ASSIGNMENT 2

Table contents

I. PART 2-1

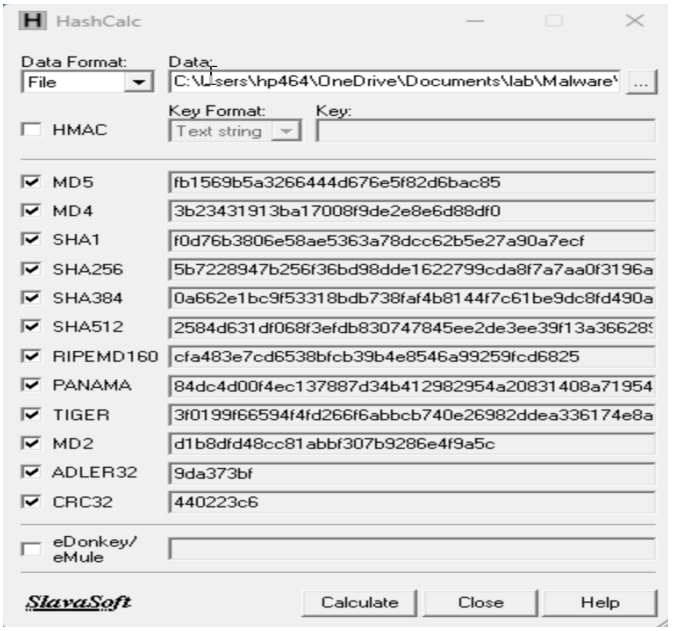
A. Basic Static

1. File Information

File: juice.exe

MD5: fb1569b5a3266444d676e5f82d6bac85

Size: 42.00 KB (43008 bytes)



2. Virus Total

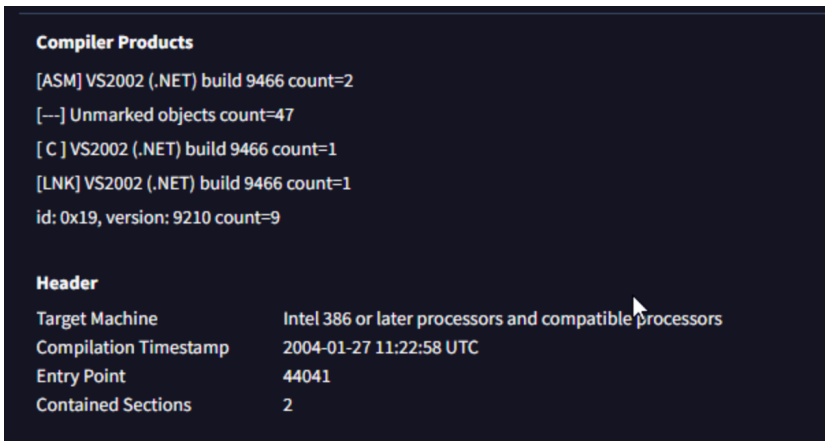
Header

Detection ratio: 62/72

Target Machine: Intel 386 or later processors and compatible processors

Compilation Timestamp: 2004-01-27 11:22:58 UTC

Entry Point: 44041

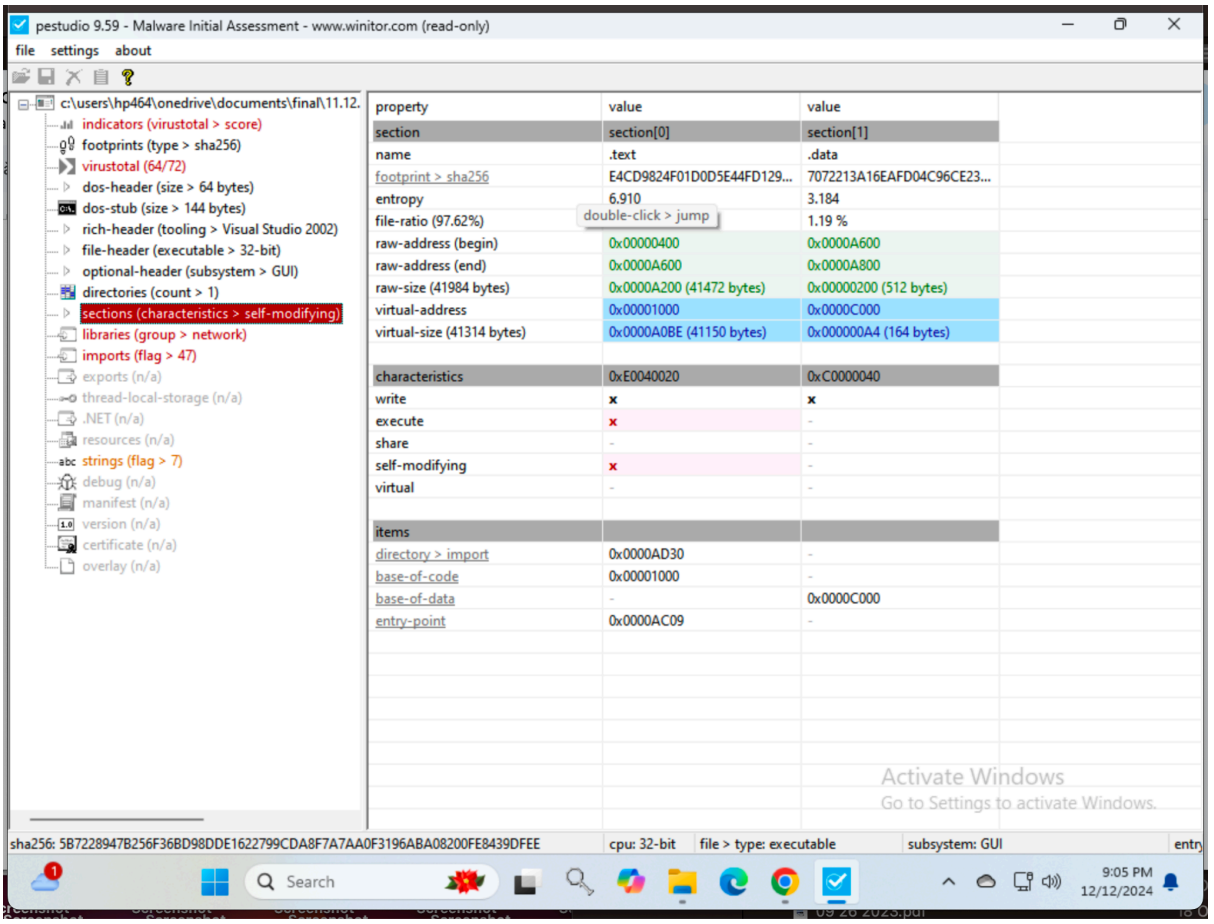


3. PESTUDIO

PeStudio shows multiple static properties and flags anomalies.

a) Sections

Contained Sections: 2



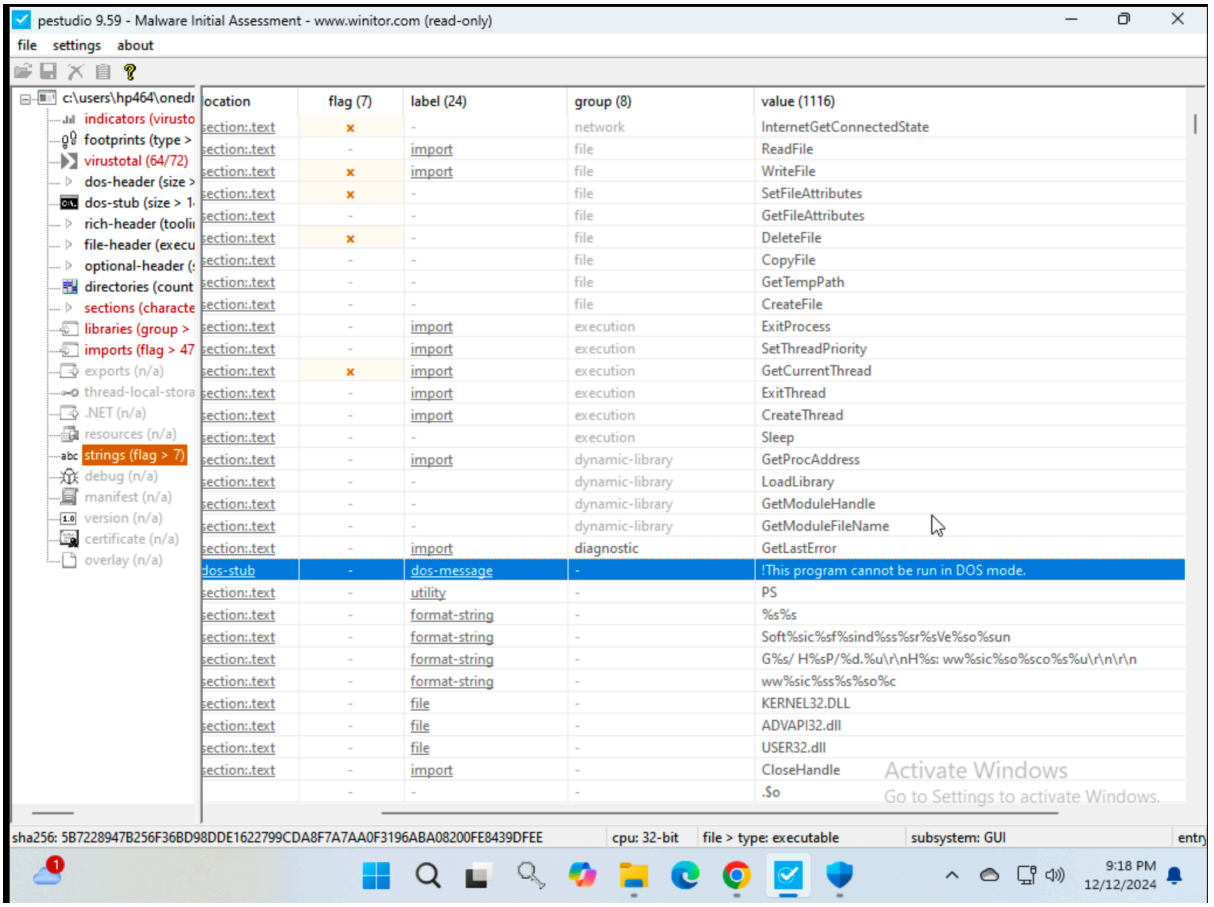
b) Strings

The string `"This program cannot be run in DOS mode"` confirms that this file is a Windows executable in the **PE (Portable Executable)** format.
The string `Soft%sic%sf%sind%ss%sr%sVe%so%sun` appears to be an obfuscated string, which is often used in malware to evade detection.
API Calls: Several Windows API functions are listed, such as `ExitProcess`, `lstrcpyA`, `SetFileAttributesA`, `DeleteFileA`, `CreateMutexA`, and others. These functions are frequently used in malware to manipulate files, manage processes, and hide its presence on the system.

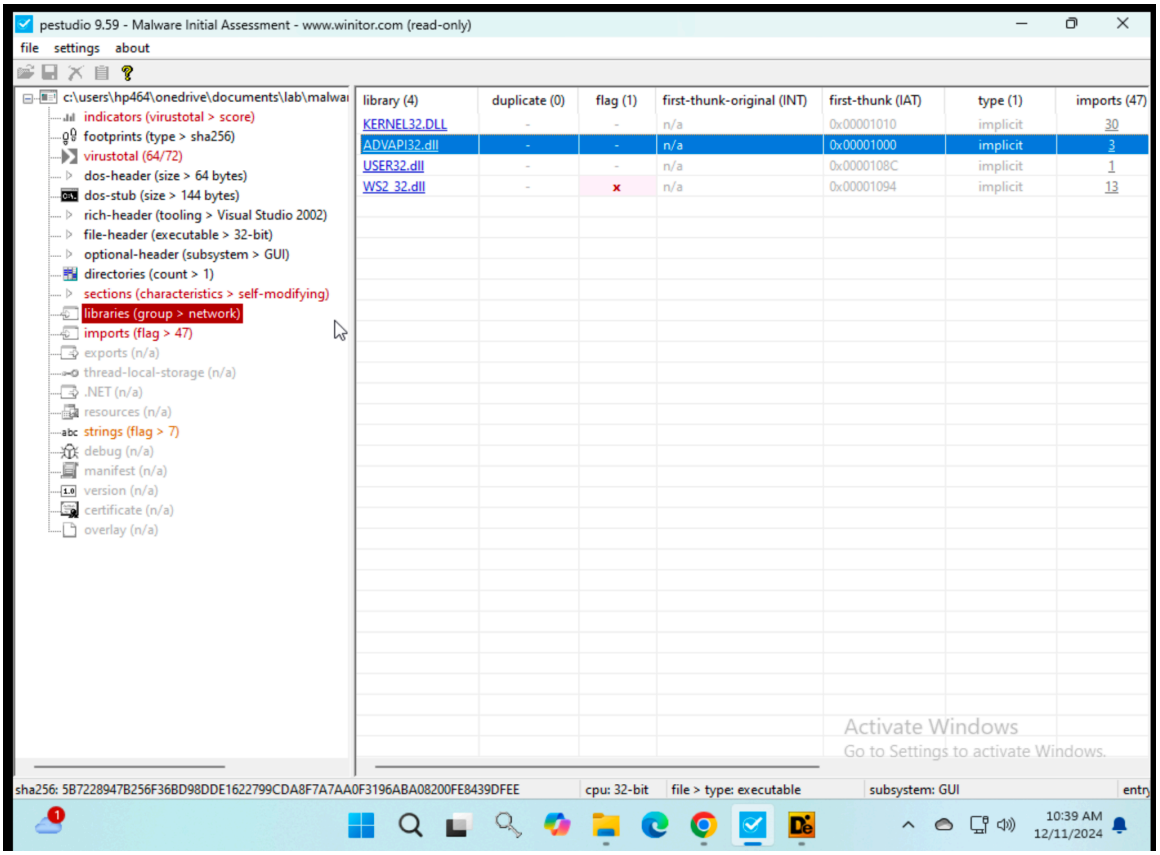
Networking: The references to `InternetGetConnectedState` and `wininet.dll` suggest the possibility of network-related behavior, such as checking the network state or establishing communications over the network.

File Operations: Functions like `SetFileAttributesA`, `DeleteFileA`, and `CopyFileA` suggest that this executable might be involved in file manipulation, possibly deleting or copying files to hide traces of its activity.

Registry Manipulation: The presence of `RegOpenKeyExA`, `RegCloseKey`, and `RegSetValueExA` indicates that the malware may interact with the

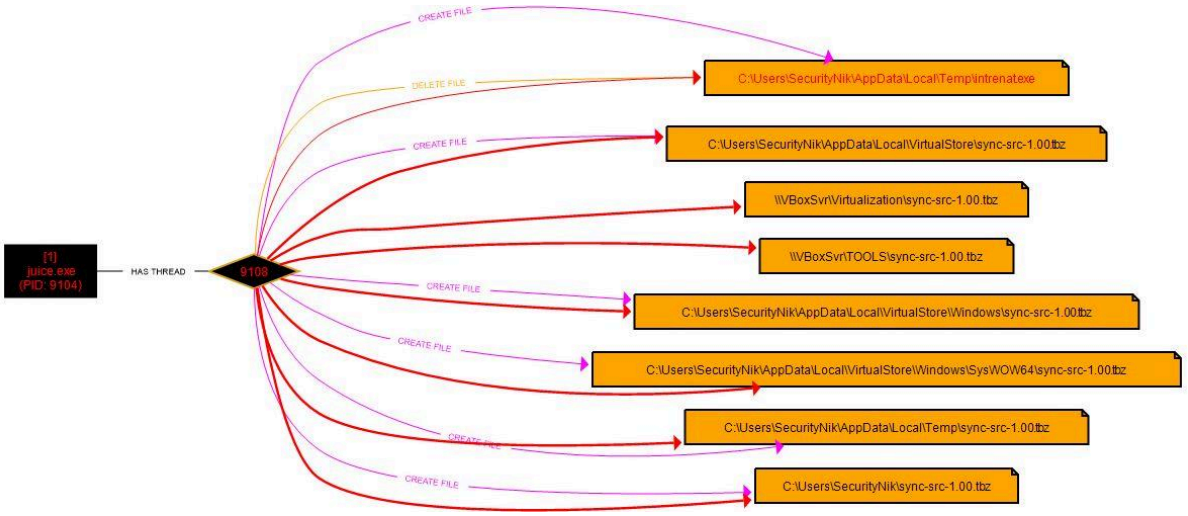

pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)
file settings about
c:\users\hp464\onedr
indicators (virusto
footprints (type >
virustotal (64/72)
dos-header (size >
dos-stub (size > 1
rich-header (toolii
file-header (execu
optional-header (
directories (count
sections (characte
libraries (group >
imports (flag > 47
exports (n/a)
thread-local-stora
.NET (n/a)
resources (n/a)
strings (flag > 7)
debug (n/a)
manifest (n/a)
version (n/a)
certificate (n/a)
overlay (n/a)
location | flag (7) | label (24) | group (8) | value (1116)
section:.text | x | - | network | InternetGetConnectedState
section:.text | - | import | file | ReadFile
section:.text | x | import | file | WriteFile
section:.text | x | - | file | SetFileAttributes
section:.text | - | - | file | GetFileAttributes
section:.text | x | - | file | DeleteFile
section:.text | - | - | file | CopyFile
section:.text | - | - | file | GetTempPath
section:.text | - | - | file | CreateFile
section:.text | - | import | execution | ExitProcess
section:.text | - | import | execution | SetThreadPriority
section:.text | x | import | execution | GetCurrentThread
section:.text | - | import | execution | ExitThread
section:.text | - | import | execution | CreateThread
section:.text | - | - | execution | Sleep
section:.text | - | import | dynamic-library | GetProcAddress
section:.text | - | - | dynamic-library | LoadLibrary
section:.text | - | - | dynamic-library | GetModuleHandle
section:.text | - | - | dynamic-library | GetModuleFileName
section:.text | - | import | diagnostic | GetLastError
dos-stub | - | dos-message | - | !This program cannot be run in DOS mode.
section:.text | - | utility | - | PS
section:.text | - | format-string | - | %s%s
section:.text | - | format-string | - | Soft%sic%sf%sind%ss%sr%sVe%so%sun
section:.text | - | format-string | - | G%s/ H%sP/%d.%u\r\nH%s: ww%sic%so%sco%s%u\r\n\r\n
section:.text | - | format-string | - | ww%sic%ss%s%so%c
section:.text | - | file | - | KERNEL32.DLL
section:.text | - | file | - | ADVAPI32.dll
section:.text | - | file | - | USER32.dll
section:.text | - | import | - | CloseHandle
- | - | - | - | .$o
Activate Windows
Go to Settings to activate Windows.
sha256: 5B7228947B256F36BD98DDE1622799CDA8F7A7AA0F3196ABA08200FE8439DFEE
cpu: 32-bit
file > type: executable
subsystem: GUI
9:18 PM
12/12/2024

c) Imports



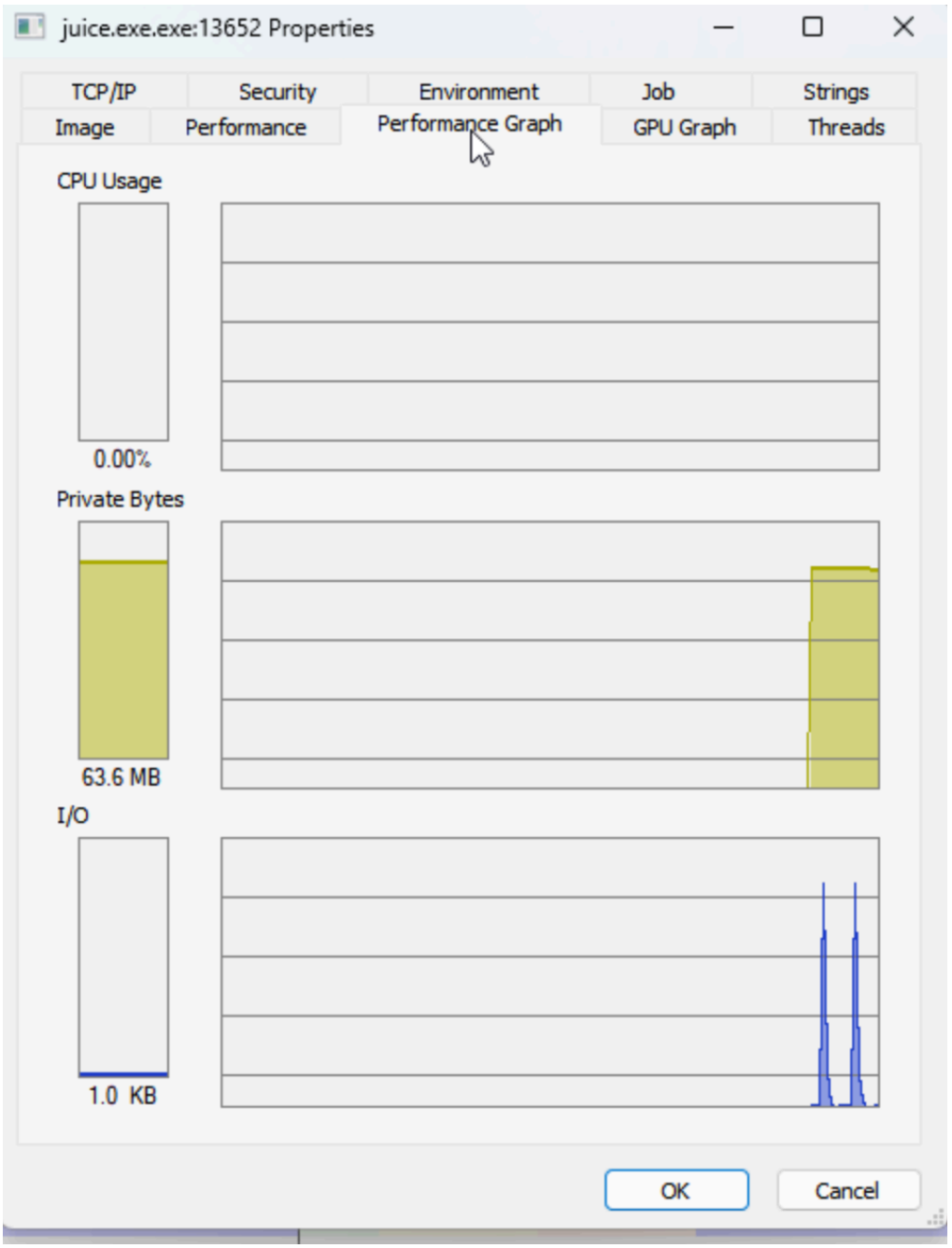
KERNEL32.DLL	ExitProcess, lstrcpyA, GetSystemTime, SetFileAttributesA, GetFileAttributesA, DeleteFileA, CopyFileA, CreateMutexA, GetLastError, GetDriveTypeA, lstrcatA, GetWindowsDirectoryA, GetSystemDirectoryA, GetTempPathA, GetEnvironmentVariableA, lstrlenA, Sleep, GetTickCount, GetProcAddress, LoadLibraryA, GetModuleHandleA, ReadFile, CreateFileA, GetModuleFileNameA, SetThreadPriority, GetCurrentThread, ExitThread, CreateThread, CloseHandle, WriteFile
ADVAPI32.dll	RegOpenKeyExA, RegCloseKey, RegSetValueExA
USER32.dll	wsprintfA
WS2_32.dll	gethostbyname, htons, htonl, send, socket, gethostname, connect, WSAGetLastError, select, __WSAFDIsSet, closesocket, WSAStartup, ioctlsocket

4. Prodot

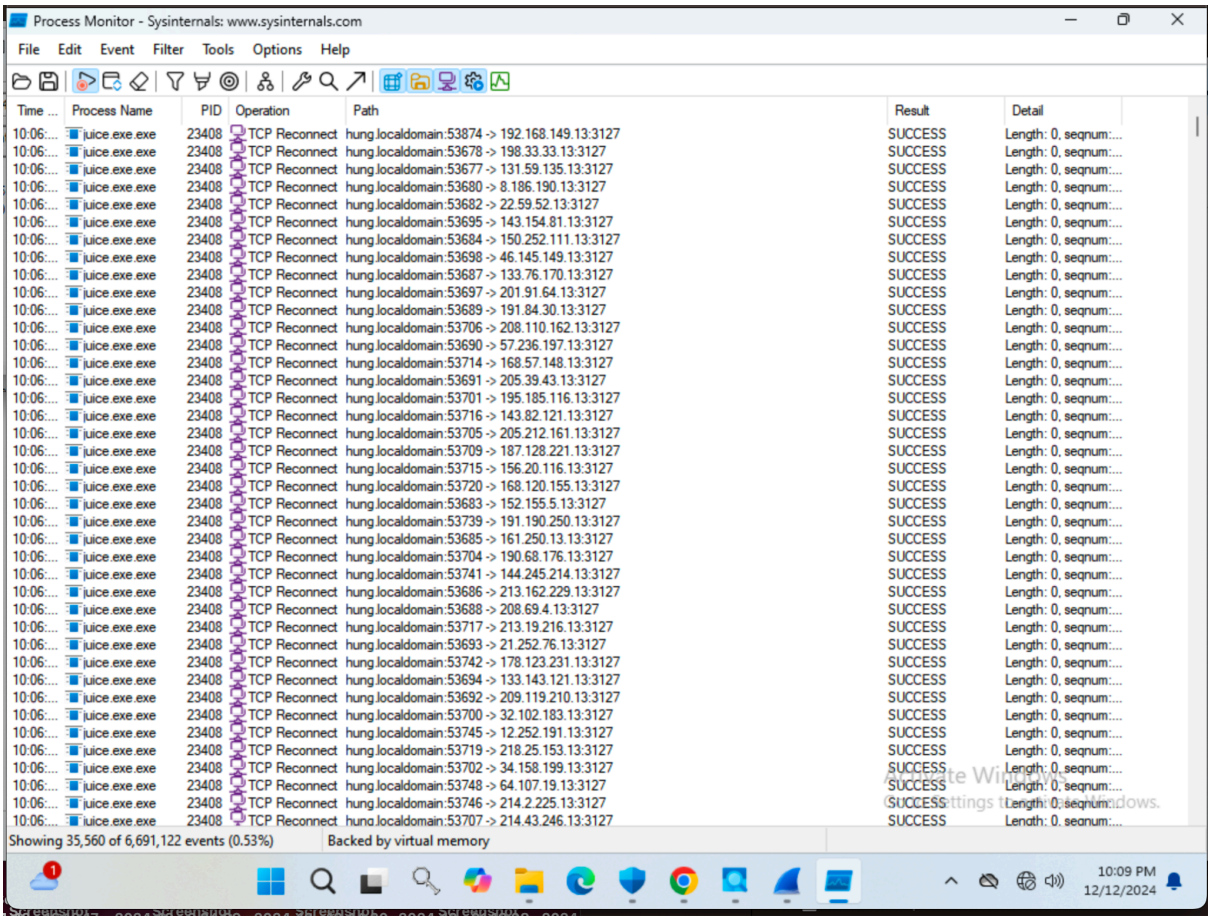


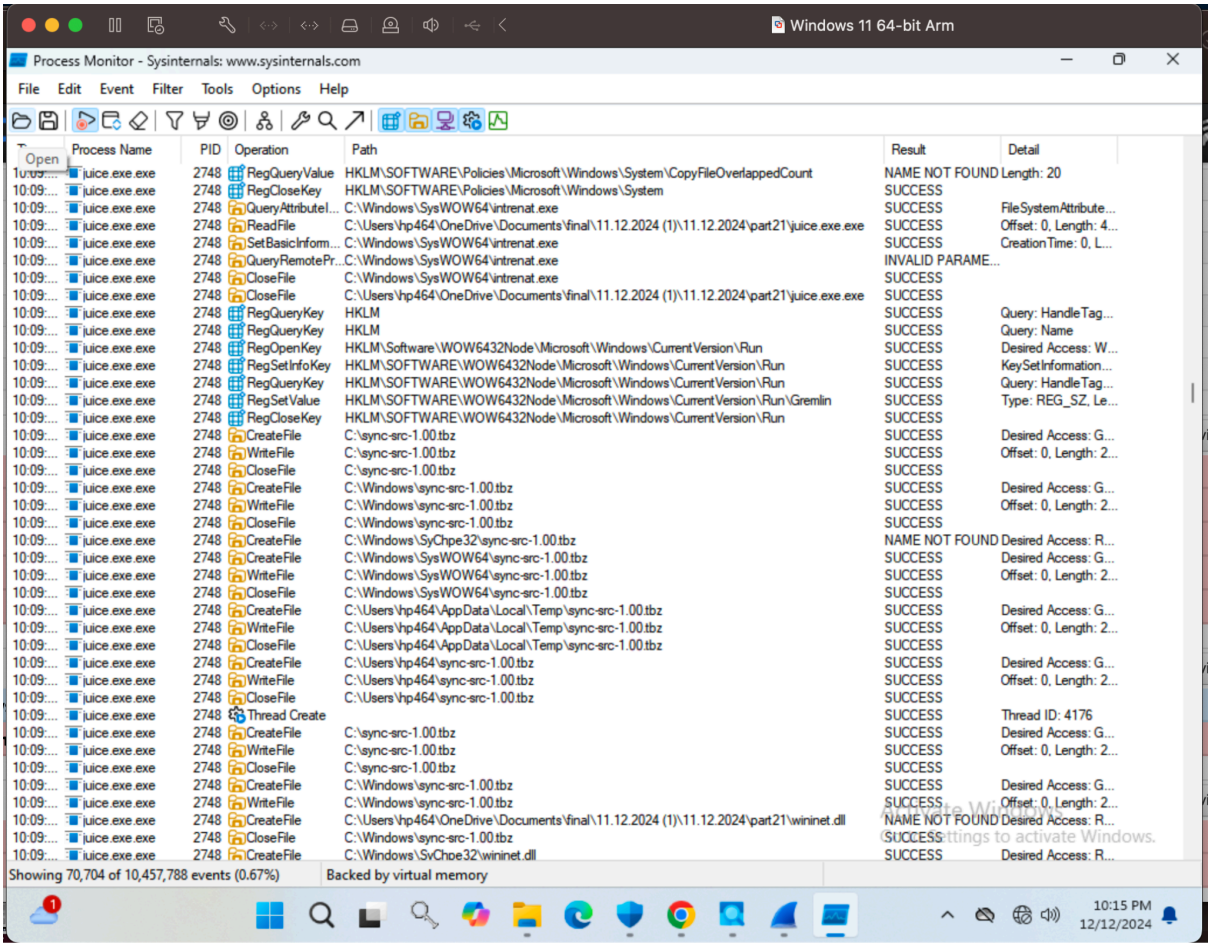
B. Basic Dynamic

1. Process Explorer



2. Procmon


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53874 -> 192.168.149.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53678 -> 198.33.33.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53677 -> 131.59.135.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53680 -> 8.186.190.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53682 -> 22.59.52.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53695 -> 143.154.81.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53684 -> 150.252.111.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53698 -> 46.145.149.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53687 -> 133.76.170.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53697 -> 201.91.64.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53689 -> 191.84.30.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53706 -> 208.110.162.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53690 -> 57.236.197.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53714 -> 168.57.148.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53691 -> 205.39.43.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53701 -> 195.185.116.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53716 -> 143.82.121.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53705 -> 205.212.161.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53709 -> 187.128.221.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53715 -> 156.20.116.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53720 -> 168.120.155.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53683 -> 152.155.5.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53739 -> 191.190.250.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53685 -> 161.250.13.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53704 -> 190.68.176.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53741 -> 144.245.214.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53686 -> 213.162.229.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53688 -> 208.69.4.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53717 -> 213.19.216.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53693 -> 21.252.76.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53742 -> 178.123.231.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53694 -> 133.143.121.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53692 -> 209.119.210.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53700 -> 32.102.183.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53745 -> 12.252.191.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53719 -> 218.25.153.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53702 -> 34.158.199.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53748 -> 64.107.19.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53746 -> 214.2.225.13:3127 SUCCESS Length: 0, seqnum:...
10:06:... juice.exe.exe 23408 TCP Reconnect hung.localdomain:53707 -> 214.43.246.13:3127 SUCCESS Length: 0, seqnum:...
Showing 35,560 of 6,691,122 events (0.53%)
Backed by virtual memory
10:09 PM
12/12/2024



Create and Drop file

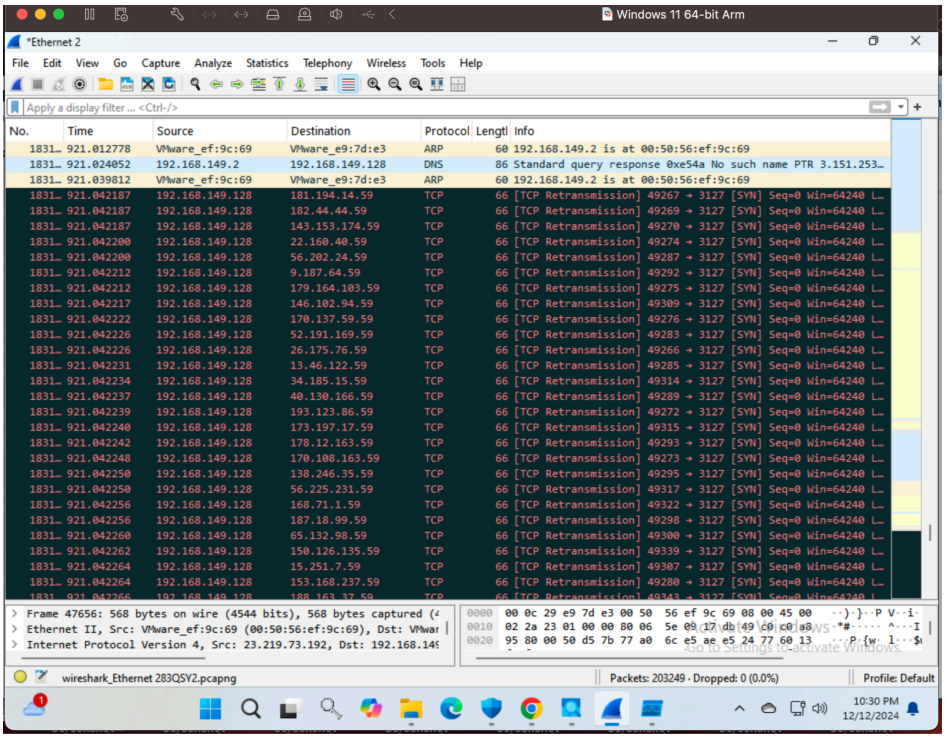
C:\User\hp464\sync-src-1.00.tbz

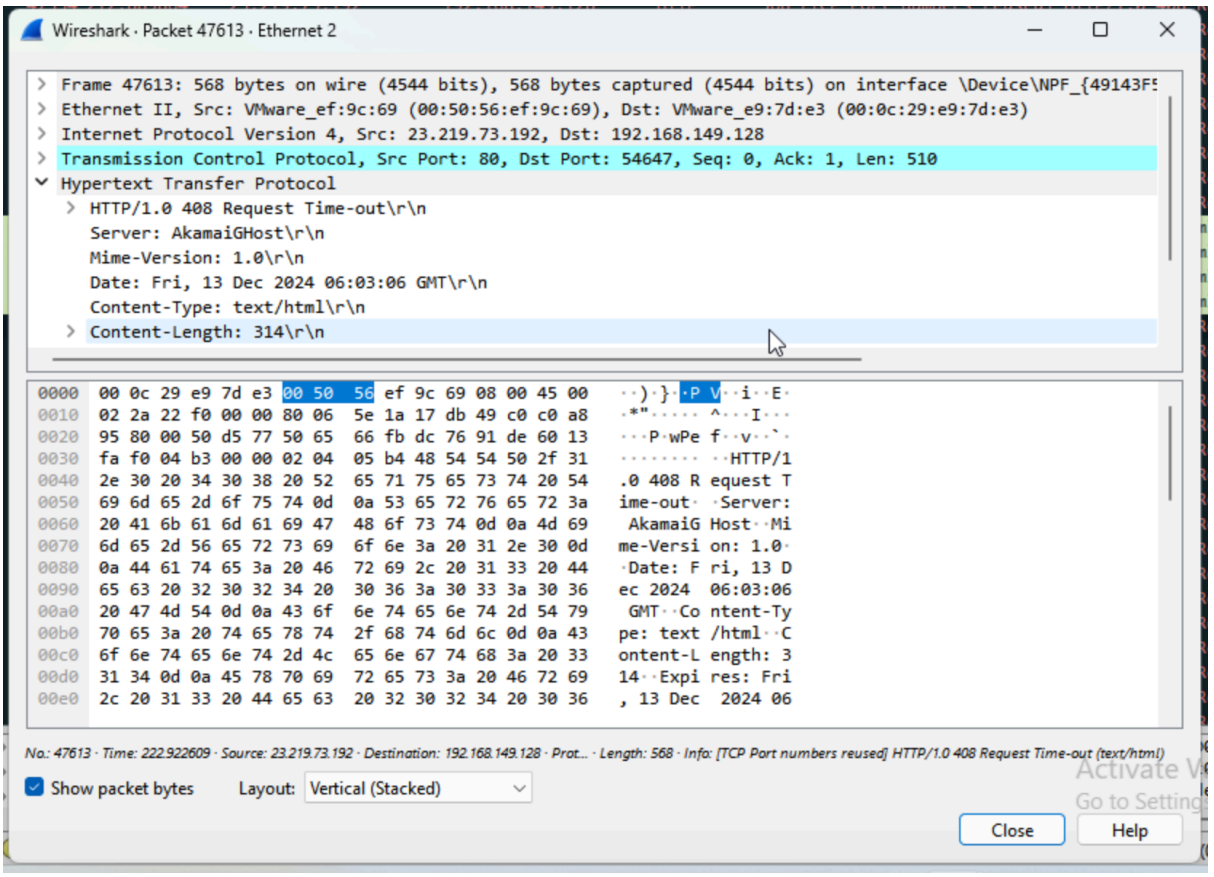
C:\Windows\SysWOW64\intrenat.exe

C:\Windows\SyChoe32\winiet.dll

3. WireShark

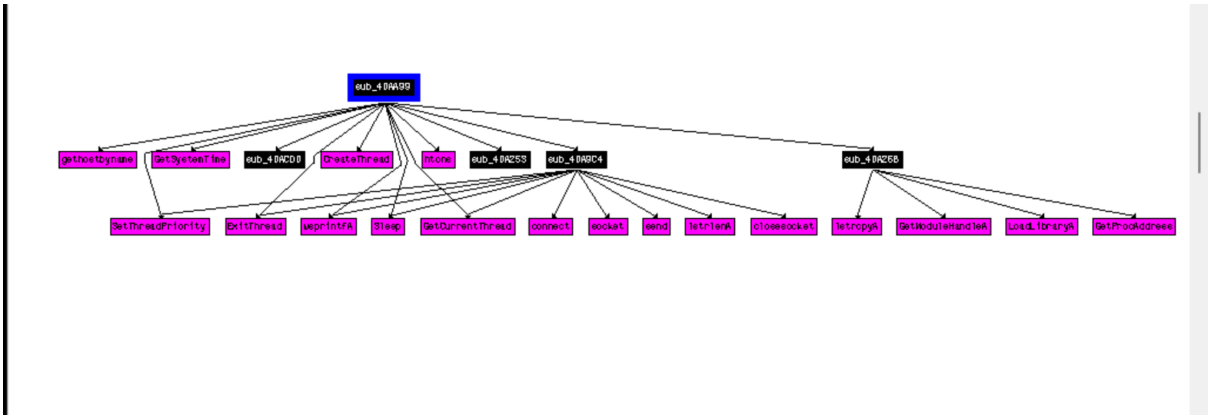
Connect Many I





C. Advanced Static

IDA Professional 9.0



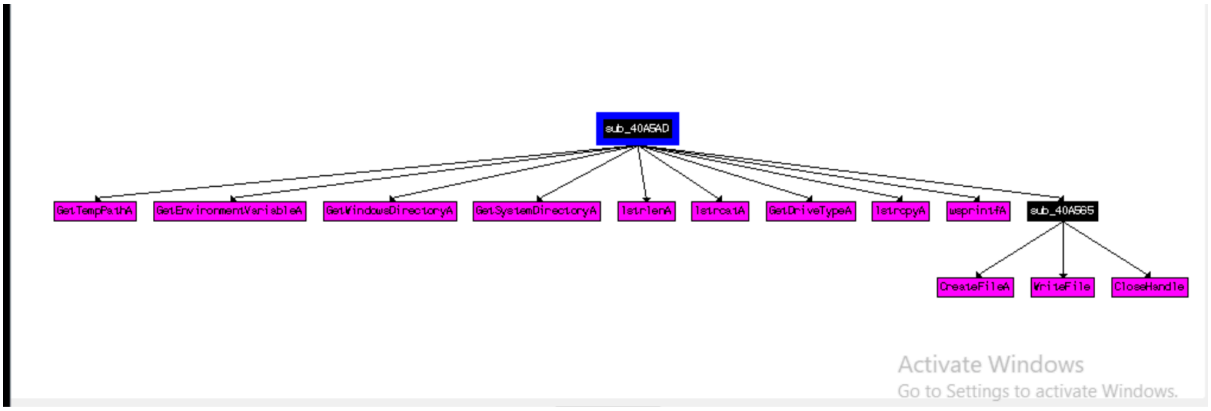
Sub_40AA99

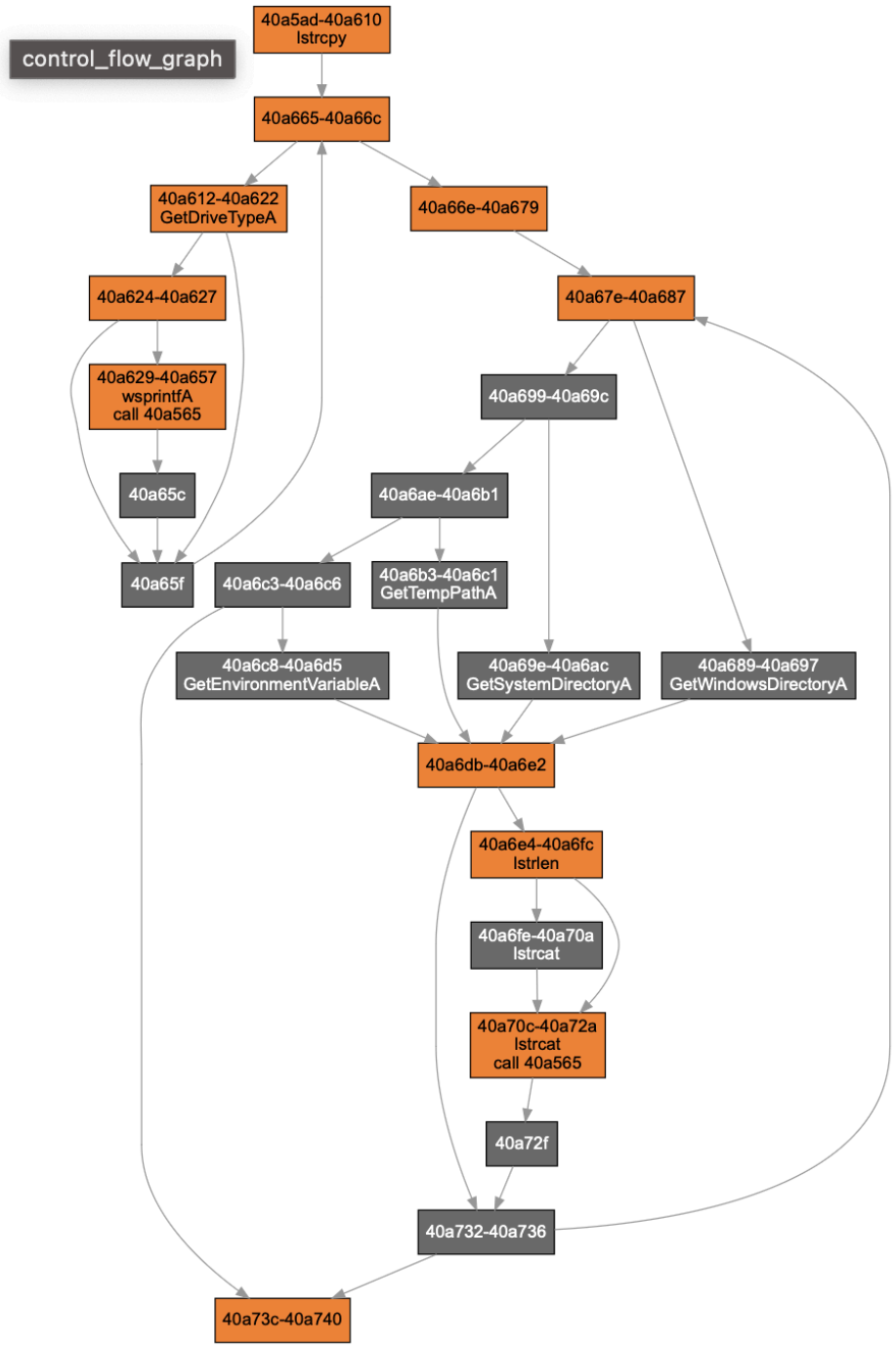
Sleep.KERNELBASE(000003E8), ref: 0040AB0C

- **GetCurrentThread**.KERNEL32 ref: 0040AB17
- **SetThreadPriority**.KERNELBASE(00000000), ref: 0040AB1E

- **wsprintfA**.USER32 ref: 0040AB46
- **htons**.WS2_32(00000050), ref: 0040AB69
- **Sleep**.KERNEL32(00004650), ref: 0040AB76
- **gethostbyname**.WS2_32(?), ref: 0040AB8C
- **htons**.WS2_32(00000050), ref: 0040ABC0
- **CreateThread**.KERNELBASE(00000000,00000000,Function_000 0A9C4,00000002,00000000,?), ref: 0040ABEF
- **RtlExitUserThread**.KERNEL32(00000000), ref: 0040AC02
- ww%sic%ss%s%so%c, xrefs: 0040AB40

Sub_40A5AD





APIs

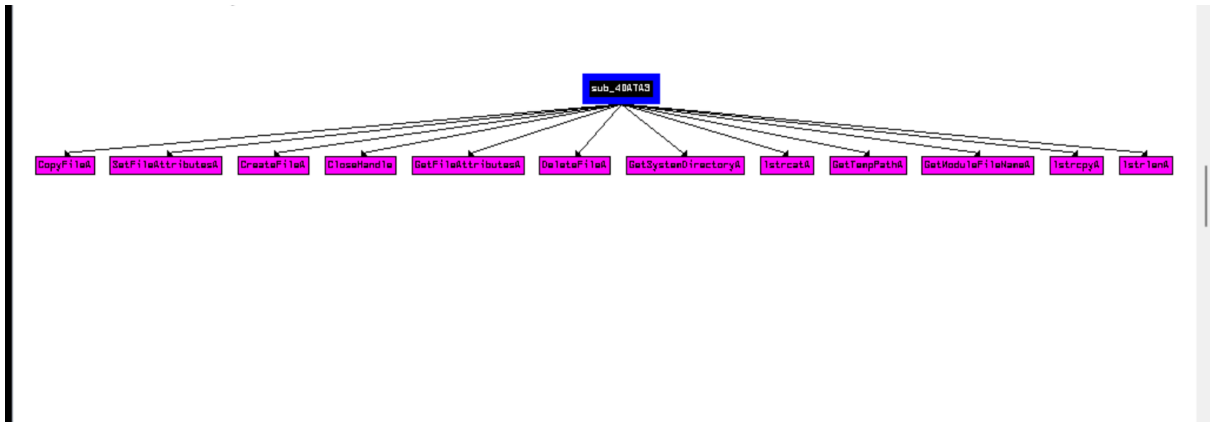
- **GetDriveTypeA**.KERNELBASE(0000007A), ref: 0040A619
- **wsprintfA**.USER32 ref: 0040A640

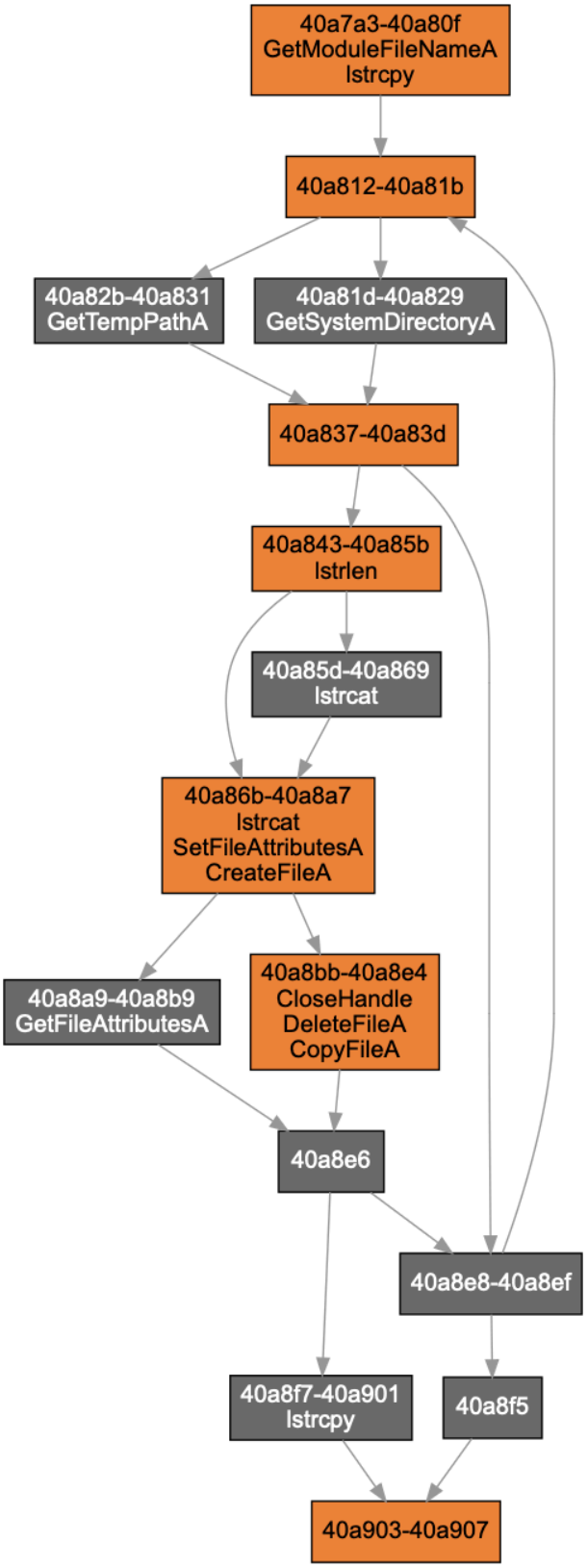
- **GetWindowsDirectoryA**.KERNEL32(00000000,00000100,?,0000 0000), ref: 0040A691
- **GetSystemDirectoryA**.KERNEL32(00000000,00000100), ref: 0040A6A6
- **GetTempPathA**.KERNEL32(00000100,00000000,?,00000000), ref: 0040A6BB
- **lstrlen**.KERNEL32(00000000,?,00000000), ref: 0040A6EB
- **lstrcat**.KERNEL32(00000000,0040A038), ref: 0040A70A
- **lstrcat**.KERNEL32(00000000,sync-src-1.00.tbz), ref: 0040A717

Strings

- %s%s, xrefs: 0040A63A
- sync-src-1.00.tbz, xrefs: 0040A629, 0040A62C
- USERPROFILE, xrefs: 0040A6D0
- z, xrefs: 0040A665
- c:\, xrefs: 0040A5BA

Sub_0040A7A3




40a7a3-40a80f
GetModuleFileNameA
lstrcpy
40a812-40a81b
40a82b-40a831
GetTempPathA
40a81d-40a829
GetSystemDirectoryA
40a837-40a83d
40a843-40a85b
lstrlen
40a85d-40a869
lstrcat
40a86b-40a8a7
lstrcat
SetFileAttributesA
CreateFileA
40a8a9-40a8b9
GetFileAttributesA
40a8bb-40a8e4
CloseHandle
DeleteFileA
CopyFileA
40a8e6
40a8e8-40a8ef
40a8f7-40a901
lstrcpy
40a8f5
40a903-40a907

APIs

GetModuleFileNameA.KERNEL32(00000000,?,00000104,?,00000000), ref: 0040A7F1

- **lstrcpy**.KERNEL32(00000200,?), ref: 0040A807
- **GetSystemDirectoryA**.KERNEL32(?,00000118), ref: 0040A823
- **GetTempPathA**.KERNEL32(00000118,?,?,00000000), ref: 0040A831
- **lstrlen**.KERNEL32(?,?,00000000), ref: 0040A84A
- **lstrcat**.KERNEL32(?,0040A038), ref: 0040A869
- **lstrcat**.KERNEL32(?,intrenat.exe), ref: 0040A876
- **SetFileAttributesA**.KERNELBASE(?,00000020,?,00000000), ref: 0040A881
- **CreateFileA**.KERNELBASE(?,40000000,00000003,00000000,00000002,00000080,00000000,?,00000000), ref: 0040A89E
- **GetFileAttributesA**.KERNEL32(?,?,00000000), ref: 0040A8B0
- **CloseHandle**.KERNEL32(00000000,?,00000000), ref: 0040A8BC
- **DeleteFileA**.KERNELBASE(?,?,00000000), ref: 0040A8C9
- **CopyFileA**.KERNEL32(?,?,00000000), ref: 0040A8DE
- **lstrcpy**.KERNEL32(00000200,?), ref: 0040A901

String

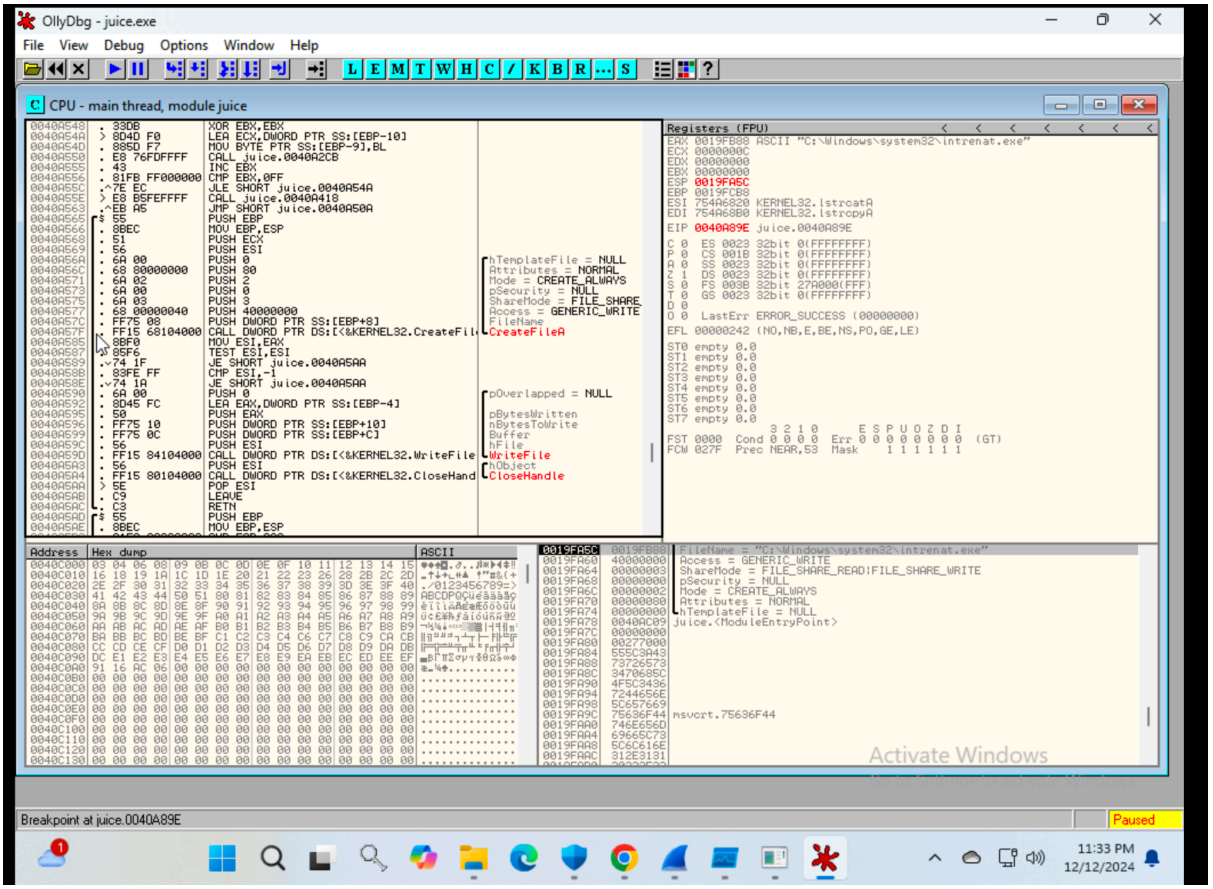
- intrenat.exe, xrefs: 0040A86B, 0040A86E

D. Advance Dynamic

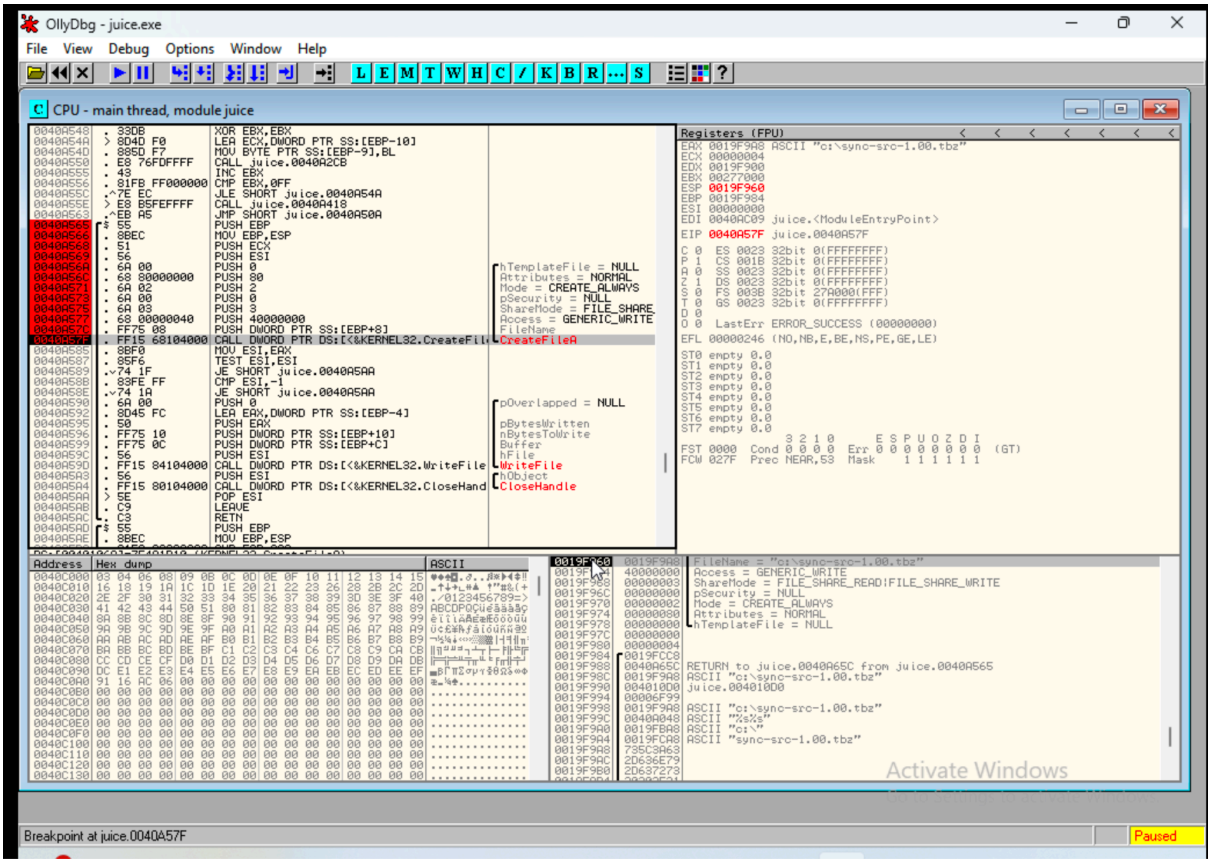
OLLYDBG

CreateFileA

C:\Windows\SysWOW64\intrenat.exe



Create sync-src-1.00.tbz



E. Conclusion

The juice.exe malware is a sophisticated threat capable of manipulating system files, modifying the registry, communicating over the network, and employing evasion techniques to avoid detection. It poses a significant risk to infected systems and highlights the need for robust monitoring and security mechanisms to detect and mitigate such threats. behaviors:

1. **File Manipulation**:
    - Creates and drops files such as intrenat.exe in the C:\Windows\SysWOW64 directory and sync-src-1.00.tbz in the user directory.
2. **Registry Operations**:
    - Uses functions like RegOpenKeyExA and RegSetValueExA to modify registry keys, ensuring persistence and obfuscating its activities.
3. **Network Communication**:
    - Employs functions like InternetGetConnectedState and references to wininet.dll to check network connectivity and establish communications with remote servers, potentially for data exfiltration or command-and-control purposes.
4. **Evasion Techniques**:
    - Utilizes obfuscated strings, such as Soft%sic%sf%sind%ss%sr%sVe%so%sun, to evade detection by security software.

F. Resources

1. Tools

PE Studio: https://www.winitor.com/download
IDA Professtional: https://hex-rays.com/ida-pro
Prodot: https://www.procdot.com/
Wireshark: https://www.wireshark.org/download.html
Ollydbg v1.10: http://www.ollydbg.de/

2. Documents

https://www.joesandbox.com/analysis/1340122/1/html#behavior

https://www.virustotal.com/gui/file/5b7228947b256f36bd98dde1622799cda8f7a7aa0f3196aba08200fe8439dfee