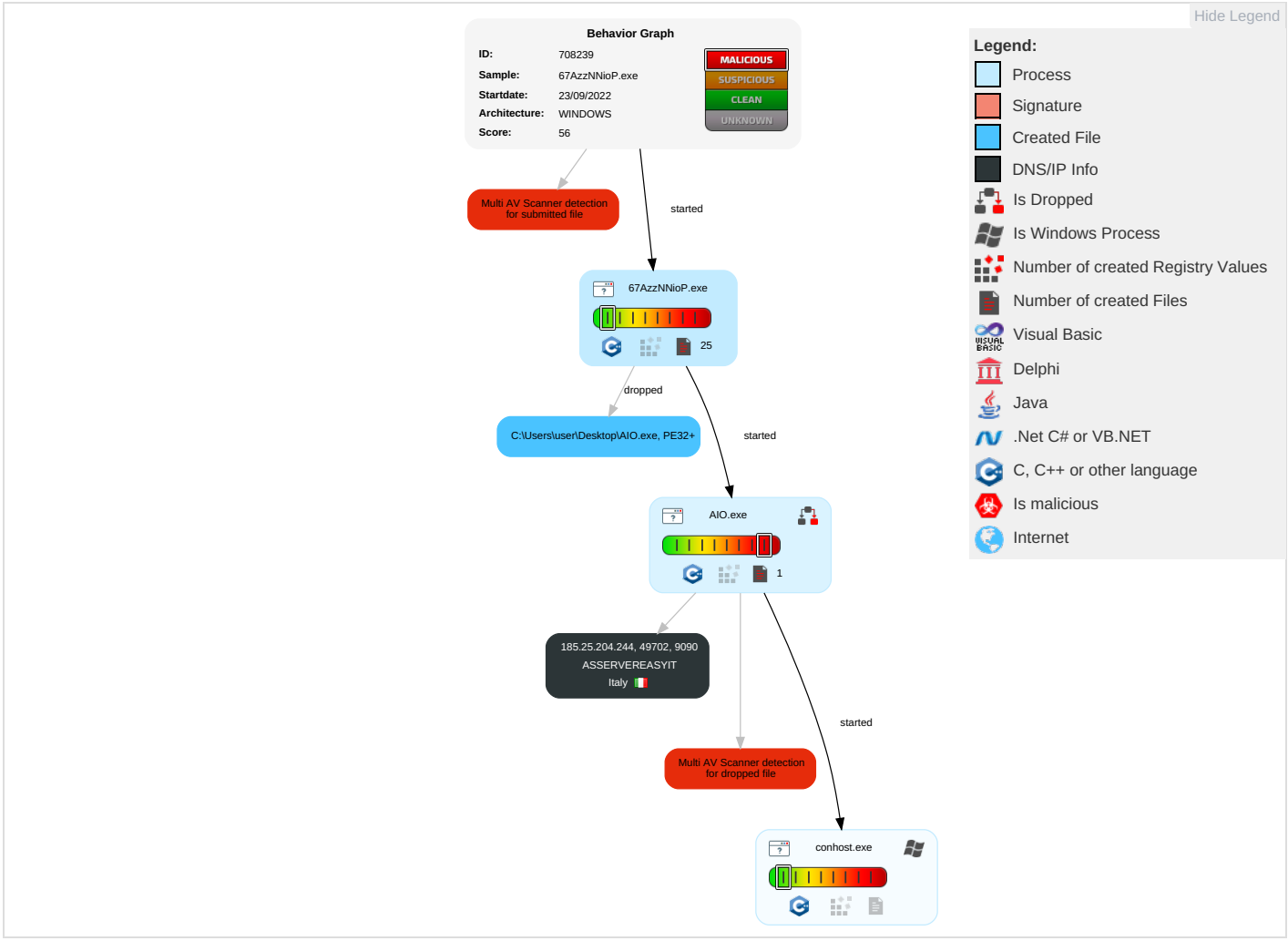
Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped 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 | 1 DLL Side-Loading | 1 1 Process Injection | 1 Masquerading | 1 1 Input Capture | 1 System Time Discovery | Remote Services | 1 Email Collection | Exfiltration Over Other Network Medium | 1 Encrypted Channel | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | 1 Native API | Boot or Logon Initialization Scripts | 1 DLL Side-Loading | 1 Virtualization/Sandbox Evasion | LSASS Memory | 1 2 1 Security Software Discovery | Remote Desktop Protocol | 1 1 Input Capture | Exfiltration Over Bluetooth | 1 Non-Standard Port | 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 Process Injection | Security Account Manager | 1 Virtualization/Sandbox Evasion | SMB/Windows Admin Shares | 1 Archive Collected Data | 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) | 1 Deobfuscate/Decode Files or Information | NTDS | 2 File and Directory 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 | 2 Obfuscated Files or Information | LSA Secrets | 3 4 System Information Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | | Manipulate App Store Rankings or Ratings |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | 2 Software Packing | Cached Domain Credentials | System Owner/User Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service | | Abuse Accessibility Features |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | 1 DLL Side-Loading | DCSync | Network Sniffing | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-Fi Access Points | | Data Encrypted for Impact |

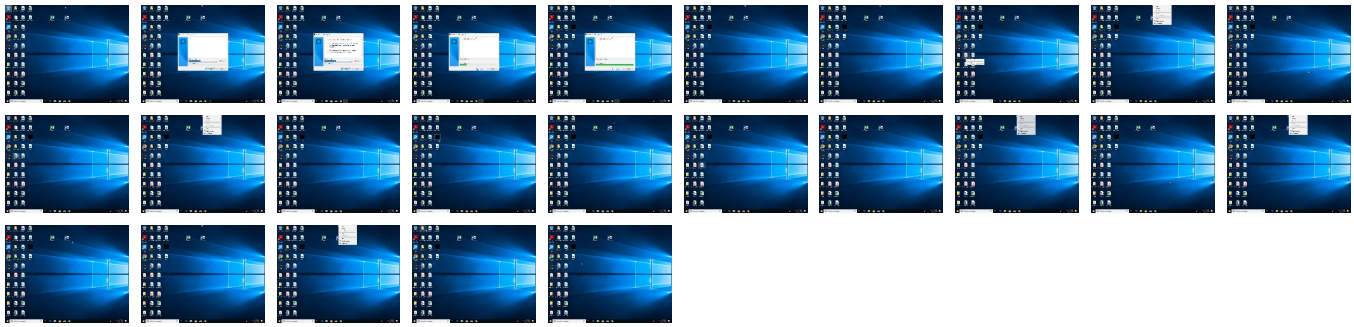
## Behavior Graph




# 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 |
|---|---|---|---|---|
| 67AzzNNioP.exe | 28% | ReversingLabs | Win32.Trojan.Generic | |
| 67AzzNNioP.exe | 23% | Virustotal | | Browse |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

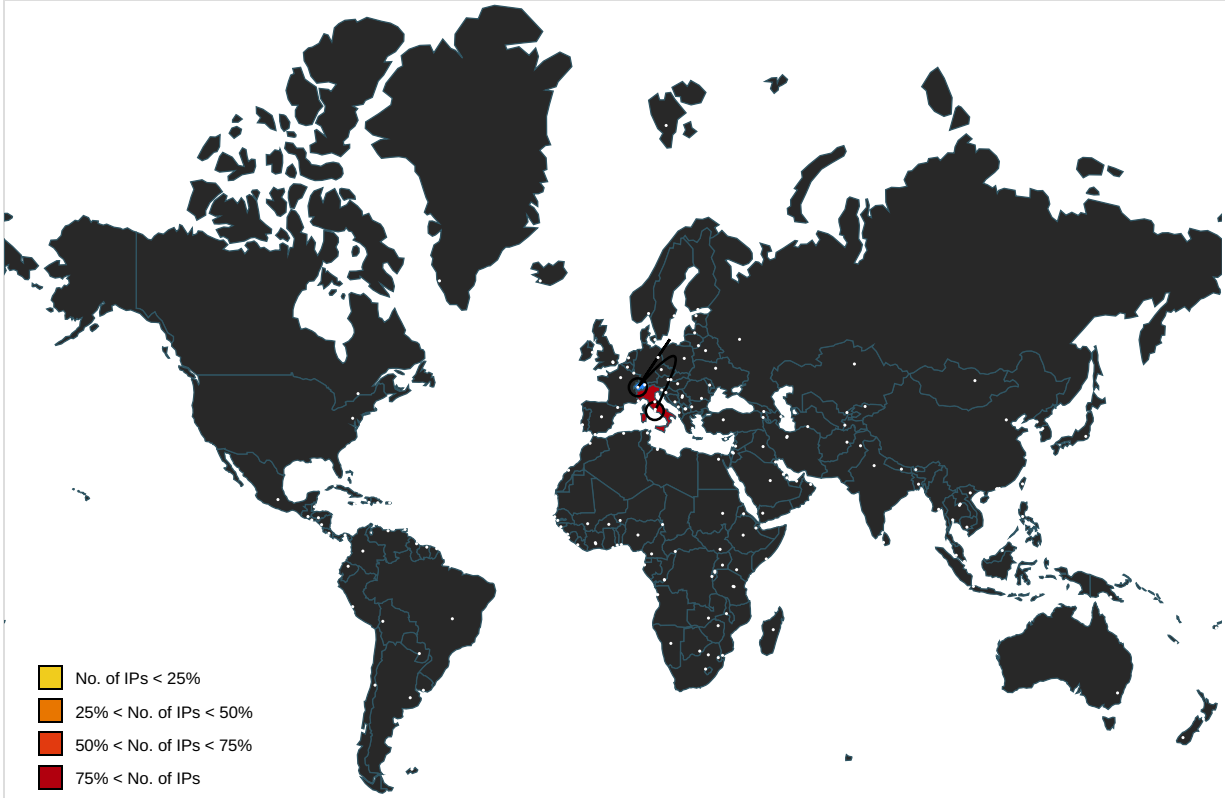
No Antivirus matches

# 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: | 708239 |
| Start date and time: | 2022-09-23 07:55:46 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 32s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 67AzzNNioP.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: | 14 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal56.winEXE@4/2@0/1 |
| EGA Information: | • Successful, ratio: 50% |
| HDC Information: | • Successful, ratio: 99.7% (good quality ratio 93.3%)<br>• Quality average: 79.8%<br>• Quality standard deviation: 28.5% |
| HCA Information: | • Successful, ratio: 98%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .exe |

### Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- Execution Graph export aborted for target AIO.exe, PID 5576 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

## 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

**C:\Users\user\Desktop\AIO.exe**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\67AzzNNioP.exe |
| File Type: | PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows |
| Category: | dropped |
| Size (bytes): | 4077056 |
| Entropy (8bit): | 6.745466282178942 |
| Encrypted: | false |
| SSDEEP: | 49152:g8CBJF3V3kt1rb/TLvO90d7HjmAFd4A64nsfJr3J66/XUg/UljSVZgxxkq1QarAU:U3WeIAnba7tKtzQ |
| MD5: | 9C1181704C48D62DE14C5F682C4F5D5E |
| SHA1: | ADA9921624F3225054745643B0D4504939EFD1AA |
| SHA-256: | 44EA8AE385D7D95D4F0B9C6969C0D0CA55ACFD996E97236C0AE04EB2B4B2D623 |
| SHA-512: | 42756AD205C3E99B3A9C0EDA1DBAA80923B714AB56E9AB987917E6A41B52571F6965254EE9DC486C2E444D080554956AD4059CA5695D36DE53D92201583E4F0 |
| Malicious: | false |
| Reputation: | low |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....7.....".....Y.....@.....D.....<br>..`... .....=.\|....@A.p1.....=..U.....!&.@.....text.....<br>.....@..@.data....w... &.....&.....@../4.....'....-.....'.....@..B/19....Gg....-..h....'.....@..B/32..... 1.....+.....@..B/46....0....1.....+.....@..B/65.....<br>c....1..d....+.....@..B/78.....0...P8..2...D2.....@..B/90.....".....<..$...v6.....@..B.idata..\|.....=.....7.....@....reloc...U....=..V....7.....@..B.symtab.....0>....<br>...7.....B.rsrc...p1...@A..2....;.....@..@..... |

**C:\Users\user\Desktop\download.jpg**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\67AzzNNioP.exe |
| File Type: | JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 236x213, frames 3 |
| Category: | dropped |
| Size (bytes): | 906 |
| Entropy (8bit): | 6.259833359660227 |
| Encrypted: | false |
| SSDEEP: | 12:baXYMFrUiV6ine/30TA4MJ8hJG1XzWFSXvEjHT7t5ct+pbV8H2b1/VgsKojP4tQ2:MFrFc/30Tg8h81WEMjHTpGkGH2ZVgIj+ |
| MD5: | F6E32B18FEB903C735501B2B188B9310 |
| SHA1: | A3F87DC9655C91FA406BFB6346288FB3A0FCCDE7 |
| SHA-256: | 71DFD33F3C6E255DBAFED40878452AFE3248F86382588F10F85D31A0BC4BB481 |
| SHA-512: | F662C58F4426AD698762E0793407305854C6BFE5242397E6D136116678EADBFD4E327A2EA499E4AAC6DDFFC5288D0F3AE43D0D5475832C7D0B4112EE0D509F8 |
| Malicious: | false |
| Reputation: | low |
| Preview: | ......JFIF.....( ..%...!1!%)7.....383,7(-:+.....-...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++.....".....<br>.....Aa.!1.....?...o.$.....(....E> ...b(.....R.LE.. -^YPZ...`...#Q.*5....y ..... ..Q` .4....C.].h .."..At..5.. .(-.U..."j...,@Z...^YX."B.TX..{.BB.K<br>...l@..AjZ )..".....A...M].....R.R..'`.* ..*E..,..E@.(h..A.$%...A.....,h.$.....$@TYSAj5Y.B..b.....H.VT..)....]C... .....CJ.!.0._....Z( .....B.....".....Ap.....M@.H.)iZ..Q.b.4.1R<br>.1R...$4.....@...a...j.Q1bPF.H....@.....P."..H..5(.....(....J...j,..PYP.YQ.QL.IH.b.....i.."....(....h.RR.0.A.J.(."....d...h R..P.Y. .....f....`")...`.....P.@TX.....j.,B.S@.S<br>@..@.....E..`....J.JP4.....%PM%:..Za.....Z ,5.....eP.....T...@.M@.....-....@... |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 7.655406020704828 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.96%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | 67AzzNNioP.exe |
| File size: | 2543411 |
| MD5: | f44d0bd72d14338b655a6d4457419493 |
| SHA1: | dbe17733409126985l5f76885f07d6faacbce09c |
| SHA256: | 8f8cb5930100e80159502fd6d224909606f47ff17614f89b41b650afc3a91b6d |
| SHA512: | c4d67a8772ef2a7325566ec9ccc8d20a4c66cef4069a52994671c21102d58ac0135998ace178a60717b52b51f08e9a2683dc888acfb2a5ff804060b0e9c2ab9e |
| SSDEEP: | 49152:tB/LNGrXDbdqRlwYDHMbYz9FUa+gXe9GeNCZpI4tUk1T:nxGrDbSTII9FUa+Ee9XN+I4tU6T |
| TLSH: | 2BC5230DB8C194F2C162D9364A616764A57879101B67CEDFE3ED4A3FCB624C1EE307A2 |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x_c.<>..<>..<br><>.....1>.....>.....$>...I..>>...I../>...I..+>...I...>..5F..7>..5F..;>..<>..)?...I...>...I..=>...I..=>...I..=>. |

### File Icon

| | |
|---|---|
| Icon Hash: | 008039c4c4384000 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x41f530 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | EXECUTABLE_IMAGE, 32BIT_MACHINE |
| DLL Characteristics: | DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE |
| Time Stamp: | 0x6220BF8D [Thu Mar 3 13:15:57 2022 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 5 |
| OS Version Minor: | 1 |
| File Version Major: | 5 |
| File Version Minor: | 1 |
| Subsystem Version Major: | 5 |
| Subsystem Version Minor: | 1 |
| Import Hash: | 12e12319f1029ec4f8fcbed7e82df162 |

### Entrypoint Preview

| Instruction |
|---|
| call 00007F9BACB06F8Bh |
| jmp 00007F9BACB0689Dh |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| push ebp |
| mov ebp, esp |
| push esi |
| push dword ptr [ebp+08h] |
| mov esi, ecx |
| call 00007F9BACAF96E7h |
| mov dword ptr [esi], 004356D0h |
| mov eax, esi |
| pop esi |
| pop ebp |
| retn 0004h |
| and dword ptr [ecx+04h], 00000000h |
| mov eax, ecx |
| and dword ptr [ecx+08h], 00000000h |
| mov dword ptr [ecx+04h], 004356D8h |
| mov dword ptr [ecx], 004356D0h |
| ret |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |

| Instruction |
| --- |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| push ebp |
| mov ebp, esp |
| push esi |
| mov esi, ecx |
| lea eax, dword ptr [esi+04h] |
| mov dword ptr [esi], 004356B8h |
| push eax |
| call 00007F9BACB09D2Fh |
| test byte ptr [ebp+08h], 00000001h |
| pop ecx |
| je 00007F9BACB06A2Ch |
| push 0000000Ch |
| push esi |
| call 00007F9BACB05FE9h |
| pop ecx |
| pop ecx |
| mov eax, esi |
| pop esi |
| pop ebp |
| retn 0004h |
| push ebp |
| mov ebp, esp |
| sub esp, 0Ch |
| lea ecx, dword ptr [ebp-0Ch] |
| call 00007F9BACAF9662h |
| push 0043BEF0h |
| lea eax, dword ptr [ebp-0Ch] |
| push eax |
| call 00007F9BACB097E9h |
| int3 |
| push ebp |
| mov ebp, esp |
| sub esp, 0Ch |
| lea ecx, dword ptr [ebp-0Ch] |
| call 00007F9BACB069A8h |
| push 0043C0F4h |
| lea eax, dword ptr [ebp-0Ch] |
| push eax |
| call 00007F9BACB097CCh |
| int3 |
| jmp 00007F9BACB0B267h |
| int3 |
| int3 |
| int3 |
| int3 |
| push 00422900h |
| push dword ptr fs:[00000000h] |

## Rich Headers

| | |
| --- | --- |
| Programming Language: | • [ C ] VS2008 SP1 build 30729<br>• [IMP] VS2008 SP1 build 30729 |

## Data Directories

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x3d070 | 0x34 | .rdata |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x3d0a4 | 0x50 | .rdata |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x64000 | 0x4698c | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0xab000 | 0x233c | .reloc |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x3b11c | 0x54 | .rdata |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x355f8 | 0x40 | .rdata |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x33000 | 0x278 | .rdata |
| IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT | 0x3c5ec | 0x120 | .rdata |
| 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 | 0x31bdc | 0x31c00 | False | 0.5909380888819096 | data | 6.712962136932442 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ |
| .rdata | 0x33000 | 0xaec0 | 0xb000 | False | 0.4579190340909091 | data | 5.261605615899847 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x3e000 | 0x24720 | 0x1000 | False | 0.451416015625 | data | 4.387459135575936 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .didat | 0x63000 | 0x190 | 0x200 | False | 0.4453125 | data | 3.3327310103022305 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .rsrc | 0x64000 | 0x4698c | 0x46a00 | False | 0.07180586283185841 | data | 2.00213285276512 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0xab000 | 0x233c | 0x2400 | False | 0.7749565972222222 | data | 6.623012966548067 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

**Resources**

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| PNG | 0x64524 | 0xb45 | PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced | English | United States |
| PNG | 0x6506c | 0x15a9 | PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced | English | United States |
| RT_ICON | 0x66618 | 0x42028 | data | | |
| RT_DIALOG | 0xa8640 | 0x286 | data | English | United States |
| RT_DIALOG | 0xa88c8 | 0x13a | data | English | United States |
| RT_DIALOG | 0xa8a04 | 0xec | data | English | United States |
| RT_DIALOG | 0xa8af0 | 0x12e | data | English | United States |
| RT_DIALOG | 0xa8c20 | 0x338 | data | English | United States |
| RT_DIALOG | 0xa8f58 | 0x252 | data | English | United States |
| RT_STRING | 0xa91ac | 0x1e2 | data | English | United States |
| RT_STRING | 0xa9390 | 0x1cc | data | English | United States |
| RT_STRING | 0xa955c | 0x1b8 | data | English | United States |
| RT_STRING | 0xa9714 | 0x146 | Hitachi SH big-endian COFF object file, not stripped, 17152 sections, symbol offset=0x73006500 | English | United States |
| RT_STRING | 0xa985c | 0x46c | data | English | United States |
| RT_STRING | 0xa9cc8 | 0x166 | data | English | United States |
| RT_STRING | 0xa9e30 | 0x152 | data | English | United States |
| RT_STRING | 0xa9f84 | 0x10a | data | English | United States |

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_STRING | 0xaa090 | 0xbc | data | English | United States |
| RT_STRING | 0xaa14c | 0xd6 | data | English | United States |
| RT_GROUP_ICON | 0xaa224 | 0x14 | data | | |
| RT_MANIFEST | 0xaa238 | 0x753 | XML 1.0 document, ASCII text, with CRLF line terminators | English | United States |

### Imports

| DLL | Import |
|---|---|
| KERNEL32.dll | GetLastError, SetLastError, FormatMessageW, GetCurrentProcess, DeviceIoControl, SetFileTime, CloseHandle, CreateDirectoryW, RemoveDirectoryW, CreateFileW, DeleteFileW, CreateHardLinkW, GetShortPathNameW, GetLongPathNameW, MoveFileW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, SetFileAttributesW, GetFileAttributesW, FindClose, FindFirstFileW, FindNextFileW, InterlockedDecrement, GetVersionExW, GetCurrentDirectoryW, GetFullPathNameW, FoldStringW, GetModuleFileNameW, GetModuleHandleW, FindResourceW, FreeLibrary, GetProcAddress, GetCurrentProcessId, ExitProcess, SetThreadExecutionState, Sleep, LoadLibraryW, GetSystemDirectoryW, CompareStringW, AllocConsole, FreeConsole, AttachConsole, WriteConsoleW, GetProcessAffinityMask, CreateThread, SetThreadPriority, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetEvent, ResetEvent, ReleaseSemaphore, WaitForSingleObject, CreateEventW, CreateSemaphoreW, GetSystemTime, SystemTimeToTzSpecificLocalTime, TzSpecificLocalTimeToSystemTime, SystemTimeToFileTime, FileTimeToLocalFileTime, LocalFileTimeToFileTime, FileTimeToSystemTime, GetCPInfo, IsDBCSLeadByte, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, LockResource, GlobalLock, GlobalUnlock, GlobalFree, LoadResource, SizeofResource, SetCurrentDirectoryW, GetExitCodeProcess, GetLocalTime, GetTickCount, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, OpenFileMappingW, GetCommandLineW, SetEnvironmentVariableW, ExpandEnvironmentStringsW, GetTempPathW, MoveFileExW, GetLocaleInfoW, GetTimeFormatW, GetDateFormatW, GetNumberFormatW, DecodePointer, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapSize, SetStdHandle, GetProcessHeap, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineA, GetOEMCP, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, TerminateProcess, LocalFree, RtlUnwind, EncodePointer, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, HeapReAlloc, GetStringTypeW, LCMapStringW, FindFirstFileExA, FindNextFileA, IsValidCodePage |
| OLEAUT32.dll | SysAllocString, SysFreeString, VariantClear |
| gdiplus.dll | GdipAlloc, GdipDisposeImage, GdipCloneImage, GdipCreateBitmapFromStream, GdipCreateBitmapFromStreamICM, GdipCreateHBITMAPFromBitmap, GdiplusStartup, GdiplusShutdown, GdipFree |

### Possible Origin

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

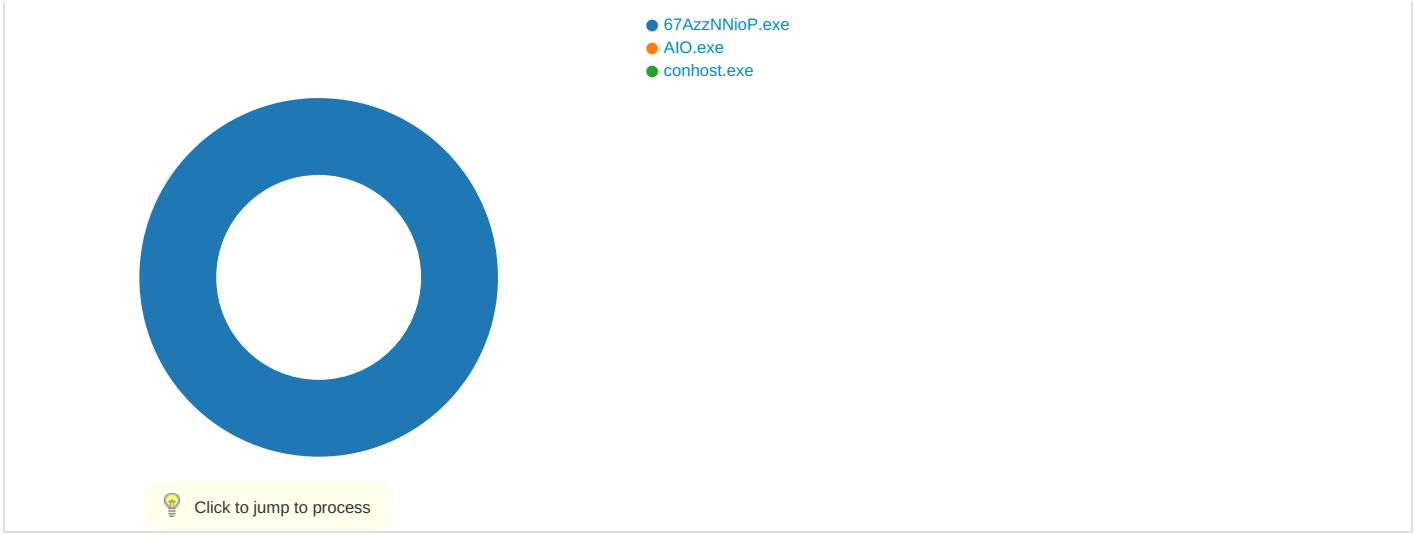
# Network Behavior

## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Sep 23, 2022 07:56:52.887993097 CEST | 49702 | 9090 | 192.168.2.3 | 185.25.204.244 |
| Sep 23, 2022 07:56:52.913883924 CEST | 9090 | 49702 | 185.25.204.244 | 192.168.2.3 |
| Sep 23, 2022 07:56:53.419513941 CEST | 49702 | 9090 | 192.168.2.3 | 185.25.204.244 |
| Sep 23, 2022 07:56:53.445174932 CEST | 9090 | 49702 | 185.25.204.244 | 192.168.2.3 |
| Sep 23, 2022 07:56:53.950766087 CEST | 49702 | 9090 | 192.168.2.3 | 185.25.204.244 |
| Sep 23, 2022 07:56:53.976298094 CEST | 9090 | 49702 | 185.25.204.244 | 192.168.2.3 |

# Statistics

## Behavior




# System Behavior

## Analysis Process: 67AzzNNioP.exe PID: **3932**, Parent PID: **5644**

### General

| | |
|---|---|
| Target ID: | 0 |
| Start time: | 07:56:40 |
| Start date: | 23/09/2022 |
| Path: | C:\Users\user\Desktop\67AzzNNioP.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\67AzzNNioP.exe" |
| Imagebase: | 0x1e0000 |
| File size: | 2543411 bytes |
| MD5 hash: | F44D0BD72D14338B655A6D4457419493 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

### File Activities

## Analysis Process: AIO.exe PID: **5576**, Parent PID: **3932**

### General

| | |
|---|---|
| Target ID: | 1 |
| Start time: | 07:56:50 |
| Start date: | 23/09/2022 |
| Path: | C:\Users\user\Desktop\AIO.exe |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Users\user\Desktop\AIO.exe" |
| Imagebase: | 0xf30000 |
| 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: **3776**, Parent PID: **5576**

### General

| | |
|---|---|
| Target ID: | 2 |
| Start time: | 07:56:51 |
| Start date: | 23/09/2022 |
| 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 |

## Disassembly

**No disassembly**