



## ASSIGNMENT 2

# Table contents

<b>I. PART 2-1</b>	<b>3</b>
A. Basic Static	3
1. File Information	
File: juice.exe	3
2. Virus Total	3
3. PESTUDIO	
PeStudio shows multiple static properties and flags anomalies.	4
4. Prodot	
	8
B. Basic Dynamic	8
1. Process Explorer	9
2. Procmon	10
3. Wireshark	12
C. Advanced Static	13
IDA Professional 9.0	13
D. Advance Dynamic	18
OLLYDBG	18
E. Conclusion	20
F. Resources	21
1. Tools	21
2. Documents	21

## I. PART 2-1

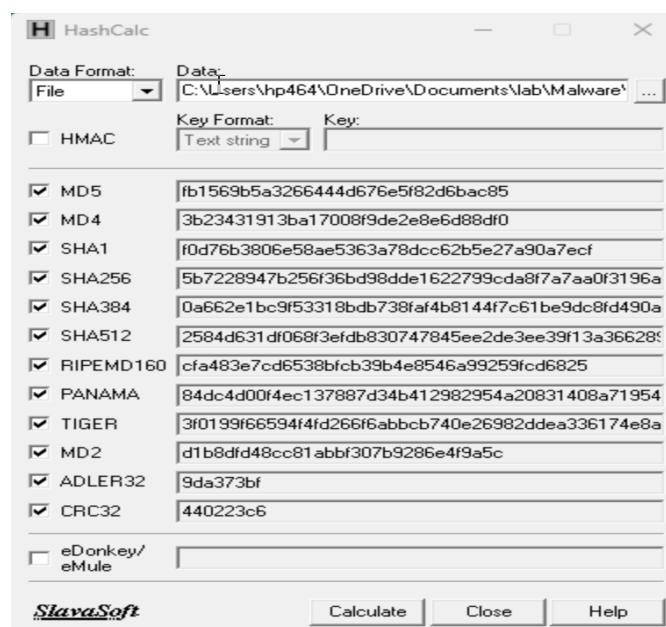
### A. Basic Static

#### 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

```

Compiler Products
[ASM] VS2002 (.NET) build 9466 count=2
[---] Unmarked objects count=47
[ C ] VS2002 (.NET) build 9466 count=1
[LNK] VS2002 (.NET) build 9466 count=1
id: 0x19, version: 9210 count=9

Header
Target Machine           Intel 386 or later processors and compatible processors
Compilation Timestamp    2004-01-27 11:22:58 UTC
Entry Point               44041
Contained Sections        2

```

### 3. PESTUDIO

PeStudio shows multiple static properties and flags anomalies.

#### a) Sections

Contained Sections: 2

property	value	value
section	section[0]	section[1]
name	.text	.data
footprint > sha256	E4CD9824F01D0D5E44FD129...	7072213A16EAFD04C96CE23...
entropy	6.910	3.184
file-ratio (97.62%)	double-click > jump	1.19 %
raw-address (begin)	0x00000400	0x0000A600
raw-address (end)	0x0000A600	0x0000A800
raw-size (41984 bytes)	0x0000A200 (41472 bytes)	0x00000200 (512 bytes)
virtual-address	0x00001000	0x0000C000
virtual-size (41314 bytes)	0x0000A0BE (41150 bytes)	0x000000A4 (164 bytes)
characteristics	0xE0040020	0xC0000040
write	x	x
execute	x	-
share	-	-
self-modifying	x	-
virtual	-	-
items		
directory > import	0x0000AD30	-
base-of-code	0x00001000	-
base-of-data	-	0x0000C000
entry-point	0x0000AC09	-

#### 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 `winnet.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\oned\indicators (virusto)

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	-	%6%
section:.text	-	format-string	-	Soft%sic%sf% sind%ss%sr%sv%so%sun
section:.text	-	format-string	-	G%5/ H%P/.%d.%u\%nH%: www%sic%so%sc%u\%r\%n
section:.text	-	format-string	-	www%sic%ss%6%so%cc
section:.text	-	file	-	KERNEL32.DLL
section:.text	-	file	-	ADVAPI32.dll
section:.text	-	file	-	USER32.dll
section:.text	-	import	-	CloseHandle
section:.text	-	-	-	.So

Activate Windows  
Go to Settings to activate Windows.

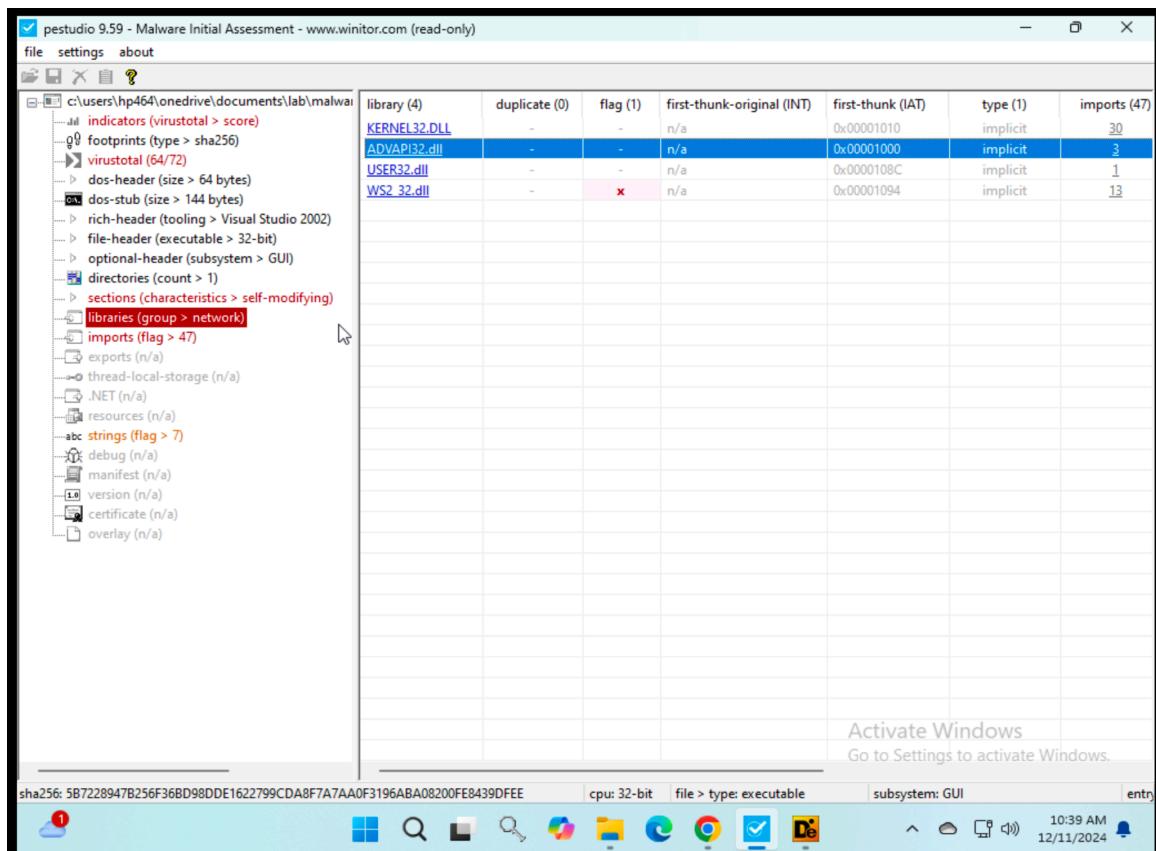
---

sha256: 5B7228947B256F36BD98DDE1622799CDA8F7A0A0F3196ABA08200FE8439DFEE

cpu: 32-bit file > type: executable subsystem: GUI entry

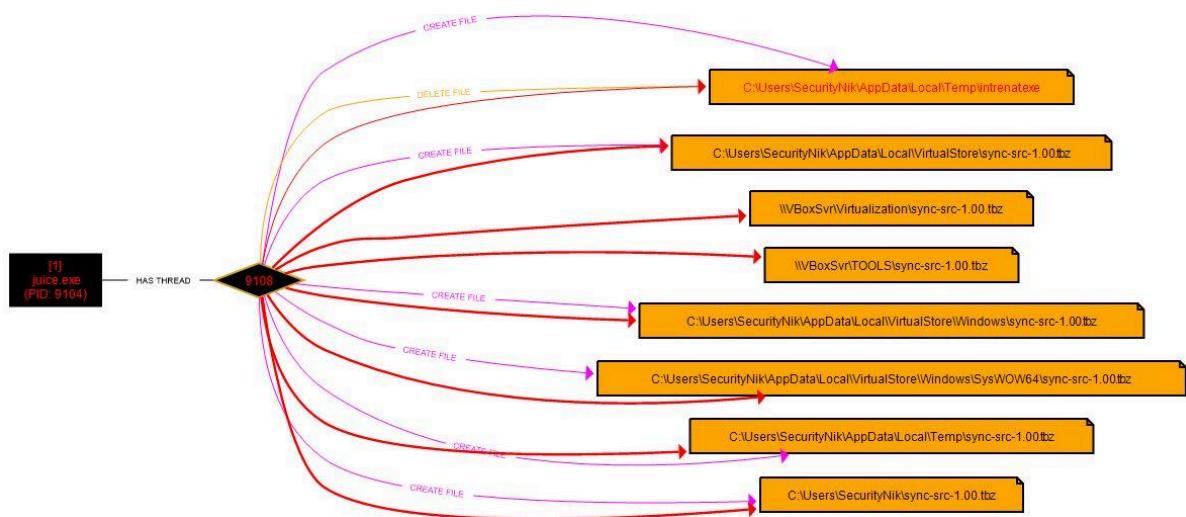
9:18 PM 12/12/2024

### c) Imports



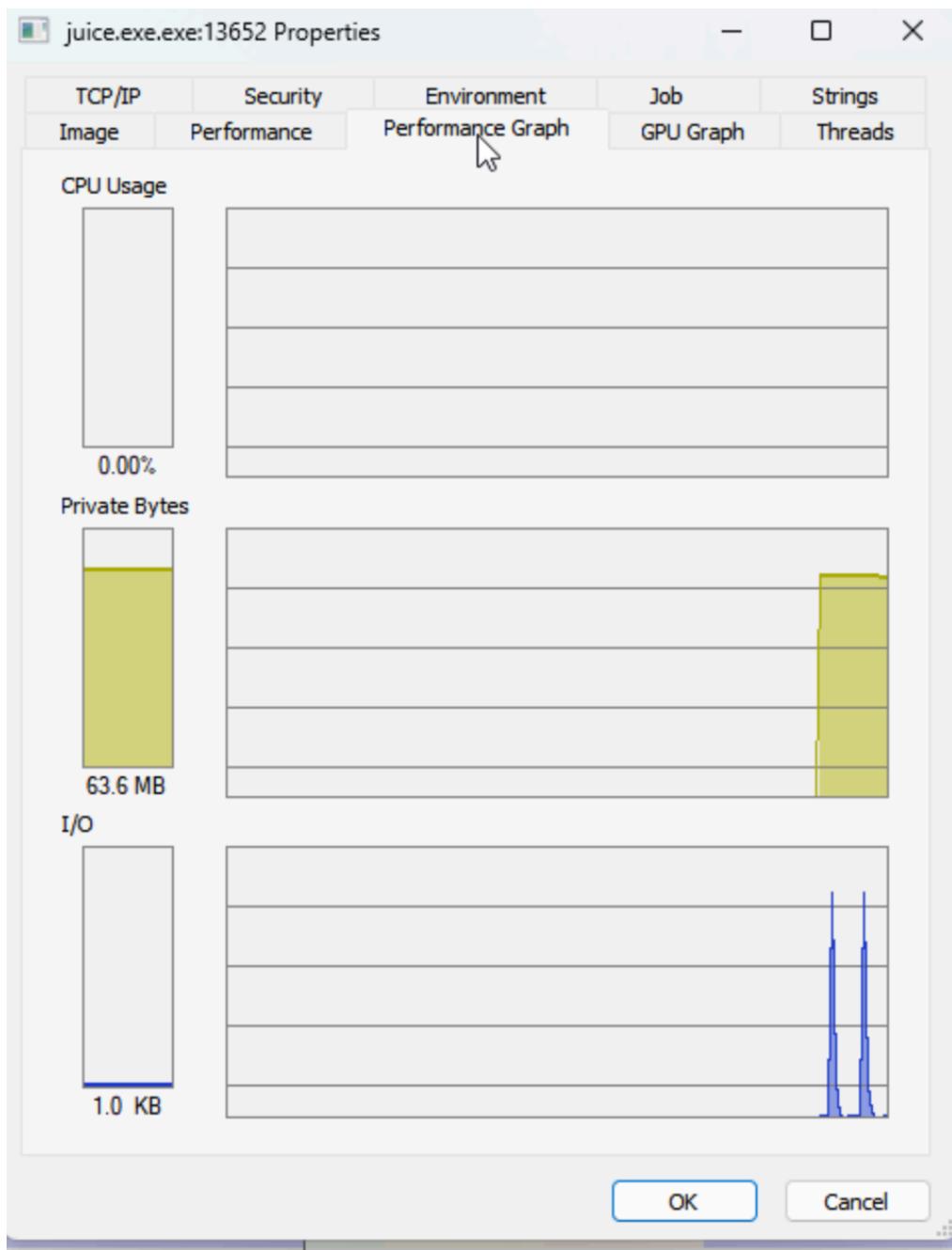
KERNEL32.DLL	ExitProcess, lstrcpyA, GetSystemTime, SetFileAttributesA, GetFileAttributesA, DeleteFileA, CopyFileA, CreateMutexA, GetLastError, GetDriveTypeA, lstrcatA, GetWindowsDirectoryA, GetSystemDirectoryA, GetTempPathA, GetEnvironmentVariableA, lstrlenA, Sleep, GetTickCount, GetProcAddress, LoadLibraryA, 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

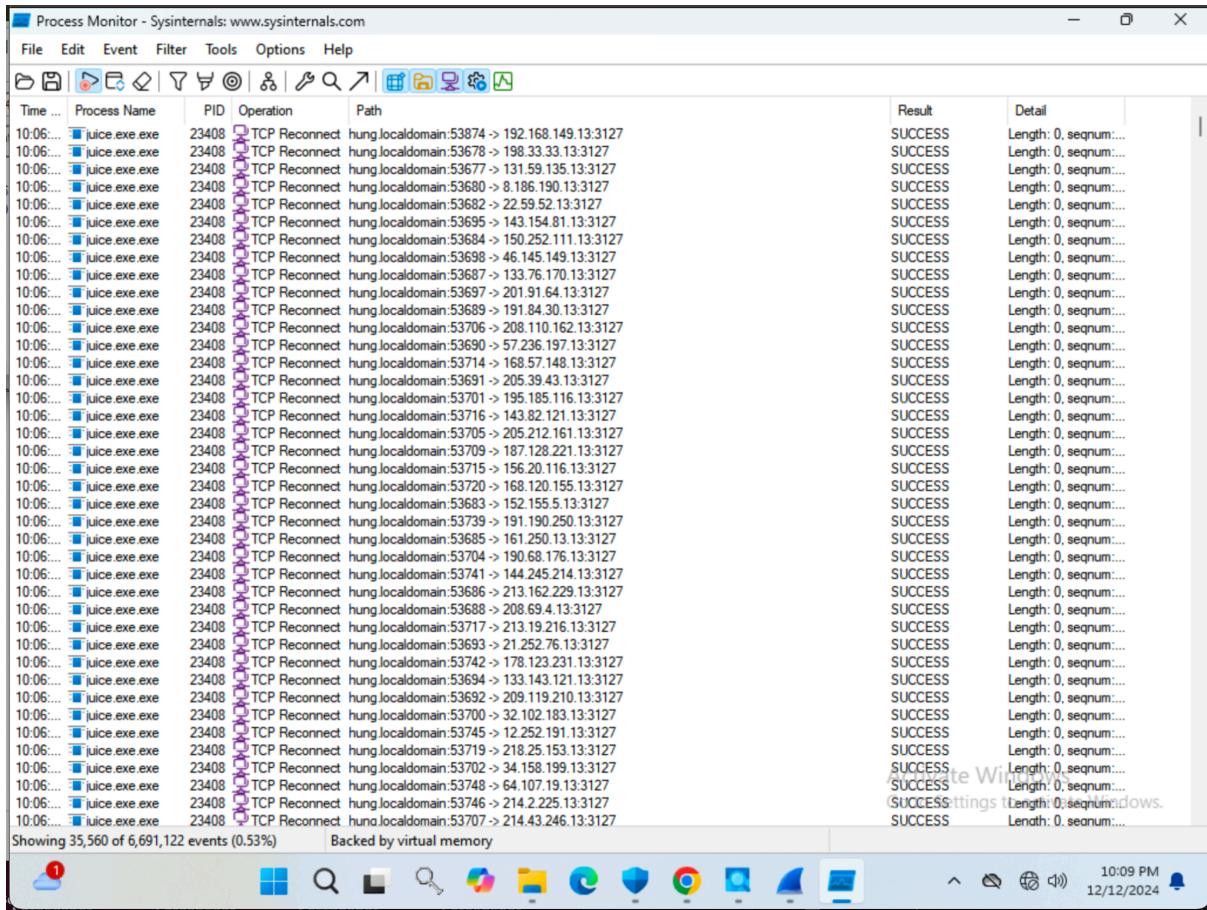


## B. Basic Dynamic

## 1. Process Explorer



## 2. Procmon



The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains icons for file operations like Open, Save, Print, and Filter. The main pane displays a table of network events. The columns are: Time ..., Process Name, PID, Operation, Path, Result, and Detail. The table lists numerous entries for the process "juice.exe.exe" (PID 23408) showing TCP Reconnect events. The "Path" column shows various IP addresses and ports, such as "hung localdomain:53874->192.168.149.13:3127" and "hung localdomain:53680->8.186.190.13:3127". The "Result" column is mostly "SUCCESS" with some entries like "Length: 0, seqnum:...". The "Detail" column shows details like "Length: 0, seqnum:...". At the bottom of the table, it says "Showing 35,560 of 6,691,122 events (0.53%) Backed by virtual memory". The status bar at the bottom right shows "10:09 PM 12/12/2024".

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: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:...

Windows 11 64-bit Arm

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Open

Process Name	PID	Operation	Path	Result	Detail
juice.exe.exe	2748	RegQueryValue	HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System\CopyFileOverlappedCount	NAME NOT FOUND	Length: 20
juice.exe.exe	2748	RegCloseKey	HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System	SUCCESS	
juice.exe.exe	2748	QueryAttribut...	C:\Windows\SysWOW64\ntrnrat.exe	SUCCESS	FileSystemAttribute...
juice.exe.exe	2748	ReadFile	C:\Users\hp464\OneDrive\Documents\final\11.12.2024 (1)\11.12.2024\part21\juice.exe.exe	SUCCESS	Offset: 0, Length: 4...
juice.exe.exe	2748	SetBasicInfor...	C:\Windows\SysWOW64\ntrnrat.exe	SUCCESS	CreationTime: 0, L...
juice.exe.exe	2748	QueryRemotePr...	C:\Windows\SysWOW64\ntrnrat.exe	INVALID PARAM...	
juice.exe.exe	2748	CloseFile	C:\Windows\SysWOW64\ntrnrat.exe	SUCCESS	
juice.exe.exe	2748	RegSetValue	C:\Users\hp464\OneDrive\Documents\final\11.12.2024 (1)\11.12.2024\part21\juice.exe.exe	SUCCESS	
juice.exe.exe	2748	RegQueryKey	HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Query: HandleTag...
juice.exe.exe	2748	RegOpenKey	HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Query: Name
juice.exe.exe	2748	RegSetInfoKey	HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: W...
juice.exe.exe	2748	RegQueryKey	HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\Gremlin	SUCCESS	KeySetInformation...
juice.exe.exe	2748	RegSetValue	HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\Gremlin	SUCCESS	Query: HandleTag...
juice.exe.exe	2748	RegCloseKey	HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Type: REG_SZ, Le...
juice.exe.exe	2748	CreateFile	C:\sync-src-1.00.tbz	SUCCESS	Desired Access: G...
juice.exe.exe	2748	WriteFile	C:\sync-src-1.00.tbz	SUCCESS	Offset: 0, Length: 2...
juice.exe.exe	2748	CloseFile	C:\sync-src-1.00.tbz	SUCCESS	
juice.exe.exe	2748	CreateFile	C:\Windows\sync-src-1.00.tbz	SUCCESS	Desired Access: G...
juice.exe.exe	2748	WriteFile	C:\Windows\sync-src-1.00.tbz	SUCCESS	Offset: 0, Length: 2...
juice.exe.exe	2748	CloseFile	C:\Windows\sync-src-1.00.tbz	SUCCESS	
juice.exe.exe	2748	CreateFile	C:\Windows\SyChpe32\sync-src-1.00.tbz	NAME NOT FOUND	Desired Access: R...
juice.exe.exe	2748	CreateFile	C:\Windows\SysWOW64\sync-src-1.00.tbz	SUCCESS	Desired Access: G...
juice.exe.exe	2748	WriteFile	C:\Windows\SysWOW64\sync-src-1.00.tbz	SUCCESS	Offset: 0, Length: 2...
juice.exe.exe	2748	CloseFile	C:\Windows\SysWOW64\sync-src-1.00.tbz	SUCCESS	
juice.exe.exe	2748	CreateFile	C:\Users\hp464\AppData\Local\Temp\sync-src-1.00.tbz	SUCCESS	Desired Access: G...
juice.exe.exe	2748	WriteFile	C:\Users\hp464\AppData\Local\Temp\sync-src-1.00.tbz	SUCCESS	Offset: 0, Length: 2...
juice.exe.exe	2748	CloseFile	C:\Users\hp464\AppData\Local\Temp\sync-src-1.00.tbz	SUCCESS	
juice.exe.exe	2748	CreateFile	C:\Users\hp464\sync-src-1.00.tbz	SUCCESS	Desired Access: G...
juice.exe.exe	2748	WriteFile	C:\Users\hp464\sync-src-1.00.tbz	SUCCESS	Offset: 0, Length: 2...
juice.exe.exe	2748	CloseFile	C:\Users\hp464\sync-src-1.00.tbz	SUCCESS	
juice.exe.exe	2748	Thread Create		SUCCESS	Thread ID: 4176
juice.exe.exe	2748	CreateFile	C:\sync-src-1.00.tbz	SUCCESS	Desired Access: G...
juice.exe.exe	2748	WriteFile	C:\sync-src-1.00.tbz	SUCCESS	Offset: 0, Length: 2...
juice.exe.exe	2748	CloseFile	C:\sync-src-1.00.tbz	SUCCESS	
juice.exe.exe	2748	CreateFile	C:\Windows\sync-src-1.00.tbz	SUCCESS	Desired Access: G...
juice.exe.exe	2748	WriteFile	C:\Windows\sync-src-1.00.tbz	SUCCESS	Offset: 0, Length: 2...
juice.exe.exe	2748	CloseFile	C:\Windows\sync-src-1.00.tbz	SUCCESS	
juice.exe.exe	2748	CreateFile	C:\Users\hp464\OneDrive\Documents\final\11.12.2024 (1)\11.12.2024\part21\wininet.dll	NAME NOT FOUND	Desired Access: R...
juice.exe.exe	2748	CloseFile	C:\Windows\sync-src-1.00.tbz	SUCCESS	
juice.exe.exe	2748	CreateFile	C:\Windows\SyChpe32\wininet.dll	SUCCESS	Desired Access: R...

## Create and Drop file

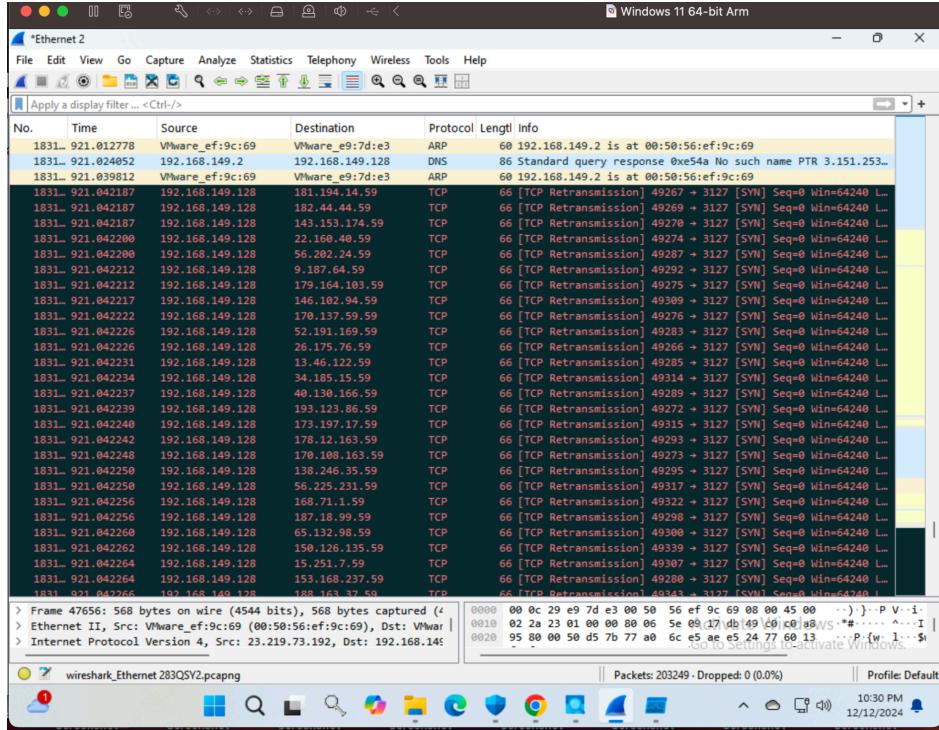
C:\User\hp464\sync-src-1.00.tbz

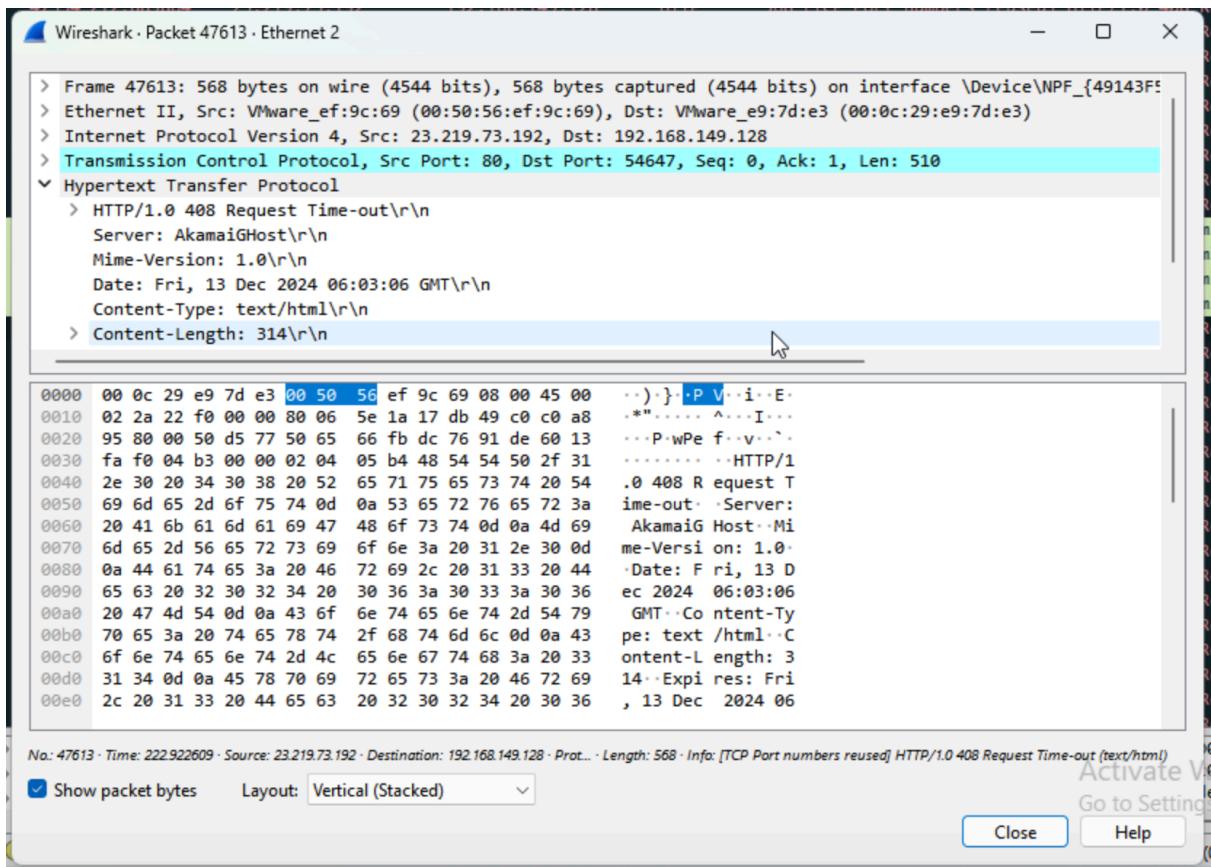
C:\Windows\SysWOW64\intrenat.exe

C:\Windows\SyChoe32\winet.dll

### 3. Wireshark

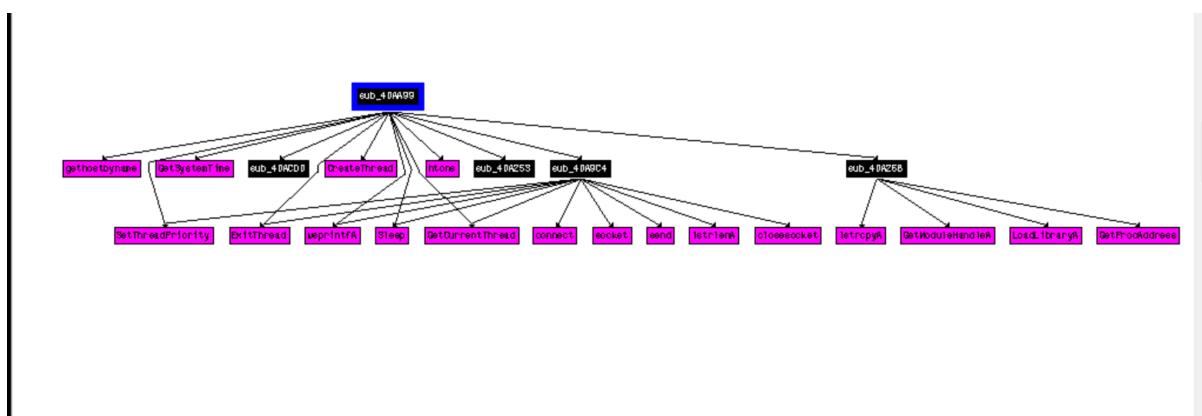
#### Connect Many I





## C. Advanced Static

IDA Professional 9.0



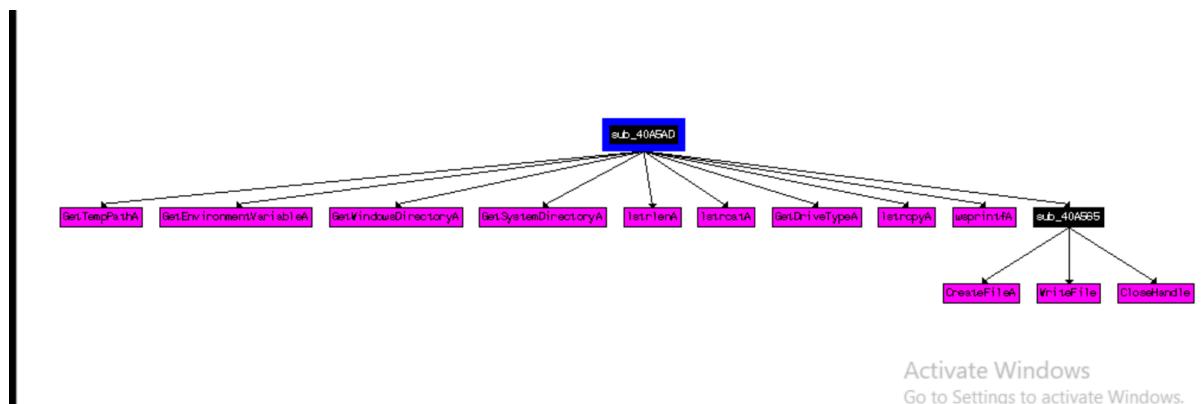
### Sub\_40AA99

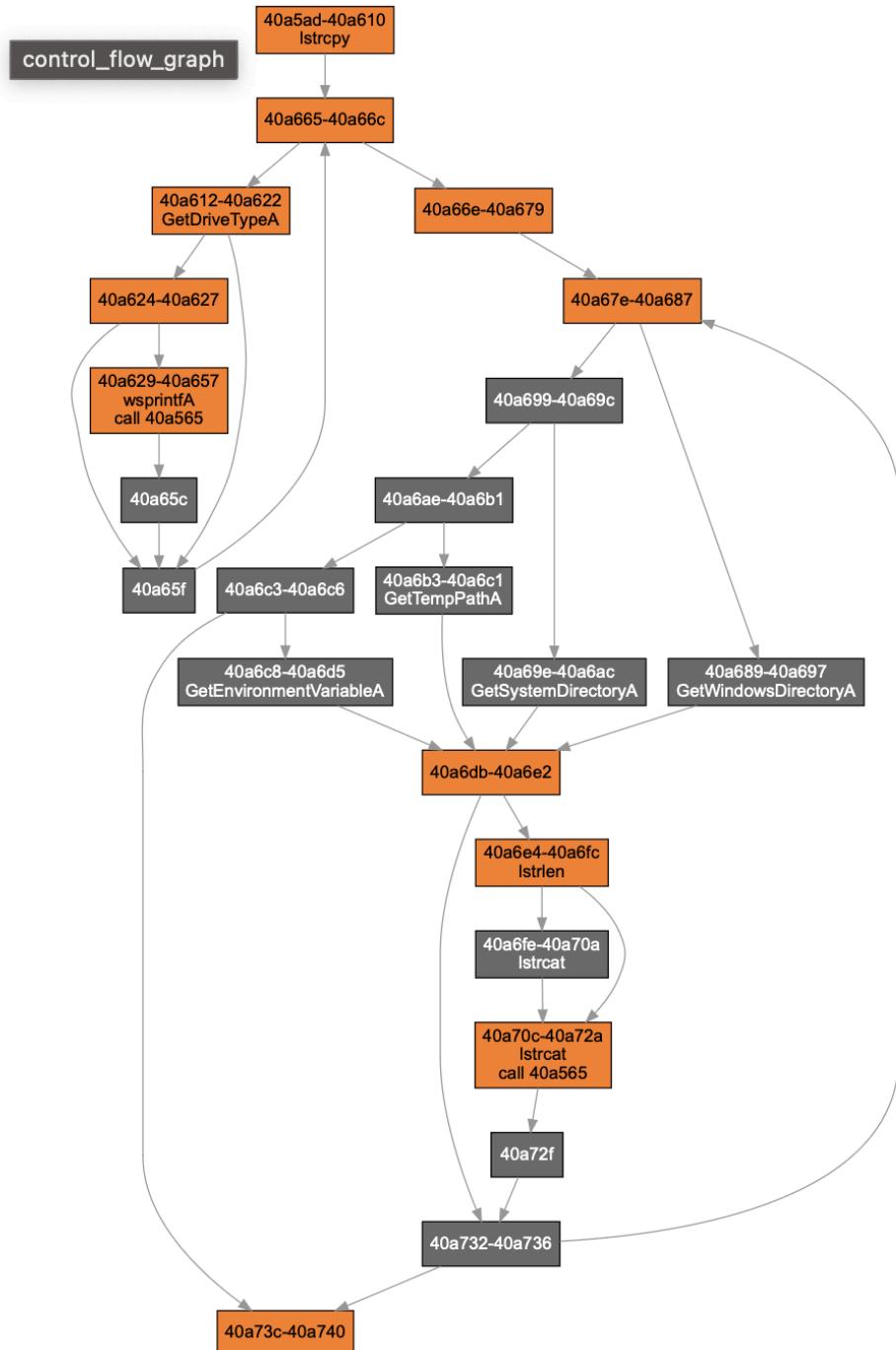
Sleep.KERNELBASE(000003E8), ref: 0040AB0C

- 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\_0000A9C4,00000002,00000000,?)**, ref: 0040ABEF
- **RtlExitUserThread.KERNEL32(00000000)**, ref: 0040AC02
- **ww%sic%ss%s%so%c**, xrefs: 0040AB40

## Sub\_40A5AD



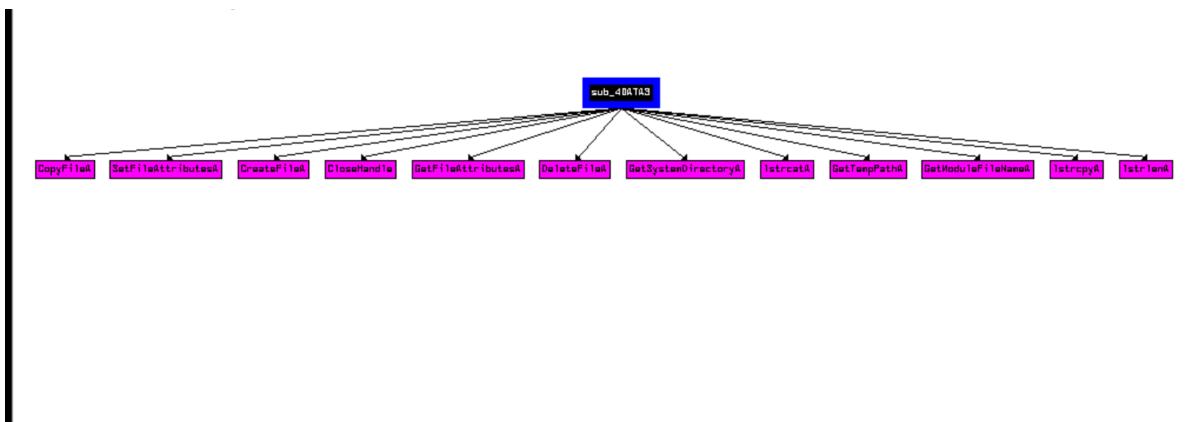


## APIs

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

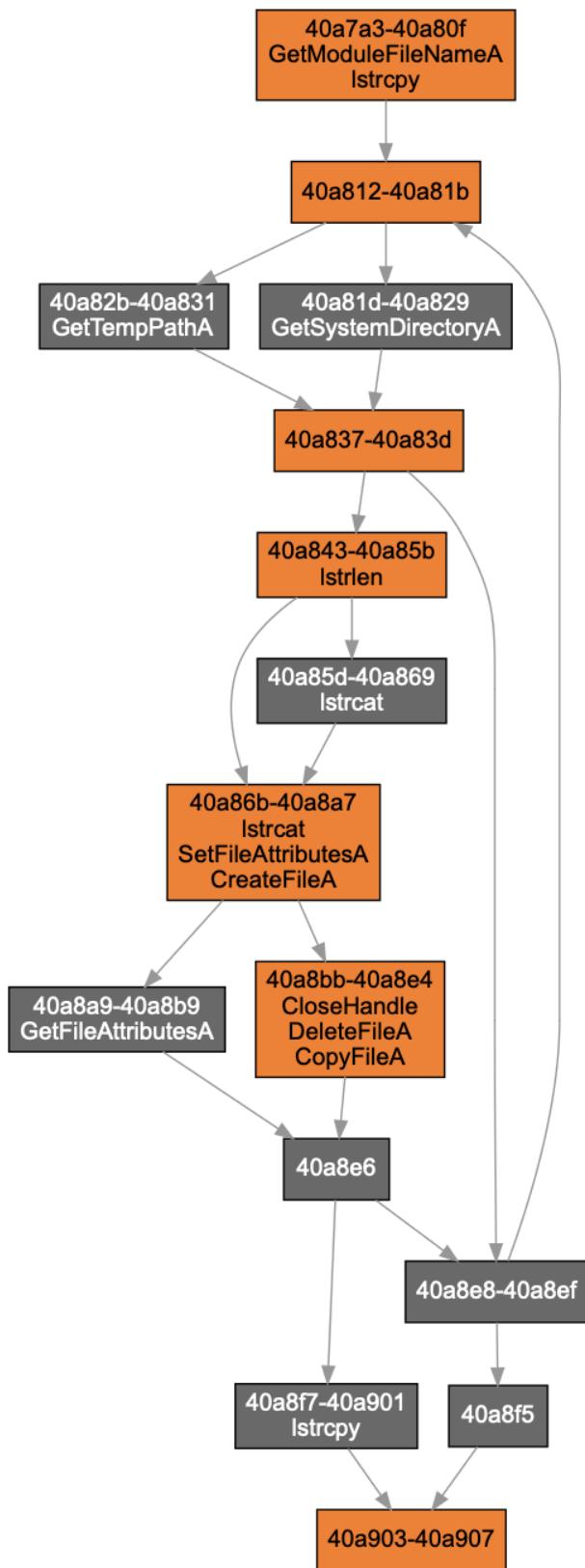
- **GetWindowsDirectoryA**.KERNEL32(00000000,00000100,?,0000 0000), ref: 0040A691
- **GetSystemDirectoryA**.KERNEL32(00000000,00000100), ref: 0040A6A6
- **GetTempPathA**.KERNEL32(00000100,00000000,?,00000000), ref: 0040A6BB
- **Istrlen**.KERNEL32(00000000,?,00000000), ref: 0040A6EB
- **Istrcat**.KERNEL32(00000000,0040A038), ref: 0040A70A
- **Istrcat**.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**



---

### Instructions



### APIs

- GetModuleFileNameA**.KERNEL32(00000000,?,00000104,?  
,00000000), ref: 0040A7F1
- **Istrcpy**.KERNEL32(00000200,?), ref: 0040A807
  - **GetSystemDirectoryA**.KERNEL32(?,00000118), ref:  
0040A823
  - **GetTempPathA**.KERNEL32(00000118,?,?,00000000), ref:  
0040A831
  - **Istrlen**.KERNEL32(?,?,00000000), ref: 0040A84A
  - **Istrcat**.KERNEL32(?,0040A038), ref: 0040A869
  - **Istrcat**.KERNEL32(?,intrenat.exe), ref: 0040A876
  - **SetFileAttributesA**.KERNELBASE(? ,00000020,?,00000000)  
, ref: 0040A881
  - **CreateFileA**.KERNELBASE(? ,40000000,00000003,0000000  
0,00000002,00000080,00000000,?,00000000), ref:  
0040A89E
  - **GetFileAttributesA**.KERNEL32(?, ?,00000000), ref:  
0040A8B0
  - **CloseHandle**.KERNEL32(00000000,?,00000000), ref:  
0040A8BC
  - **DeleteFileA**.KERNELBASE(?, ?,00000000), ref: 0040A8C9
  - **CopyFileA**.KERNEL32(?, ?,00000000), ref: 0040A8DE
  - **Istrcpy**.KERNEL32(00000200,?), ref: 0040A901

String

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

## D. Advance Dynamic

OLLYDBG

CreateFileA

C:\Windows\SysWOW64\intrenat.exe

OllyDbg - juice.exe

File View Debug Options Window Help

C CPU - main thread, module juice

```

00400548 > 33DB XOR EBX, EBX
00400549 > 8040 F8 XER ECX, DWORD PTR SS:[EBP-10]
0040054A > 48 8D 4C EC LODD PTR SS:[EBP-9],BL
0040054B > E8 76FDFFF CALL juice.<0040A2CB>
00400555 > .43 INC EBX
00400556 > 81FB FF000000 CMP EBX,0FF
00400557 > 7E 01 JE SHORT juice.<0040A54A>
0040055E > E8 BSFEDFFF CALL juice.<0040A418>
00400563 > ^EB A5 JMP SHORT juice.<0040A50A>
00400565 > .43 INC EBX
00400566 > 8BED MOV EBX,ESP
00400568 > 51 PUSH ECX
00400569 > 55 PUSH ESI
0040056A > 64 00 PUSH EDI
0040056B > 64 00 PUSH ECX
00400571 > .64 02 PUSH 2
00400573 > .64 00 PUSH 0
00400575 > .64 00 PUSH 0
00400577 > .64 00 PUSH 0
00400579 > .64 00 PUSH 0
0040057A > .64 00 PUSH 0
0040057C > .64 00 PUSH 0
0040057D > .64 00 PUSH 0
0040057E > .64 00 PUSH 0
0040057F > .64 00 PUSH 0
00400581 > .64 00 PUSH 0
00400583 > .64 00 PUSH 0
00400585 > .64 00 PUSH 0
00400587 > .64 00 PUSH 0
00400588 > .64 00 PUSH 0
00400589 > .74 1F TEST ESI,ESI
0040058A > .74 05 JE SHORT juice.<0040A5AA>
00400590 > .64 00 PUSH 0
00400592 > 8045 FC LEA ECX,DWORD PTR SS:[EBP-4]
00400595 > .59 PUSH ECX
00400597 > .FF75 0C PUSH DWORD PTR SS:[EBP+10]
00400599 > .FF75 0C PUSH DWORD PTR SS:[EBP+C]
0040059C > .56 PUSH ESI
0040059D > FF15 84104000 CALL DWORD PTR DS:[&KERNEL32.WriteFile]
0040059E > .56 PUSH ESI
0040059F > .5E LEAVE
004005A0 > C3 RETN
004005A2 > .55 PUSH EBX
004005A3 > 8BED MOV EBX,ESP

```

Registers (FPU)

ERX	0019FB88	ASCII "c:\Windows\system32\intrenat.exe"
ECX	00000000	
EDX	00000000	
EBX	00277000	
ESP	0019FAC8	
EBP	0019FCB8	
EDS	7544C800	KERNEL32!lstrcpyA
EDI	0040A500	KERNEL32!lstrcpyA
EIP	0040059E	juice.<0040A59E>

Stack

C 0	ES 0023	32bit 0xFFFFFFFF
A 0	CS 0018	32bit 0xFFFFFFFF
D 1	SS 0023	32bit 0xFFFFFFFF
F 0	DS 0023	32bit 0xFFFFFFFF
T 0	FS 0028	32bit 0xFFFFFFFF
G 0	GS 0023	32bit 0xFFFFFFFF

Registers

D 0	LastErr	ERROR_SUCCESS (00000000)
EFL	00000242	(NO,NB,E,BE,NS,PO,GE,LE)
ST0	empty	0,0
ST1	empty	0,0
ST2	empty	0,0
ST3	empty	0,0
ST4	empty	0,0
ST5	empty	0,0
ST6	empty	0,0
ST7	empty	0,0

Call Stack

FST	0000	Cond 0 0 0 0 Err 0 0 0 0 Z O I
FCM	027F	Freq NEAR,53 Mask 1 1 1 1 1

File

Activate Windows

Breakpoint at juice.<0040A59E>

Paused

11:33 PM  
12/12/2024

## Create sync-src-1.00.tbz

OllyDbg - juice.exe

File View Debug Options Window Help

C CPU - main thread, module juice

```

00400548 > 33DB XOR EBX, EBX
00400549 > 8040 F8 XER ECX, DWORD PTR SS:[EBP-10]
0040054A > 48 8D 4C EC LODD PTR SS:[EBP-9],BL
0040054B > E8 76FDFFF CALL juice.<0040A2CB>
00400555 > .43 INC EBX
00400556 > 81FB FF000000 CMP EBX,0FF
00400557 > 7E 01 JE SHORT juice.<0040A54A>
0040055E > E8 BSFEDFFF CALL juice.<0040A418>
00400563 > ^EB A5 JMP SHORT juice.<0040A50A>
00400565 > .43 INC EBX
00400566 > 8BED MOV EBX,ESP
00400568 > 51 PUSH ECX
00400569 > 55 PUSH ESI
0040056A > 64 00 PUSH EDI
0040056B > 64 00 PUSH ECX
00400571 > .64 02 PUSH 2
00400573 > .64 00 PUSH 0
00400575 > .64 00 PUSH 0
00400577 > .64 00 PUSH 0
00400579 > .64 00 PUSH 0
0040057C > .64 00 PUSH 0
0040057D > .64 00 PUSH 0
0040057E > .64 00 PUSH 0
0040057F > .64 00 PUSH 0
00400581 > .64 00 PUSH 0
00400583 > .64 00 PUSH 0
00400585 > .64 00 PUSH 0
00400587 > .64 00 PUSH 0
00400588 > .64 00 PUSH 0
00400589 > .74 1F TEST ESI,ESI
0040058A > .74 05 JE SHORT juice.<0040A5AA>
00400590 > .64 00 PUSH 0
00400592 > 8045 FC LEA ECX,DWORD PTR SS:[EBP-4]
00400595 > .59 PUSH ECX
00400597 > .FF75 0C PUSH DWORD PTR SS:[EBP+10]
00400599 > .FF75 0C PUSH DWORD PTR SS:[EBP+C]
0040059C > .56 PUSH ESI
0040059D > FF15 84104000 CALL DWORD PTR DS:[&KERNEL32.WriteFile]
0040059E > .56 PUSH ESI
0040059F > .5E LEAVE
004005A0 > C3 RETN
004005A2 > .55 PUSH EBX
004005A3 > 8BED MOV EBX,ESP

```

Registers (FPU)

ERX	0019F968	ASCII "c:\sync-src-1.00.tbz"
ECX	00000000	
EDX	00000000	
EBX	00277000	
ESP	0019F960	
EBP	0019F984	
EDS	00000000	
EDI	0040A500	
EIP	0040057F	juice.<ModuleEntryPoint>

Stack

C 0	ES 0023	32bit 0xFFFFFFFF
A 0	CS 0018	32bit 0xFFFFFFFF
D 1	SS 0023	32bit 0xFFFFFFFF
F 0	DS 0023	32bit 0xFFFFFFFF
T 0	FS 0028	32bit 0xFFFFFFFF
G 0	GS 0023	32bit 0xFFFFFFFF

Registers

D 0	LastErr	ERROR_SUCCESS (00000000)
EFL	00000246	(NO,NB,E,BE,NS,PE,GE,LE)
ST0	empty	0,0
ST1	empty	0,0
ST2	empty	0,0
ST3	empty	0,0
ST4	empty	0,0
ST5	empty	0,0
ST6	empty	0,0
ST7	empty	0,0

Call Stack

FST	0000	Cond 0 0 0 0 Err 0 0 0 0 Z O I
FCM	027F	Freq NEAR,53 Mask 1 1 1 1 1

File

Activate Windows

Breakpoint at juice.<0040A57F>

Paused

## 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 Professional: <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>