NAME: Adeyemi Akande

REG NO: 2024/INT/EH/3800

INTRODUCTION

In this lab, I gained practical exposure to real-world malware investigation processes. My documentation relies heavily on screenshots captured during each stage of the analysis, demonstrating both the workflow and the findings that highlight how TeslaCrypt executes, conceals its payload, and impacts infected systems. The primary objective was to identify and unpack the ransomware's structure, detect the use of custom packers, and examine its runtime behavior through memory dumping. Tools such as PEStudio, xdbg debugger, and Process Hacker were employed to uncover hidden functionality, extract indicators of compromise (IoCs), and better understand the ransomware's infection strategy.

TOOLS USED

PE Studio,

PEid,

CFF Explorer,

Binary Ninja,

IDA,

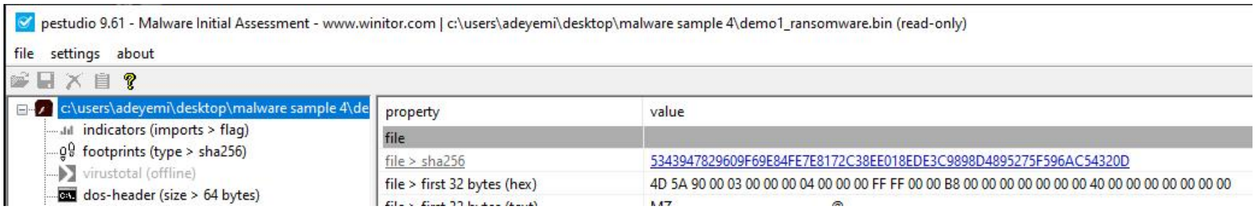
Ghidra,

X32dbg,

Process Hacker.

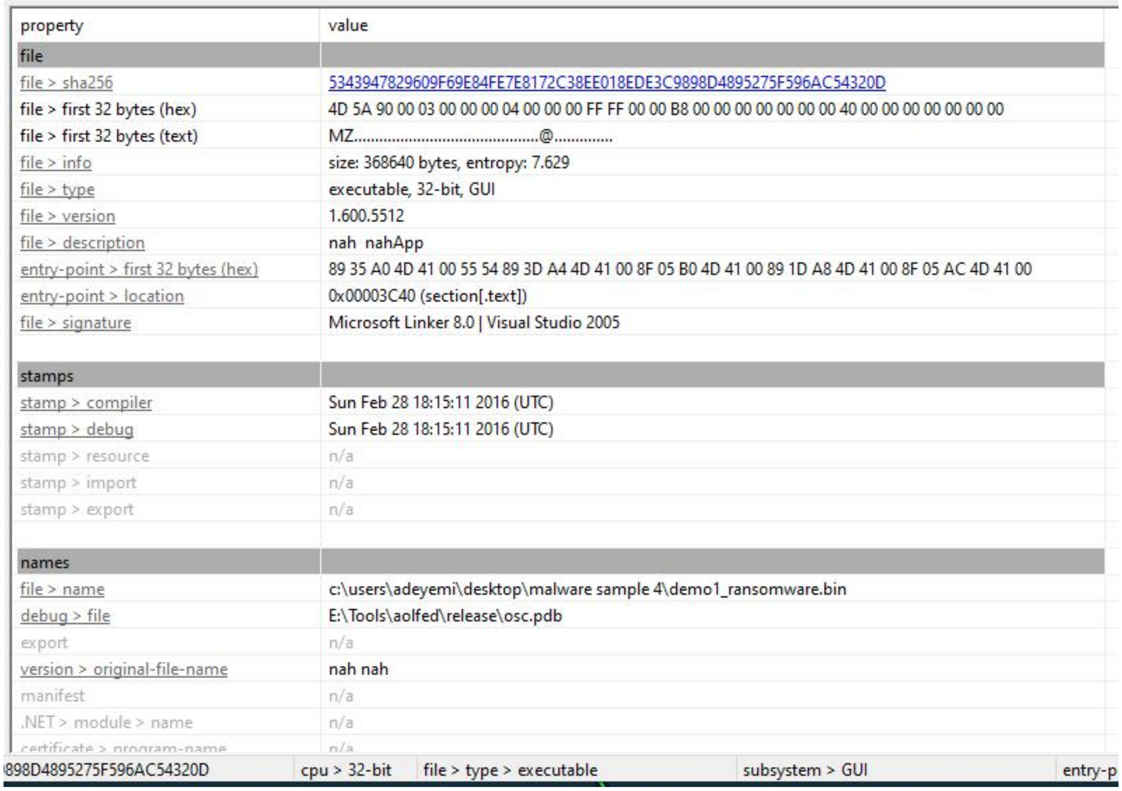
I used multiple tool to solidify my findings

FILE IDENTIFICATION BY PE STUDIO


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\adeyemi\desktop\malware sample 4\demo1_ransomware.bin (read-only)

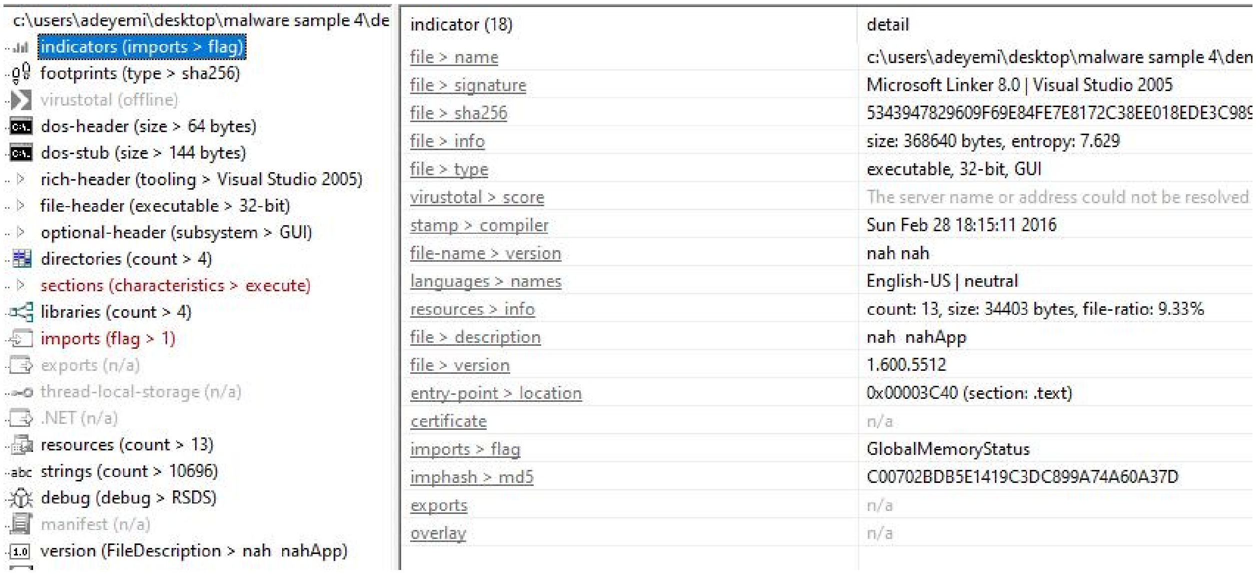
file
settings
about
c:\users\adeyemi\desktop\malware sample 4\de
indicators (imports > flag)
footprints (type > sha256)
virustotal (offline)
dos-header (size > 64 bytes)

property	value
file	
file > sha256	5343947829609F69E84FE7E8172C38EE018EDE3C9898D4895275F596AC54320D
file > first 32 bytes (hex)	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00



property	value
file	
file > sha256	5343947829609F69E84FE7E8172C38EE018EDE3C9898D4895275F596AC54320D
file > first 32 bytes (hex)	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
file > first 32 bytes (text)	MZ..@..............
file > info	size: 368640 bytes, entropy: 7.629
file > type	executable, 32-bit, GUI
file > version	1.600.5512
file > description	nah nahApp
entry-point > first 32 bytes (hex)	89 35 A0 4D 41 00 55 54 89 3D A4 4D 41 00 8F 05 B0 4D 41 00 89 1D A8 4D 41 00 8F 05 AC 4D 41 00
entry-point > location	0x00003C40 (section[.text])
file > signature	Microsoft Linker 8.0 | Visual Studio 2005
stamps	
stamp > compiler	Sun Feb 28 18:15:11 2016 (UTC)
stamp > debug	Sun Feb 28 18:15:11 2016 (UTC)
stamp > resource	n/a
stamp > import	n/a
stamp > export	n/a
names	
file > name	c:\users\adeyemi\desktop\malware sample 4\demo1_ransomware.bin
debug > file	E:\Tools\aolfed\release\osc.pdb
export	n/a
version > original-file-name	nah nah
manifest	n/a
.NET > module > name	n/a
certificate > program-name	n/a

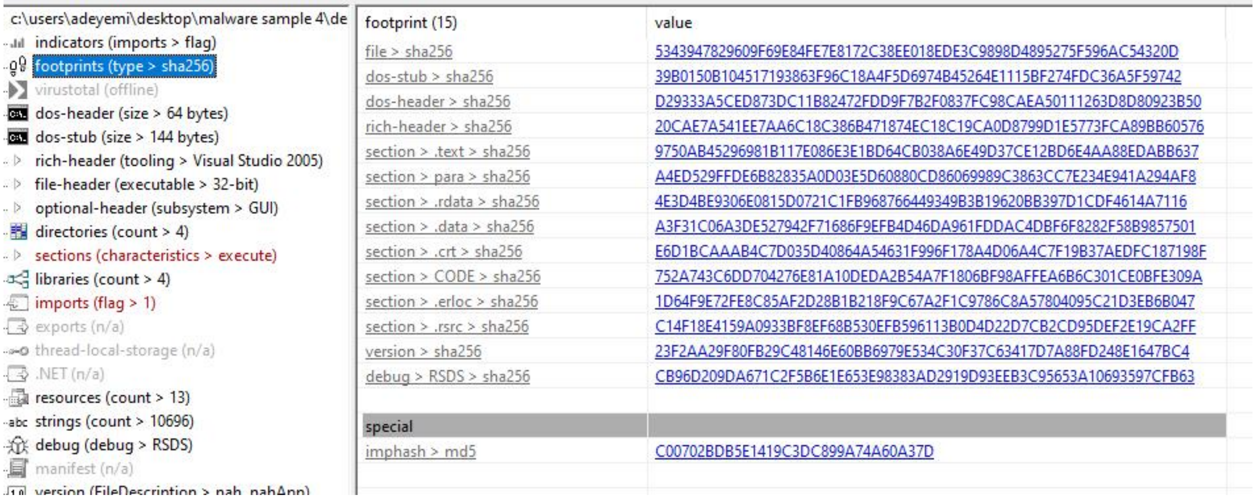
898D4895275F596AC54320D | cpu > 32-bit | file > type > executable | subsystem > GUI | entry-p



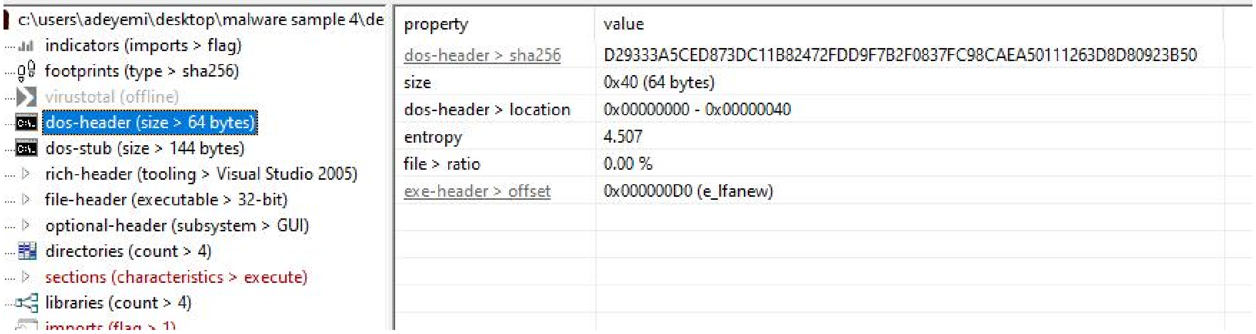
c:\users\adeyemi\desktop\malware sample 4\de

- indicators (imports > flag)
- footprints (type > sha256)
- virustotal (offline)
- dos-header (size > 64 bytes)
- dos-stub (size > 144 bytes)
- rich-header (tooling > Visual Studio 2005)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 4)
- sections (characteristics > execute)
- libraries (count > 4)
- imports (flag > 1)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (count > 13)
- strings (count > 10696)
- debug (debug > RSDS)
- manifest (n/a)
- version (FileDescription > nah nahApp)

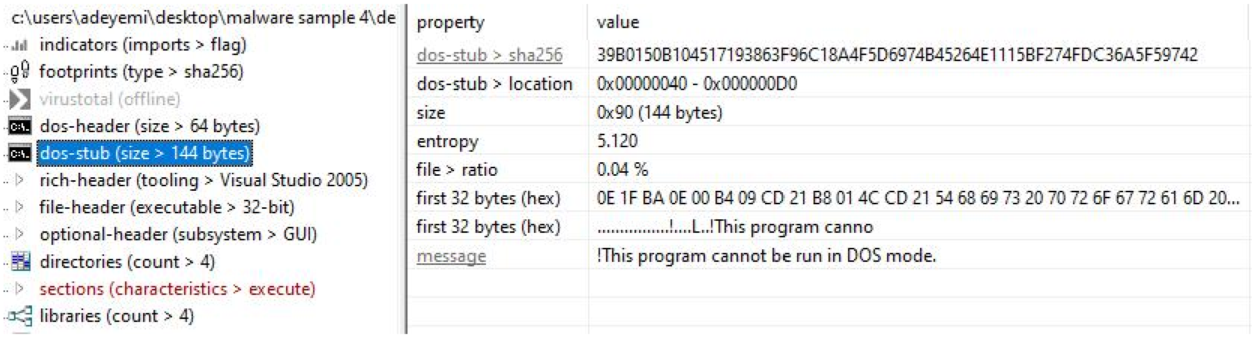
indicator (18)	detail
file > name	c:\users\adeyemi\desktop\malware sample 4\den
file > signature	Microsoft Linker 8.0 | Visual Studio 2005
file > sha256	5343947829609F69E84FE7E8172C38EE018EDE3C989
file > info	size: 368640 bytes, entropy: 7.629
file > type	executable, 32-bit, GUI
virustotal > score	The server name or address could not be resolved
stamp > compiler	Sun Feb 28 18:15:11 2016
file-name > version	nah nah
languages > names	English-US | neutral
resources > info	count: 13, size: 34403 bytes, file-ratio: 9.33%
file > description	nah nahApp
file > version	1.600.5512
entry-point > location	0x00003C40 (section: .text)
certificate	n/a
imports > flag	GlobalMemoryStatus
imphash > md5	C00702BDB5E1419C3DC899A74A60A37D
exports	n/a
overlay	n/a


c:\users\adeyemi\desktop\malware sample 4\de
indicators (imports > flag)
footprints (type > sha256)
virustotal (offline)
dos-header (size > 64 bytes)
dos-stub (size > 144 bytes)
rich-header (tooling > Visual Studio 2005)
file-header (executable > 32-bit)
optional-header (subsystem > GUI)
directories (count > 4)
sections (characteristics > execute)
libraries (count > 4)
imports (flag > 1)
exports (n/a)
thread-local-storage (n/a)
.NET (n/a)
resources (count > 13)
strings (count > 10696)
debug (debug > RSDS)
manifest (n/a)
version (FileDescription > nah, nahApp)

footprint (15)	value
file > sha256	5343947829609F69E84FE7E8172C38EE018EDE3C9898D4895275F596AC54320D
dos-stub > sha256	39B0150B104517193863F96C18A4F5D6974B45264E1115BF274FDC36A5F59742
dos-header > sha256	D29333A5CED873DC11B82472FDD9F7B2F0837FC98CAEA50111263D8D80923B50
rich-header > sha256	20CAE7A541EE7AA6C18C386B471874EC18C19CA0D8799D1E5773FCA89BB60576
section > .text > sha256	9750AB45296981B117E086E3E1BD64CB038A6E49D37CE12BD6E4AA88EDABB637
section > para > sha256	A4ED529FFDE6B82835A0D03E5D60880CD86069989C3863CC7E234E941A294AF8
section > .rdata > sha256	4E3D4BE9306E0815D0721C1FB968766449349B3B19620BB397D1CDF4614A7116
section > .data > sha256	A3F31C06A3DE527942F71686F9EFB4D46DA961FDDAC4DBF6F8282F58B9857501
section > .crt > sha256	E6D1BCAAAB4C7D035D40864A54631F996F178A4D06A4C7F19B37AEDFC187198F
section > CODE > sha256	752A743C6DD704276E81A10DEDA2B54A7F1806BF98AFFEA6B6C301CE0BFE309A
section > .erloc > sha256	1D64F9E72FE8C85AF2D28B1B218F9C67A2F1C9786C8A57804095C21D3EB6B047
section > .rsrc > sha256	C14F18E4159A0933BF8EF68B530EFB596113B0D4D22D7CB2CD95DEF2E19CA2FF
version > sha256	23F2AA29F80FB29C48146E60BB6979E534C30F37C63417D7A88FD248E1647BC4
debug > RSDS > sha256	CB96D209DA671C2F5B6E1E653E98383AD2919D93EEB3C95653A10693597CFB63
special	
imphash > md5	C00702BDB5E1419C3DC899A74A60A37D

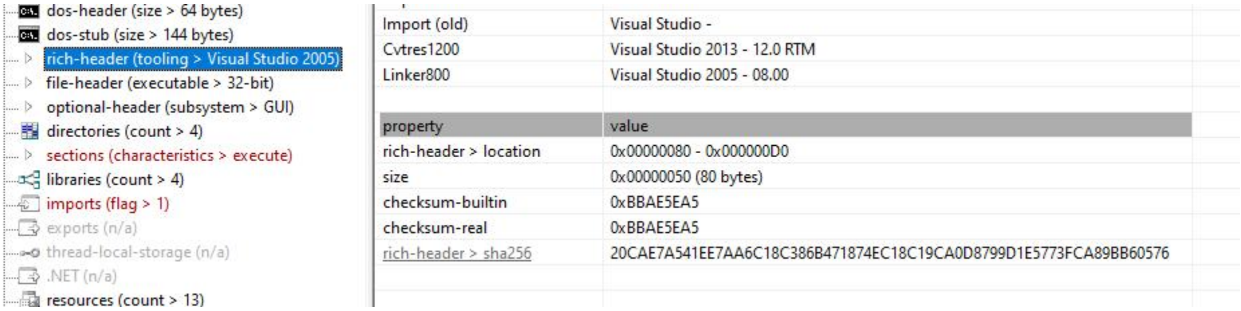

c:\users\adeyemi\desktop\malware sample 4\de
indicators (imports > flag)
footprints (type > sha256)
virustotal (offline)
dos-header (size > 64 bytes)
dos-stub (size > 144 bytes)
rich-header (tooling > Visual Studio 2005)
file-header (executable > 32-bit)
optional-header (subsystem > GUI)
directories (count > 4)
sections (characteristics > execute)
libraries (count > 4)
imports (flag > 1)

property	value
dos-header > sha256	D29333A5CED873DC11B82472FDD9F7B2F0837FC98CAEA50111263D8D80923B50
size	0x40 (64 bytes)
dos-header > location	0x00000000 - 0x00000040
entropy	4.507
file > ratio	0.00 %
exe-header > offset	0x000000D0 (e_lfanew)


c:\users\adeyemi\desktop\malware sample 4\de
indicators (imports > flag)
footprints (type > sha256)
virustotal (offline)
dos-header (size > 64 bytes)
dos-stub (size > 144 bytes)
rich-header (tooling > Visual Studio 2005)
file-header (executable > 32-bit)
optional-header (subsystem > GUI)
directories (count > 4)
sections (characteristics > execute)
libraries (count > 4)

property	value
dos-stub > sha256	39B0150B104517193863F96C18A4F5D6974B45264E1115BF274FDC36A5F59742
dos-stub > location	0x00000040 - 0x000000D0
size	0x90 (144 bytes)
entropy	5.120
file > ratio	0.04 %
first 32 bytes (hex)	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20...
first 32 bytes (hex)	................!.....L..!This program canno
message	!This program cannot be run in DOS mode.

Binary Memory location

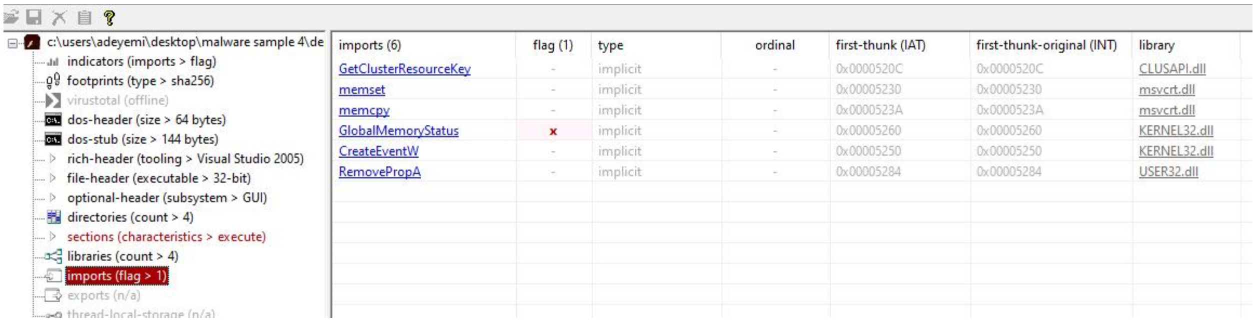


- dos-header (size > 64 bytes)
- dos-stub (size > 144 bytes)
- rich-header (tooling > Visual Studio 2005)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 4)
- sections (characteristics > execute)
- libraries (count > 4)
- imports (flag > 1)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (count > 13)

Import (old)	Visual Studio -
Cvtres1200	Visual Studio 2013 - 12.0 RTM
Linker800	Visual Studio 2005 - 08.00

property	value
rich-header > location	0x00000080 - 0x000000D0
size	0x00000050 (80 bytes)
checksum-builtin	0xBBAE5EA5
checksum-real	0xBBAE5EA5
rich-header > sha256	20CAE7A541EE7AA6C18C386B471874EC18C19CA0D8799D1E5773FCA89BB60576

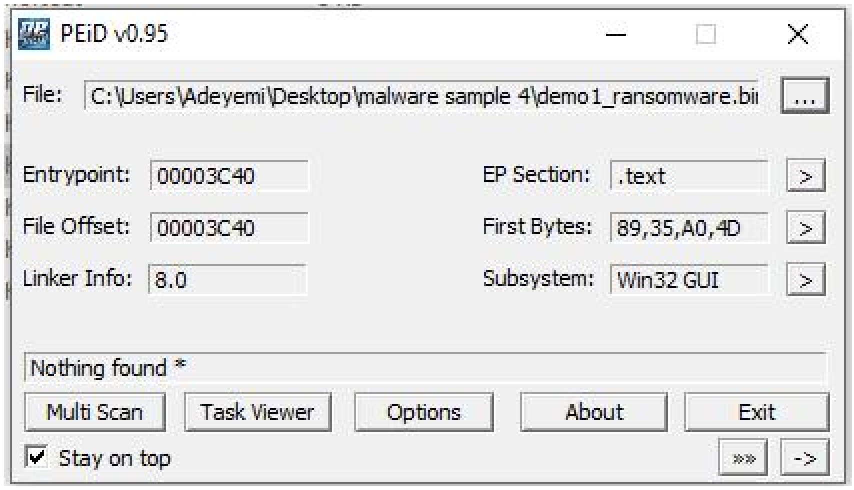
Import flag



- c:\users\adeyemi\desktop\malware sample 4\de
- indicators (imports > flag)
- footprints (type > sha256)
- virustotal (offline)
- dos-header (size > 64 bytes)
- dos-stub (size > 144 bytes)
- rich-header (tooling > Visual Studio 2005)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 4)
- sections (characteristics > execute)
- libraries (count > 4)
- imports (flag > 1)
- exports (n/a)
- thread-local-storage (n/a)

imports (6)	flag (1)	type	ordinal	first-thunk (IAT)	first-thunk-original (INT)	library
GetClusterResourceKey	-	implicit	-	0x0000520C	0x0000520C	CLUSAPI.dll
memset	-	implicit	-	0x00005230	0x00005230	msvcrt.dll
memcpy	-	implicit	-	0x0000523A	0x0000523A	msvcrt.dll
GlobalMemoryStatus	x	implicit	-	0x00005260	0x00005260	KERNEL32.dll
CreateEventW	-	implicit	-	0x00005250	0x00005250	KERNEL32.dll
RemovePropA	-	implicit	-	0x00005284	0x00005284	USER32.dll

PEid investigation



PEiD v0.95

File: C:\Users\Adeyemi\Desktop\malware sample 4\demo1_ransomware.bi

Entrypoint: 00003C40

EP Section: .text

File Offset: 00003C40

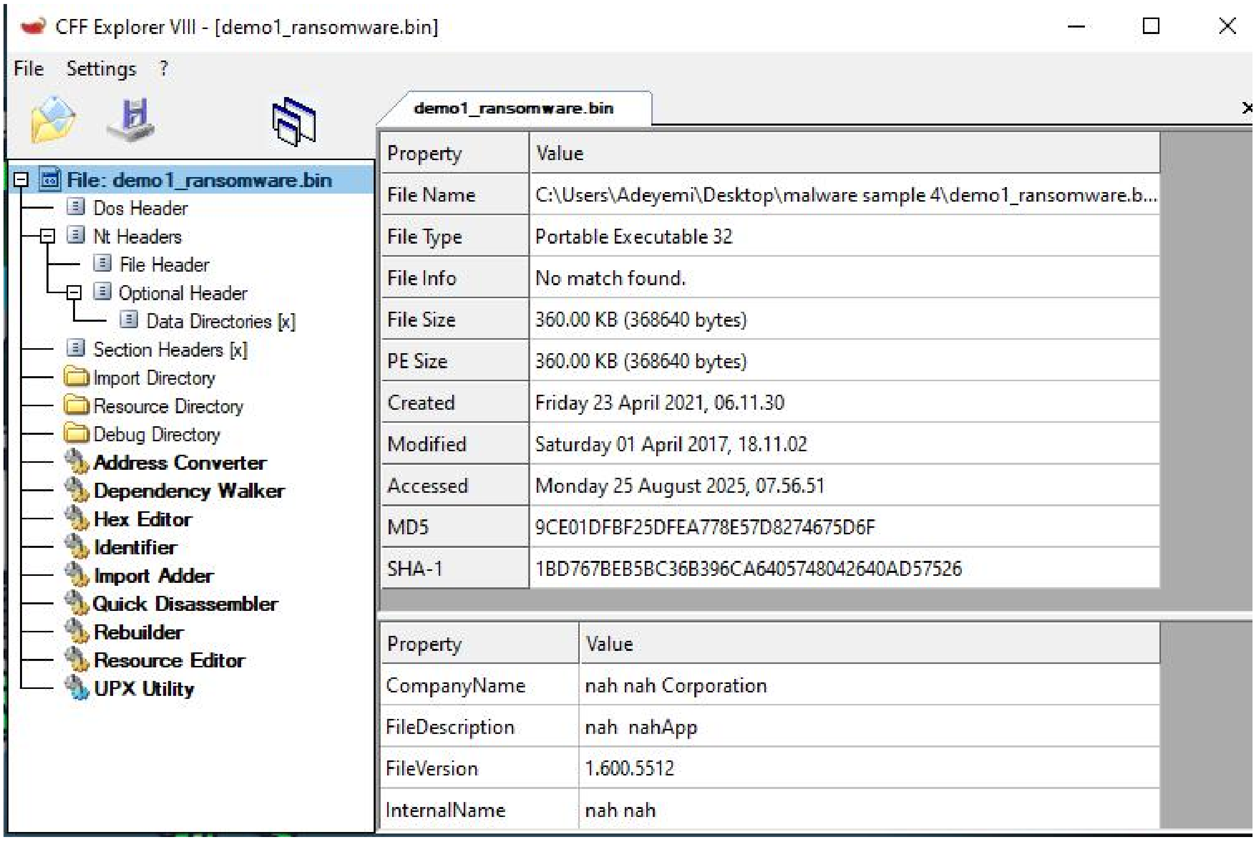
First Bytes: 89,35,A0,4D

Linker Info: 8.0

Subsystem: Win32 GUI

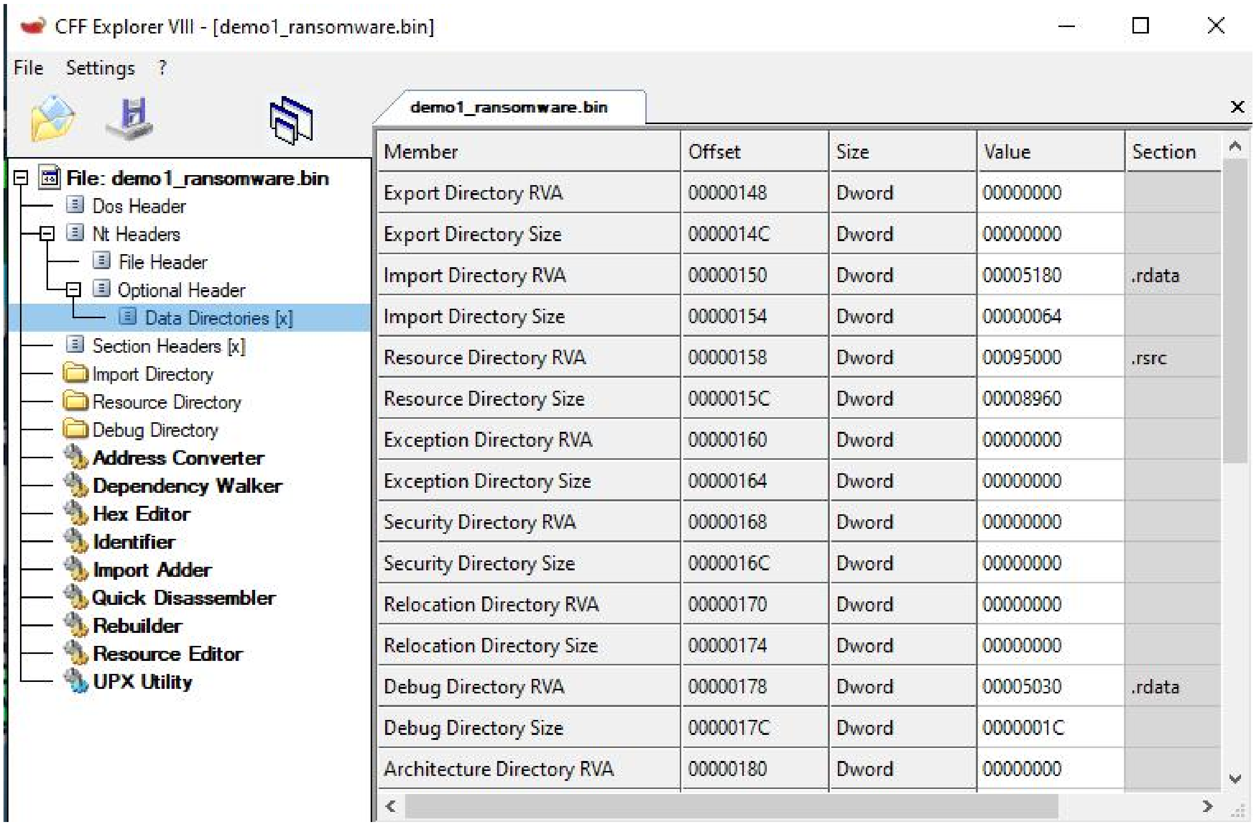
Nothing found *

Examination from CFF Explorer

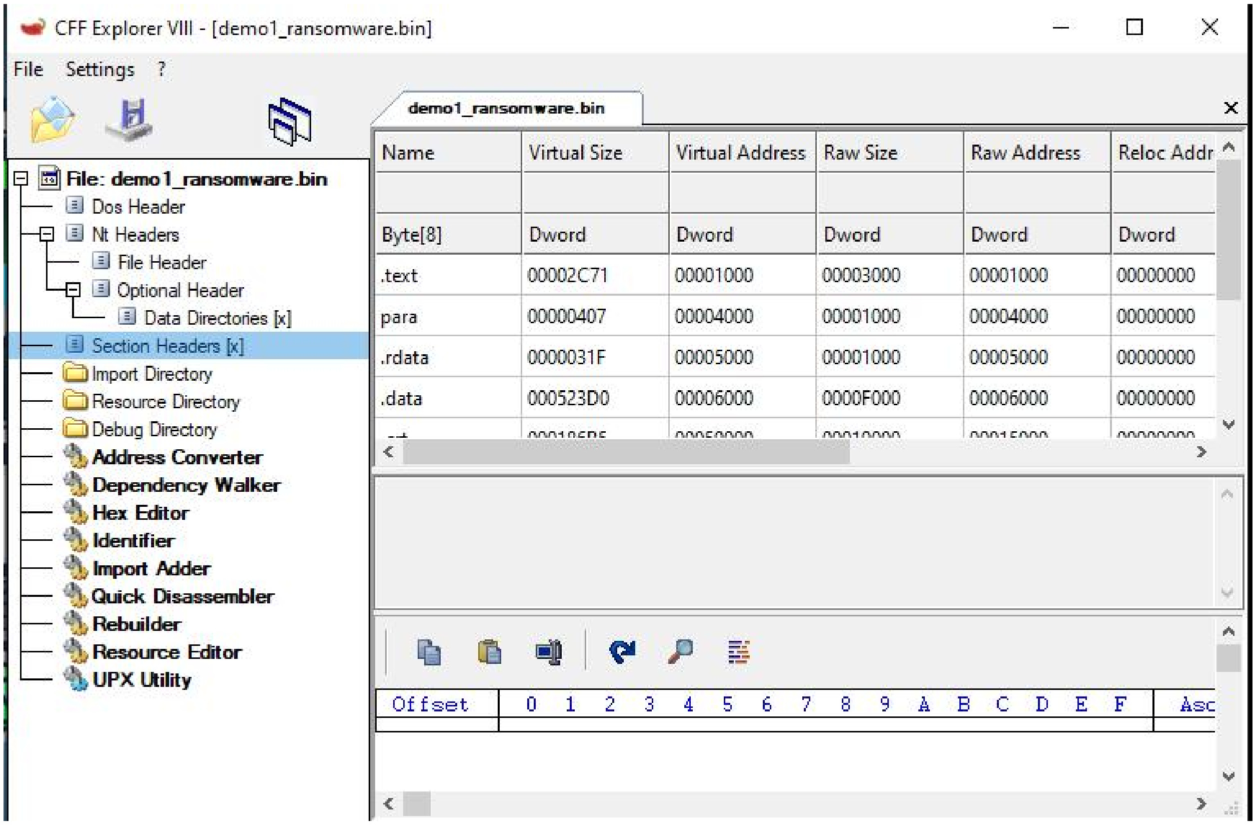


Property	Value
File Name	C:\Users\Adeyemi\Desktop\malware sample 4\demo1_ransomware.b...
File Type	Portable Executable 32
File Info	No match found.
File Size	360.00 KB (368640 bytes)
PE Size	360.00 KB (368640 bytes)
Created	Friday 23 April 2021, 06.11.30
Modified	Saturday 01 April 2017, 18.11.02
Accessed	Monday 25 August 2025, 07.56.51
MD5	9CE01DFBF25DFEA778E57D8274675D6F
SHA-1	1BD767BEB5BC36B396CA6405748042640AD57526

Property	Value
CompanyName	nah nah Corporation
FileDescription	nah nahApp
FileVersion	1.600.5512
InternalName	nah nah

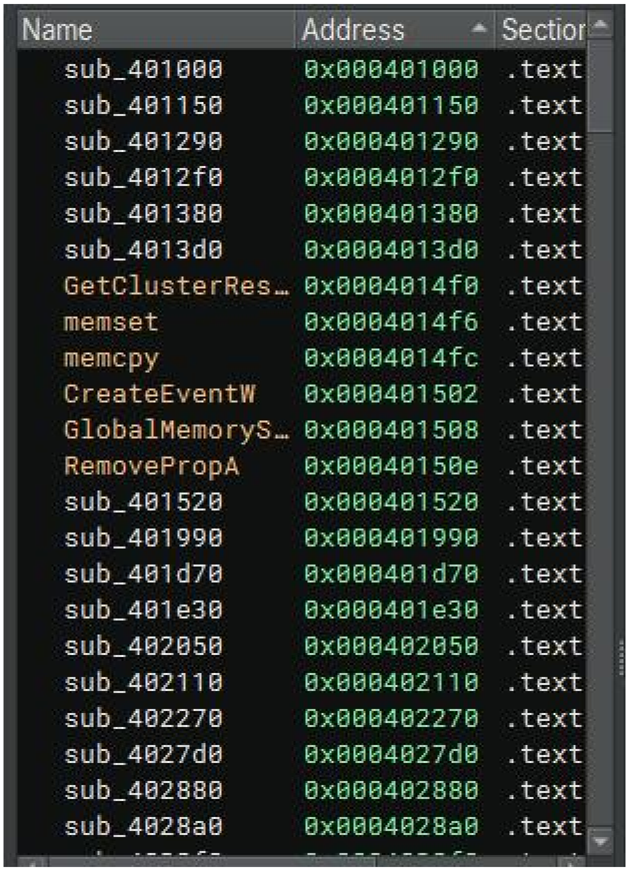


Member	Offset	Size	Value	Section
Export Directory RVA	00000148	Dword	00000000	
Export Directory Size	0000014C	Dword	00000000	
Import Directory RVA	00000150	Dword	00005180	.rdata
Import Directory Size	00000154	Dword	00000064	
Resource Directory RVA	00000158	Dword	00095000	.rsrc
Resource Directory Size	0000015C	Dword	00008960	
Exception Directory RVA	00000160	Dword	00000000	
Exception Directory Size	00000164	Dword	00000000	
Security Directory RVA	00000168	Dword	00000000	
Security Directory Size	0000016C	Dword	00000000	
Relocation Directory RVA	00000170	Dword	00000000	
Relocation Directory Size	00000174	Dword	00000000	
Debug Directory RVA	00000178	Dword	00005030	.rdata
Debug Directory Size	0000017C	Dword	0000001C	
Architecture Directory RVA	00000180	Dword	00000000	

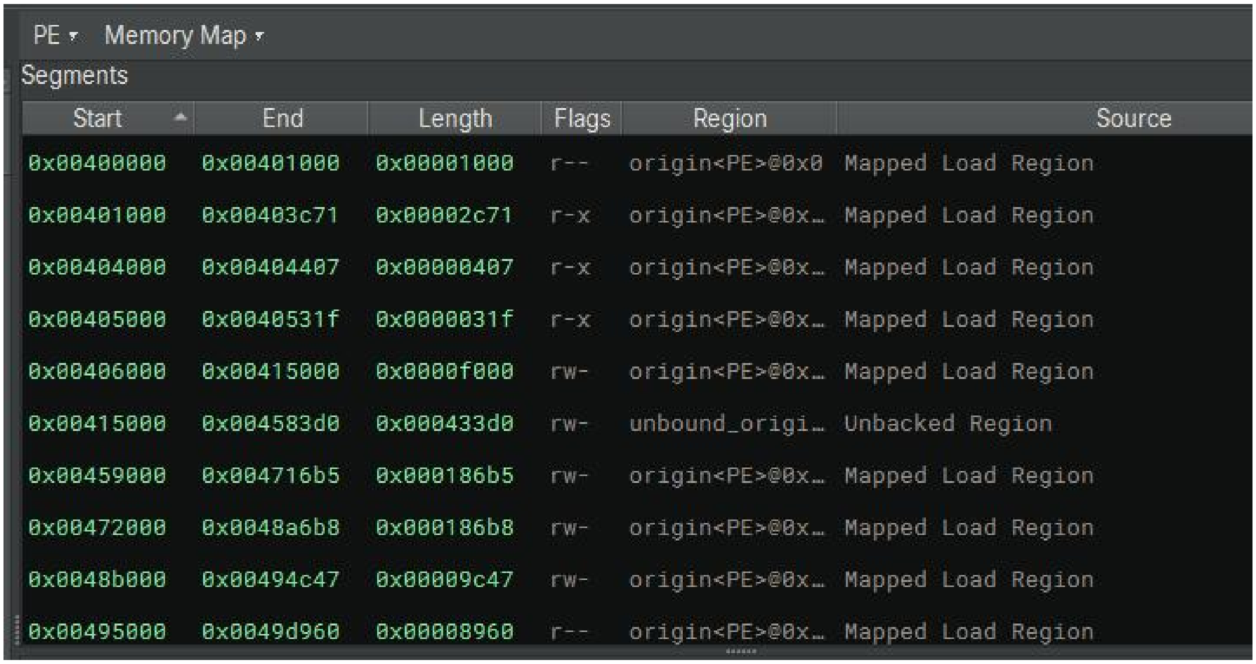


Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Addr
Byte[8]	Dword	Dword	Dword	Dword	Dword
.text	00002C71	00001000	00003000	00001000	00000000
para	00000407	00004000	00001000	00004000	00000000
.rdata	0000031F	00005000	00001000	00005000	00000000
.data	000523D0	00006000	0000F000	00006000	00000000
[illegible]	000186B5	00059000	00010000	00015000	00000000

Binary ninja was able to identify important memory location as shown below

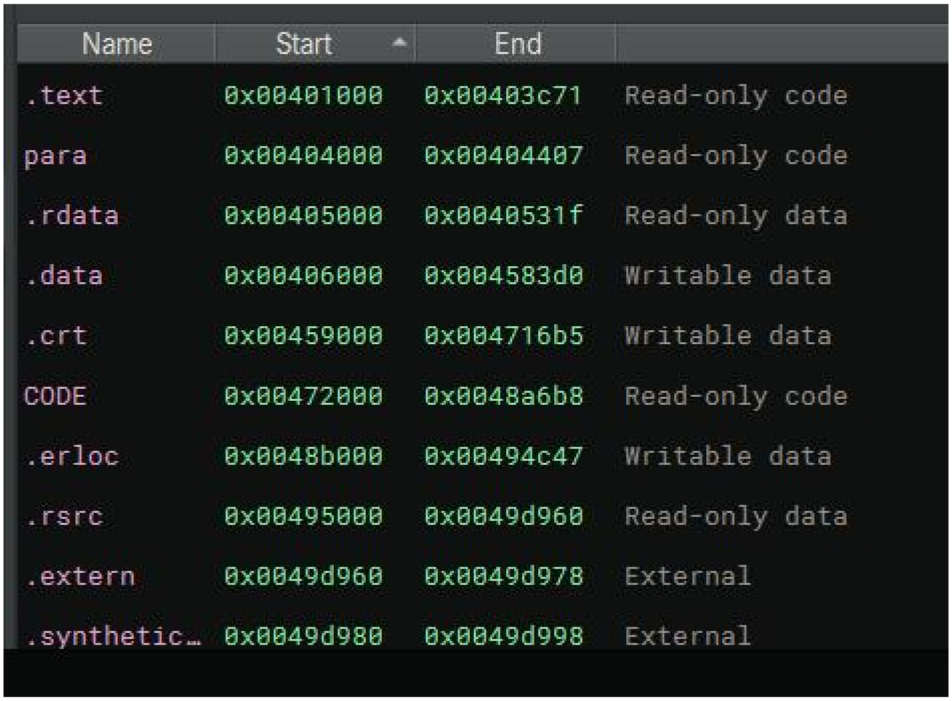


Name	Address	Sectior
sub_401000	0x000401000	.text
sub_401150	0x000401150	.text
sub_401290	0x000401290	.text
sub_4012f0	0x0004012f0	.text
sub_401380	0x000401380	.text
sub_4013d0	0x0004013d0	.text
GetClusterRes…	0x0004014f0	.text
memset	0x0004014f6	.text
memcpy	0x0004014fc	.text
CreateEventW	0x000401502	.text
GlobalMemoryS…	0x000401508	.text
RemovePropA	0x00040150e	.text
sub_401520	0x000401520	.text
sub_401990	0x000401990	.text
sub_401d70	0x000401d70	.text
sub_401e30	0x000401e30	.text
sub_402050	0x000402050	.text
sub_402110	0x000402110	.text
sub_402270	0x000402270	.text
sub_4027d0	0x0004027d0	.text
sub_402880	0x000402880	.text
sub_4028a0	0x0004028a0	.text

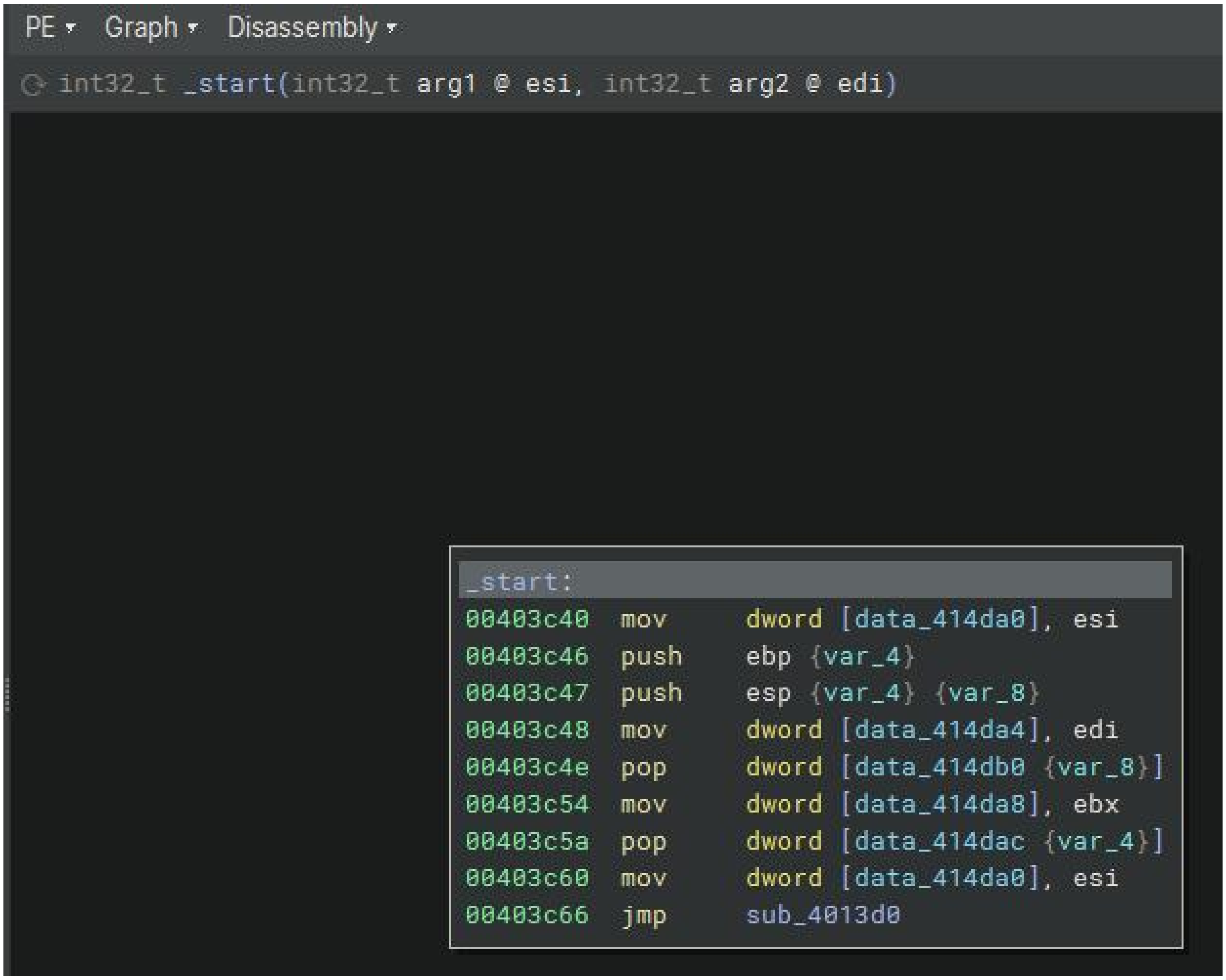


Segments

Start	End	Length	Flags	Region	Source
0x00400000	0x00401000	0x00001000	r--	origin<PE>@0x0	Mapped Load Region
0x00401000	0x00403c71	0x00002c71	r-x	origin<PE>@0x…	Mapped Load Region
0x00404000	0x00404407	0x00000407	r-x	origin<PE>@0x…	Mapped Load Region
0x00405000	0x0040531f	0x0000031f	r-x	origin<PE>@0x…	Mapped Load Region
0x00406000	0x00415000	0x0000f000	rw-	origin<PE>@0x…	Mapped Load Region
0x00415000	0x004583d0	0x000433d0	rw-	unbound_origi…	Unbacked Region
0x00459000	0x004716b5	0x000186b5	rw-	origin<PE>@0x…	Mapped Load Region
0x00472000	0x0048a6b8	0x000186b8	rw-	origin<PE>@0x…	Mapped Load Region
0x0048b000	0x00494c47	0x00009c47	rw-	origin<PE>@0x…	Mapped Load Region
0x00495000	0x0049d960	0x00008960	r--	origin<PE>@0x…	Mapped Load Region

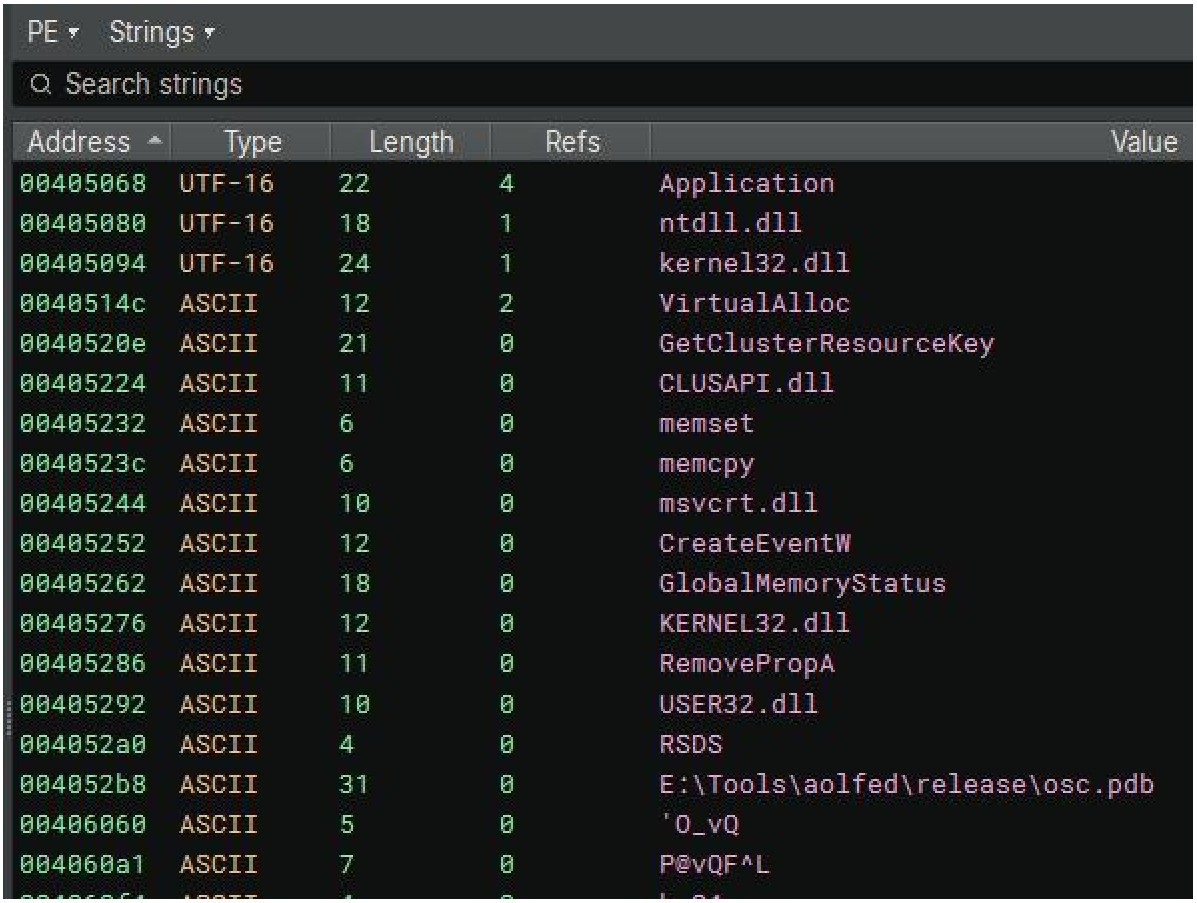


Name	Start	End	
.text	0x00401000	0x00403c71	Read-only code
para	0x00404000	0x00404407	Read-only code
.rdata	0x00405000	0x0040531f	Read-only data
.data	0x00406000	0x004583d0	Writable data
.crt	0x00459000	0x004716b5	Writable data
CODE	0x00472000	0x0048a6b8	Read-only code
.erloc	0x0048b000	0x00494c47	Writable data
.rsrc	0x00495000	0x0049d960	Read-only data
.extern	0x0049d960	0x0049d978	External
.synthetic…	0x0049d980	0x0049d998	External



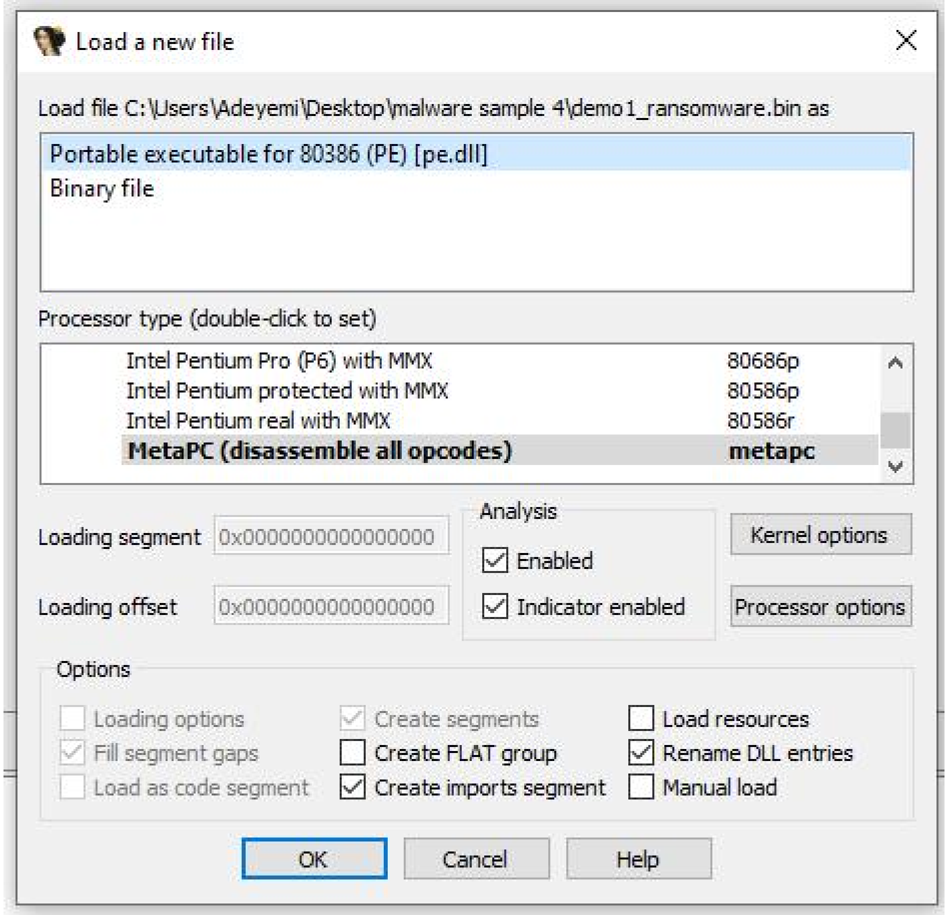
```
int32_t _start(int32_t arg1 @ esi, int32_t arg2 @ edi)

_start:
00403c40  mov     dword [data_414da0], esi
00403c46  push    ebp {var_4}
00403c47  push    esp {var_4} {var_8}
00403c48  mov     dword [data_414da4], edi
00403c4e  pop     dword [data_414db0 {var_8}]
00403c54  mov     dword [data_414da8], ebx
00403c5a  pop     dword [data_414dac {var_4}]
00403c60  mov     dword [data_414da0], esi
00403c66  jmp     sub_4013d0
```

Important string identified in binary ninja



Address ▲	Type	Length	Refs	Value
00405068	UTF-16	22	4	Application
00405080	UTF-16	18	1	ntdll.dll
00405094	UTF-16	24	1	kernel32.dll
0040514c	ASCII	12	2	VirtualAlloc
0040520e	ASCII	21	0	GetClusterResourceKey
00405224	ASCII	11	0	CLUSAPI.dll
00405232	ASCII	6	0	memset
0040523c	ASCII	6	0	memcpy
00405244	ASCII	10	0	msvcrt.dll
00405252	ASCII	12	0	CreateEventW
00405262	ASCII	18	0	GlobalMemoryStatus
00405276	ASCII	12	0	KERNEL32.dll
00405286	ASCII	11	0	RemovePropA
00405292	ASCII	10	0	USER32.dll
004052a0	ASCII	4	0	RSDS
004052b8	ASCII	31	0	E:\Tools\aolfed\release\osc.pdb
00406060	ASCII	5	0	'O_vQ
004060a1	ASCII	7	0	P@vQF^L

IDA Examination



Load file C:\Users\Adeyemi\Desktop\malware sample 4\demo1_ransomware.bin as

Portable executable for 80386 (PE) [pe.dll]
Binary file

Processor type (double-click to set)

Intel Pentium Pro (P6) with MMX	80686p
Intel Pentium protected with MMX	80586p
Intel Pentium real with MMX	80586r
MetaPC (disassemble all opcodes)	**metapc**

Loading segment 0x0000000000000000

Loading offset 0x0000000000000000

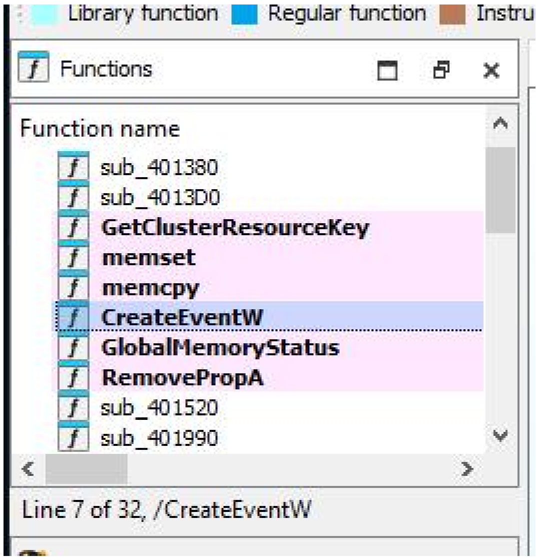
Analysis

☑ Enabled
☑ Indicator enabled

Options

☐ Loading options ☑ Create segments ☐ Load resources
☑ Fill segment gaps ☐ Create FLAT group ☑ Rename DLL entries
☐ Load as code segment ☑ Create imports segment ☐ Manual load

These are the functions in the code as identified by IDA Tool

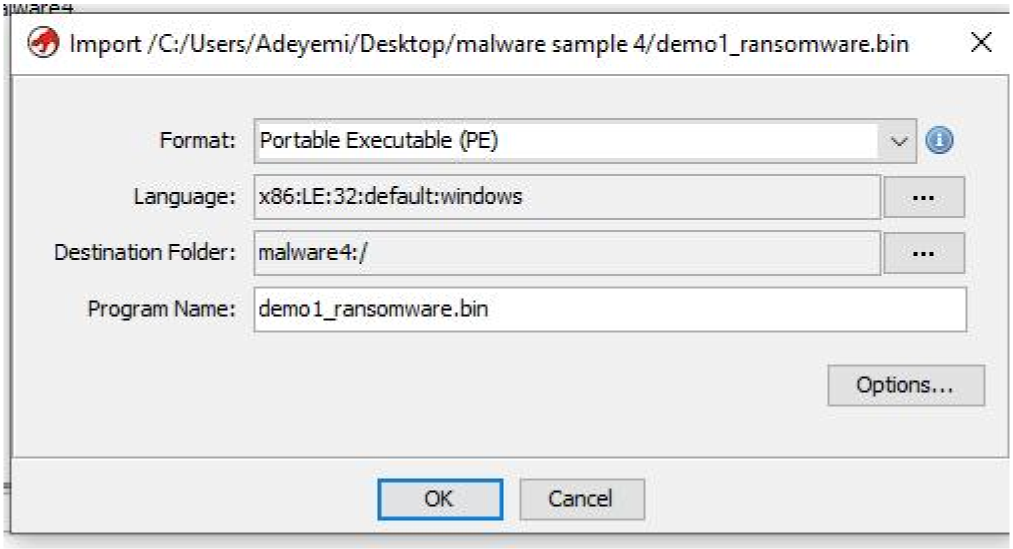


Function name

sub_401380
sub_4013D0
GetClusterResourceKey
memset
memcpy
CreateEventW
GlobalMemoryStatus
RemovePropA
sub_401520
sub_401990

Line 7 of 32, /CreateEventW

GHIDRA LOADING



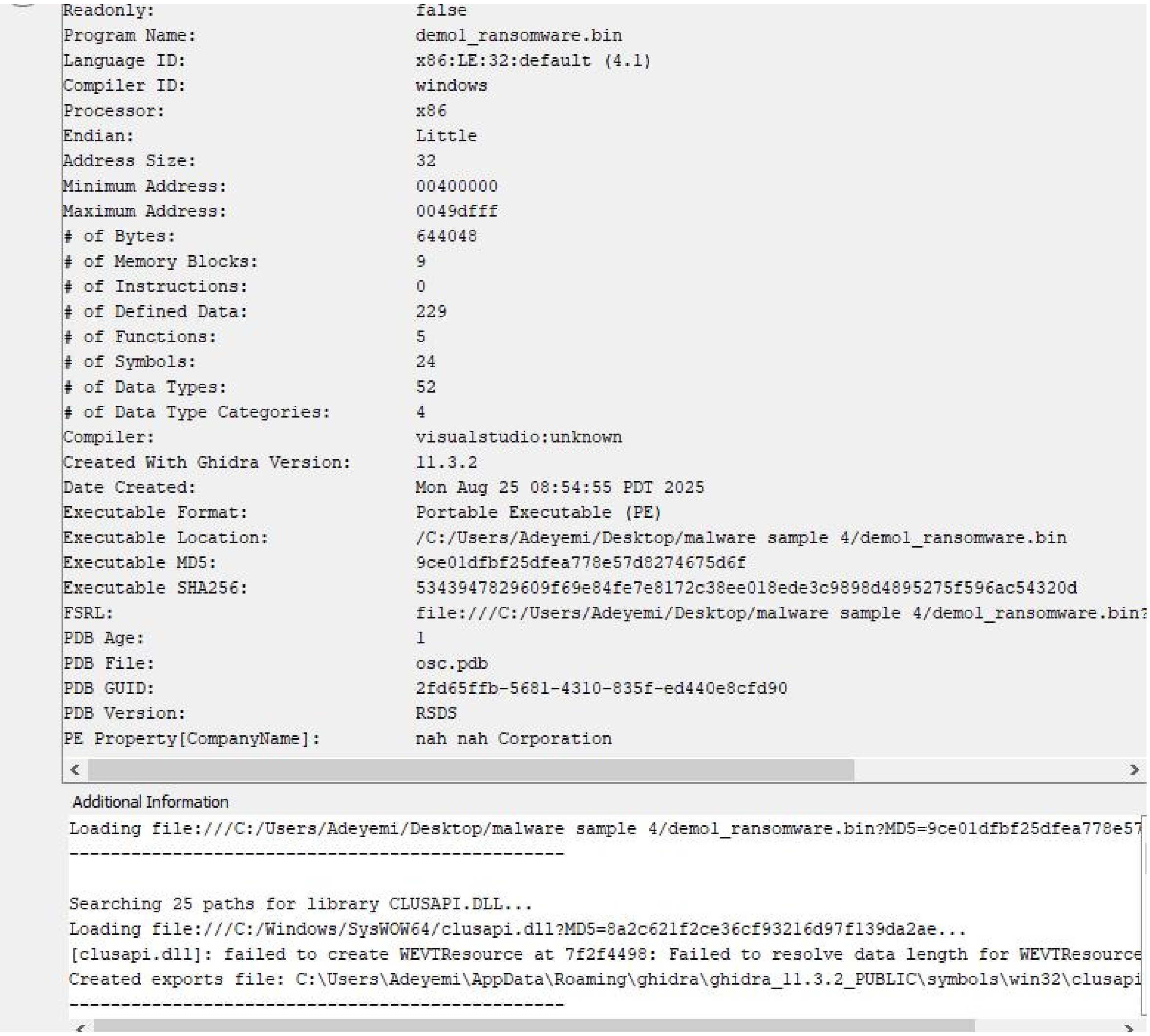
Import /C:/Users/Adeyemi/Desktop/malware sample 4/demo1_ransomware.bin

Format: Portable Executable (PE)

Language: x86:LE:32:default:windows

Destination Folder: malware4:/

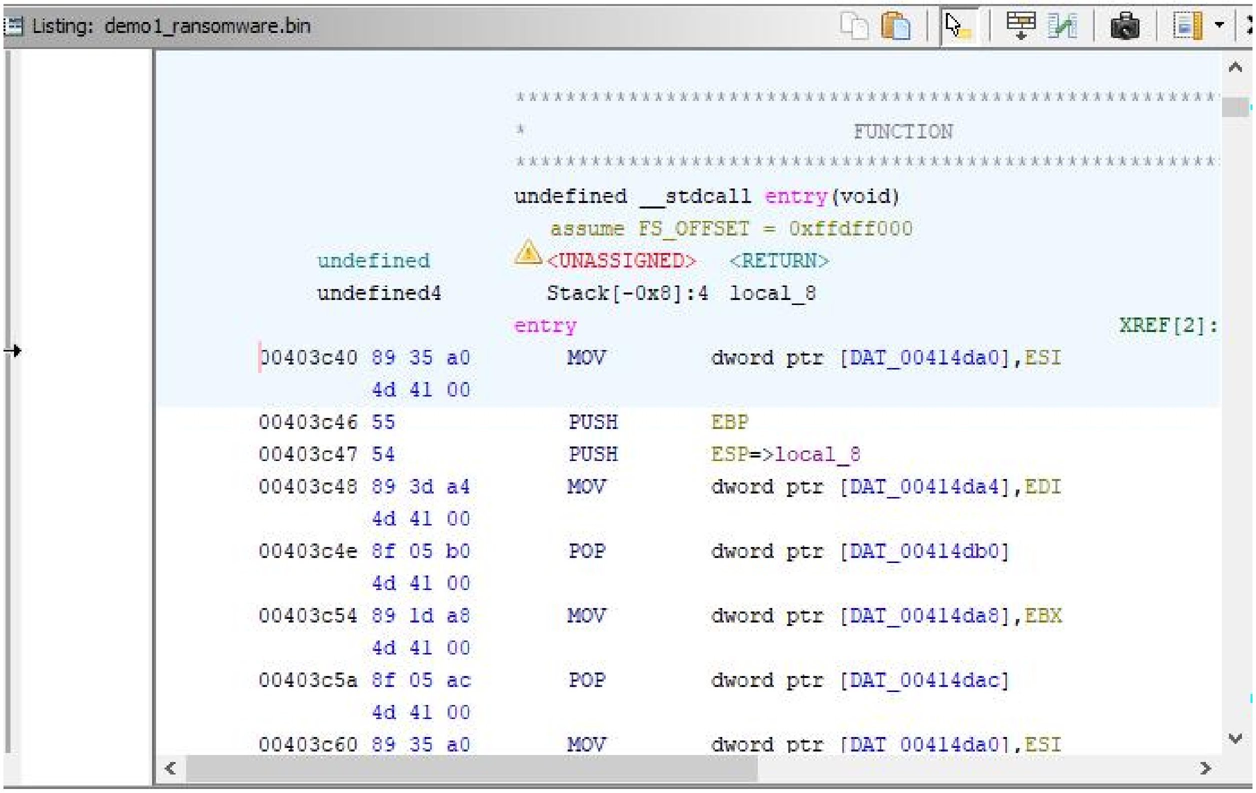
Program Name: demo1_ransomware.bin



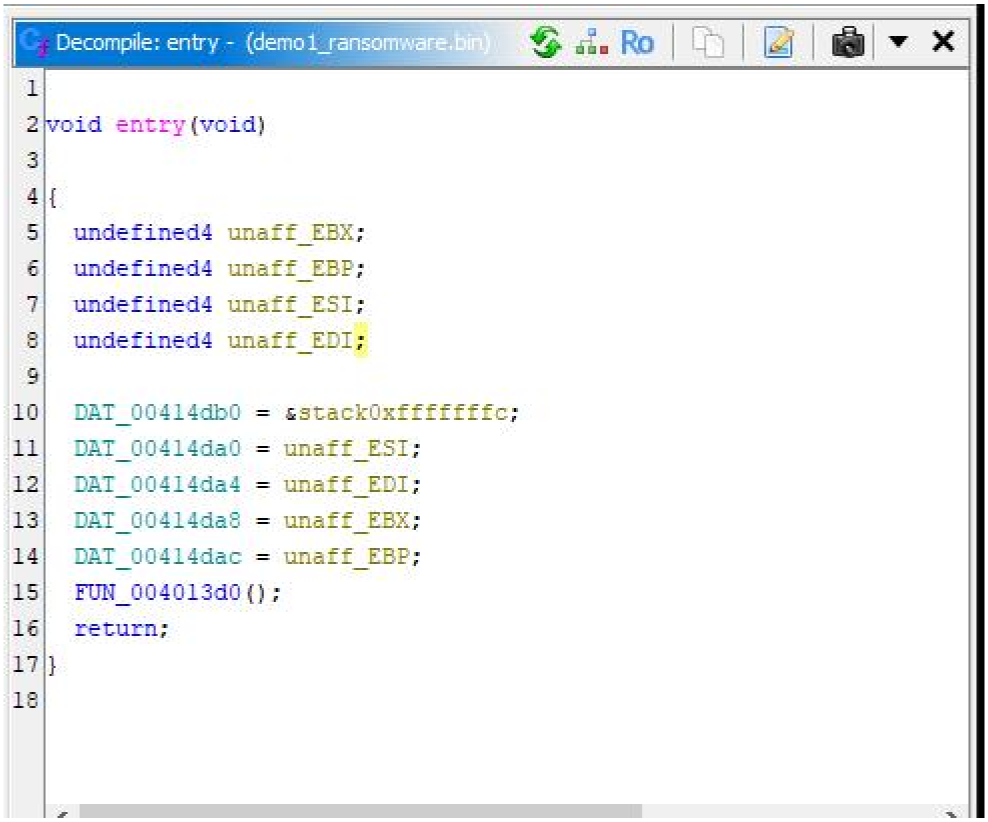
```
Readonly:                         false
Program Name:                     demol_ransomware.bin
Language ID:                      x86:LE:32:default (4.1)
Compiler ID:                      windows
Processor:                        x86
Endian:                           Little
Address Size:                     32
Minimum Address:                  00400000
Maximum Address:                  0049dfff
# of Bytes:                       644048
# of Memory Blocks:               9
# of Instructions:                0
# of Defined Data:                229
# of Functions:                   5
# of Symbols:                     24
# of Data Types:                  52
# of Data Type Categories:        4
Compiler:                         visualstudio:unknown
Created With Ghidra Version:      11.3.2
Date Created:                     Mon Aug 25 08:54:55 PDT 2025
Executable Format:                Portable Executable (PE)
Executable Location:              /C:/Users/Adeyemi/Desktop/malware sample 4/demol_ransomware.bin
Executable MD5:                   9ce01dfbf25dfea778e57d8274675d6f
Executable SHA256:                5343947829609f69e84fe7e8172c38ee018ede3c9898d4895275f596ac54320d
FSRL:                             file:///C:/Users/Adeyemi/Desktop/malware sample 4/demol_ransomware.bin?
PDB Age:                          1
PDB File:                         osc.pdb
PDB GUID:                         2fd65ffb-5681-4310-835f-ed440e8cfd90
PDB Version:                      RSDS
PE Property[CompanyName]:         nah nah Corporation
```

Additional Information

```
Loading file:///C:/Users/Adeyemi/Desktop/malware sample 4/demol_ransomware.bin?MD5=9ce01dfbf25dfea778e57
-----------------------------------------------

Searching 25 paths for library CLUSAPI.DLL...
Loading file:///C:/Windows/SysWOW64/clusapi.dll?MD5=8a2c621f2ce36cf93216d97f139da2ae...
[clusapi.dll]: failed to create WEVTResource at 7f2f4498: Failed to resolve data length for WEVTResource
Created exports file: C:\Users\Adeyemi\AppData\Roaming\ghidra\ghidra_11.3.2_PUBLIC\symbols\win32\clusapi
-----------------------------------------------
```

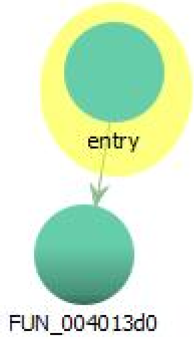


```
                              ************************************************************
                              *                          FUNCTION
                              ************************************************************
                              undefined __stdcall entry(void)
                                assume FS_OFFSET = 0xffdff000
          undefined             <UNASSIGNED>   <RETURN>
          undefined4              Stack[-0x8]:4  local_8
                              entry                                             XREF[2]:
     00403c40 89 35 a0        MOV        dword ptr [DAT_00414da0],ESI
              4d 41 00
     00403c46 55              PUSH       EBP
     00403c47 54              PUSH       ESP=>local_8
     00403c48 89 3d a4        MOV        dword ptr [DAT_00414da4],EDI
              4d 41 00
     00403c4e 8f 05 b0        POP        dword ptr [DAT_00414db0]
              4d 41 00
     00403c54 89 1d a8        MOV        dword ptr [DAT_00414da8],EBX
              4d 41 00
     00403c5a 8f 05 ac        POP        dword ptr [DAT_00414dac]
              4d 41 00
     00403c60 89 35 a0        MOV        dword ptr [DAT_00414da0],ESI
```

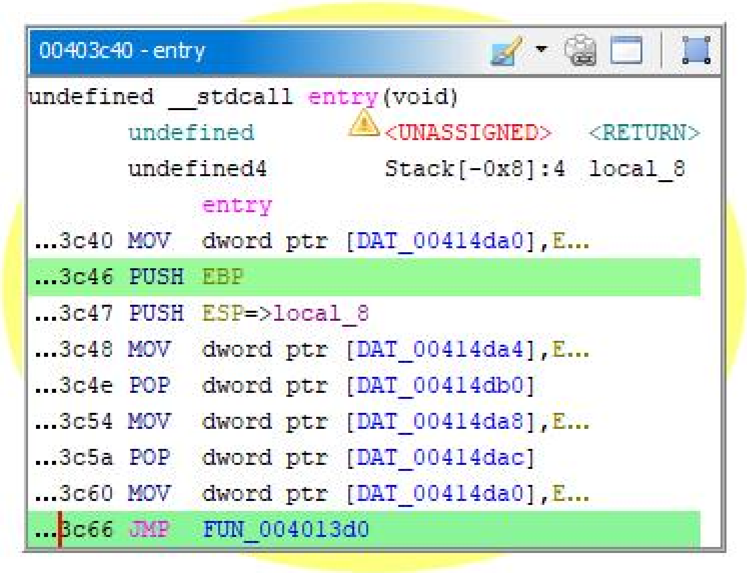


```

void entry(void)

{
  undefined4 unaff_EBX;
  undefined4 unaff_EBP;
  undefined4 unaff_ESI;
  undefined4 unaff_EDI;

  DAT_00414db0 = &stack0xfffffffc;
  DAT_00414da0 = unaff_ESI;
  DAT_00414da4 = unaff_EDI;
  DAT_00414da8 = unaff_EBX;
  DAT_00414dac = unaff_EBP;
  FUN_004013d0();
  return;
}

```

Function call graph

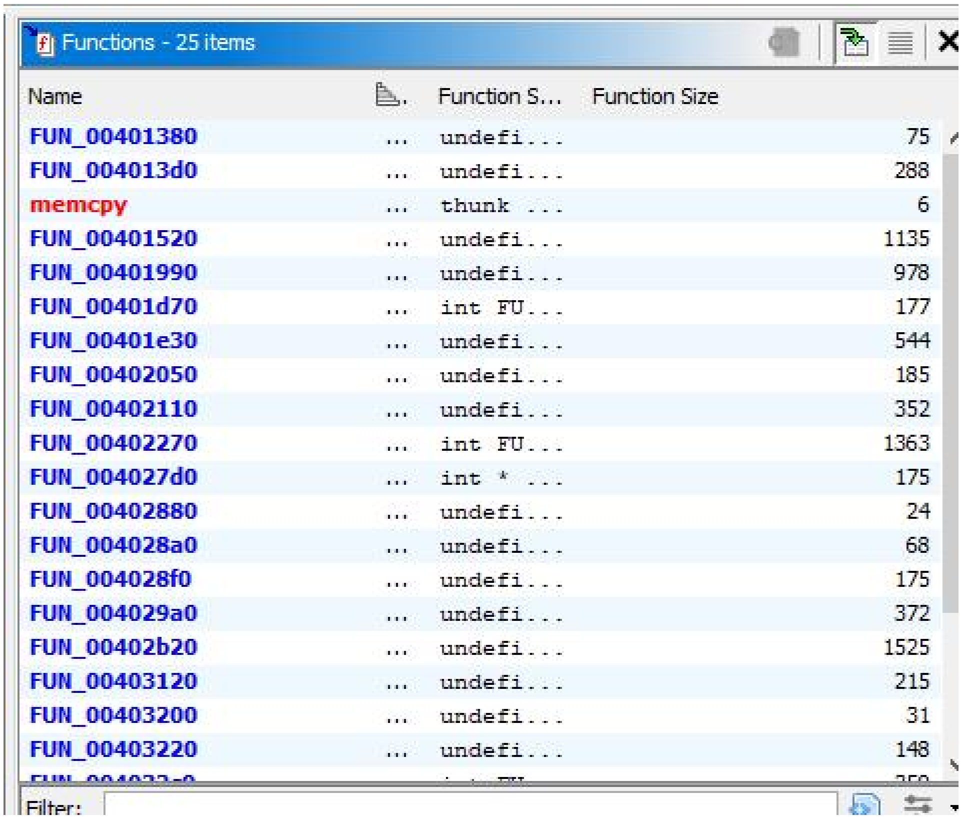


Function graph



```
undefined __stdcall entry(void)
        undefined          <UNASSIGNED>   <RETURN>
        undefined4         Stack[-0x8]:4  local_8
              entry
...3c40 MOV   dword ptr [DAT_00414da0],E...
...3c46 PUSH  EBP
...3c47 PUSH  ESP=>local_8
...3c48 MOV   dword ptr [DAT_00414da4],E...
...3c4e POP   dword ptr [DAT_00414db0]
...3c54 MOV   dword ptr [DAT_00414da8],E...
...3c5a POP   dword ptr [DAT_00414dac]
...3c60 MOV   dword ptr [DAT_00414da0],E...
...3c66 JMP   FUN_004013d0
```

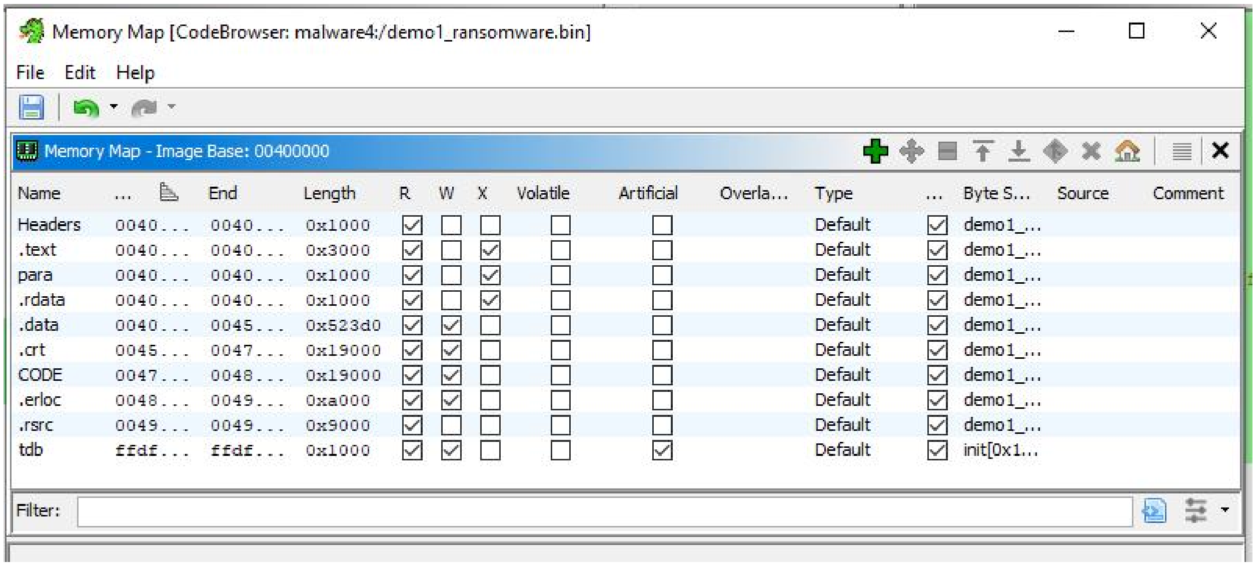
For proper analysis it is important that malware analyst look into all 25 functions that makesup the code for this malware



Functions - 25 items

Name		Function S...	Function Size
FUN_00401380	...	undefi...	75
FUN_004013d0	...	undefi...	288
memcpy	...	thunk ...	6
FUN_00401520	...	undefi...	1135
FUN_00401990	...	undefi...	978
FUN_00401d70	...	int FU...	177
FUN_00401e30	...	undefi...	544
FUN_00402050	...	undefi...	185
FUN_00402110	...	undefi...	352
FUN_00402270	...	int FU...	1363
FUN_004027d0	...	int * ...	175
FUN_00402880	...	undefi...	24
FUN_004028a0	...	undefi...	68
FUN_004028f0	...	undefi...	175
FUN_004029a0	...	undefi...	372
FUN_00402b20	...	undefi...	1525
FUN_00403120	...	undefi...	215
FUN_00403200	...	undefi...	31
FUN_00403220	...	undefi...	148

Memory map from Ghidra

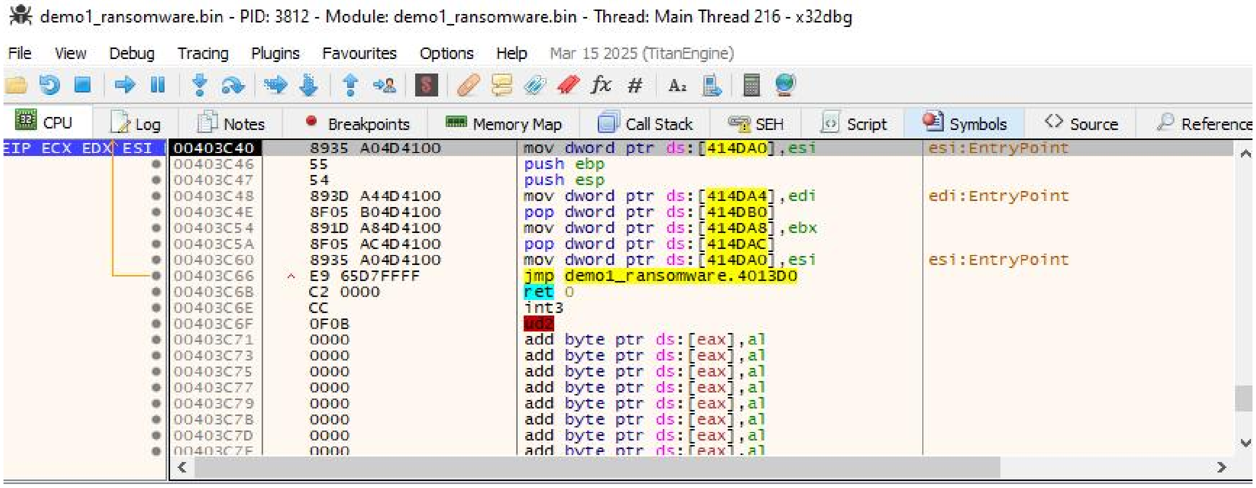


Memory Map [CodeBrowser: malware4:/demo1_ransomware.bin]

Memory Map - Image Base: 00400000

Name	...	End	Length	R	W	X	Volatile	Artificial	Overla...	Type	...	Byte S...	Source	Comment
Headers	0040...	0040...	0x1000	☑	□	□	□	□		Default	☑	demo1_...		
.text	0040...	0040...	0x3000	☑	□	☑	□	□		Default	☑	demo1_...		
para	0040...	0040...	0x1000	☑	□	☑	□	□		Default	☑	demo1_...		
.rdata	0040...	0040...	0x1000	☑	□	☑	□	□		Default	☑	demo1_...		
.data	0040...	0045...	0x523d0	☑	☑	□	□	□		Default	☑	demo1_...		
.crt	0045...	0047...	0x19000	☑	☑	□	□	□		Default	☑	demo1_...		
CODE	0047...	0048...	0x19000	☑	☑	□	□	□		Default	☑	demo1_...		
.erloc	0048...	0049...	0xa000	☑	☑	□	□	□		Default	☑	demo1_...		
.rsrc	0049...	0049...	0x9000	☑	□	□	□	□		Default	☑	demo1_...		
tdb	ffdf...	ffdf...	0x1000	☑	☑	□	□	☑		Default	☑	init[0x1...		

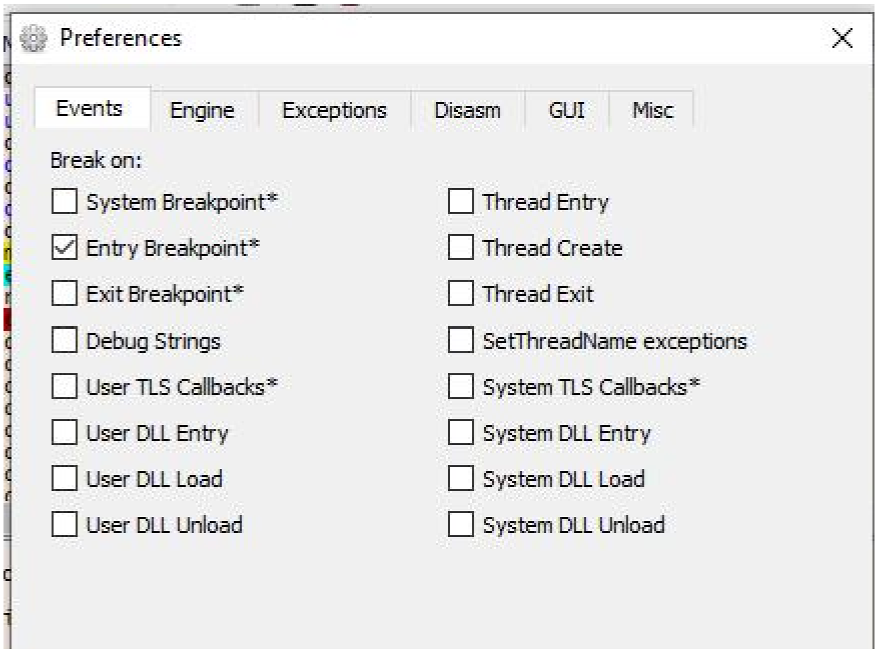
The sample is 32bits executable as identified by PE Studio and other software used for sample identification



demo1_ransomware.bin - PID: 3812 - Module: demo1_ransomware.bin - Thread: Main Thread 216 - x32dbg

File View Debug Tracing Plugins Favourites Options Help Mar 15 2025 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source Reference
EIP ECX EDX ESI

```
00403C40   8935 A04D4100   mov dword ptr ds:[414DA0],esi      esi:EntryPoint
00403C46   55              push ebp
00403C47   54              push esp
00403C48   893D A44D4100   mov dword ptr ds:[414DA4],edi      edi:EntryPoint
00403C4E   8F05 B04D4100   pop dword ptr ds:[414DB0]
00403C54   891D A84D4100   mov dword ptr ds:[414DA8],ebx
00403C5A   8F05 AC4D4100   pop dword ptr ds:[414DAC]
00403C60   8935 A04D4100   mov dword ptr ds:[414DA0],esi      esi:EntryPoint
00403C66 ^ E9 65D7FFFF     jmp demo1_ransomware.4013D0
00403C6B   C2 0000         ret 0
00403C6E   CC              int3
00403C6F   0F0B            ud2
00403C71   0000            add byte ptr ds:[eax],al
00403C73   0000            add byte ptr ds:[eax],al
00403C75   0000            add byte ptr ds:[eax],al
00403C77   0000            add byte ptr ds:[eax],al
00403C79   0000            add byte ptr ds:[eax],al
00403C7B   0000            add byte ptr ds:[eax],al
00403C7D   0000            add byte ptr ds:[eax],al
00403C7F   0000            add byte ptr ds:[eax],al
```

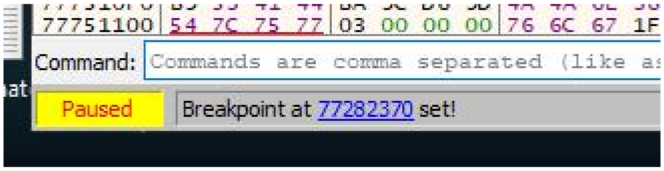


Preferences

Break on:

☐ System Breakpoint*
☑ Entry Breakpoint*
☐ Exit Breakpoint*
☐ Debug Strings
☐ User TLS Callbacks*
☐ User DLL Entry
☐ User DLL Load
☐ User DLL Unload
☐ Thread Entry
☐ Thread Create
☐ Thread Exit
☐ SetThreadName exceptions
☐ System TLS Callbacks*
☐ System DLL Entry
☐ System DLL Load
☐ System DLL Unload

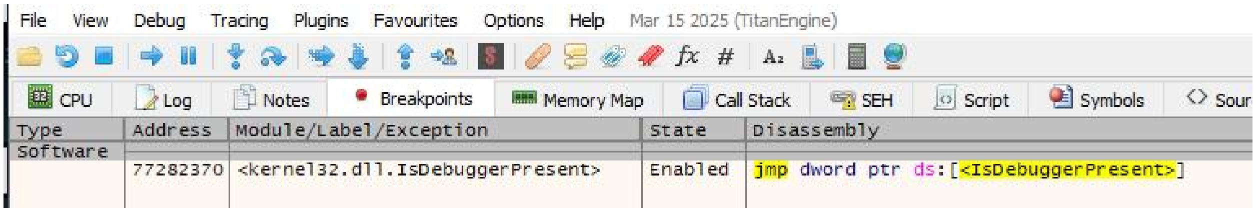
Bp set



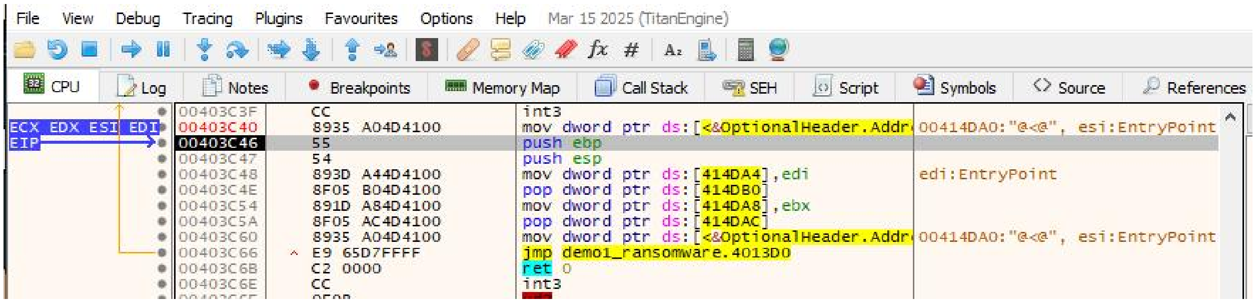
```
77751100 | 54 7C 75 77 | 03 00 00 00 | 76 6C 67 1F
```

Command: Commands are comma separated (like as

Paused   Breakpoint at 77282370 set!



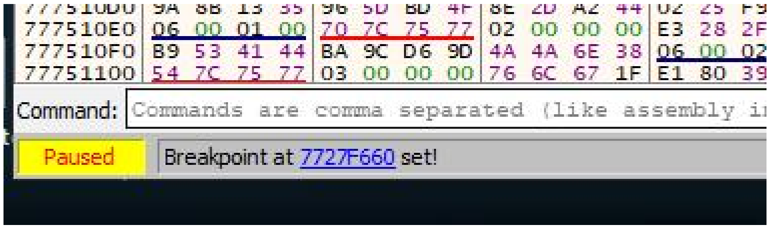
Type	Address	Module/Label/Exception	State	Disassembly
Software				
	77282370	<kernel32.dll.IsDebuggerPresent>	Enabled	jmp dword ptr ds:[<IsDebuggerPresent>]



```
00403C3F    CC              int3
00403C40    8935 A04D4100   mov dword ptr ds:[<&OptionalHeader.Addr   00414DA0:"@<@", esi:EntryPoint
00403C46    55              push ebp
00403C47    54              push esp
00403C48    893D A44D4100   mov dword ptr ds:[414DA4],edi             edi:EntryPoint
00403C4E    8F05 B04D4100   pop dword ptr ds:[414DB0]
00403C54    891D A84D4100   mov dword ptr ds:[414DA8],ebx
00403C5A    8F05 AC4D4100   pop dword ptr ds:[414DAC]
00403C60    8935 A04D4100   mov dword ptr ds:[<&OptionalHeader.Addr   00414DA0:"@<@", esi:EntryPoint
00403C66  ^ E9 65D7FFFF     jmp demo1_ransomware.4013D0
00403C6B    C2 0000         ret 0
00403C6E    CC              int3
```

Bp isdebuggerpresent failed to run

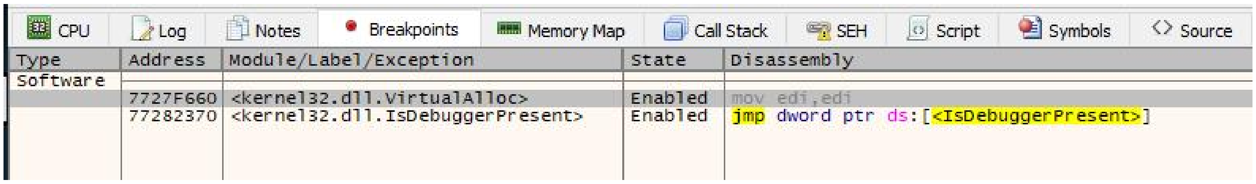
This is bp virtualalloc which i was able to run and step over



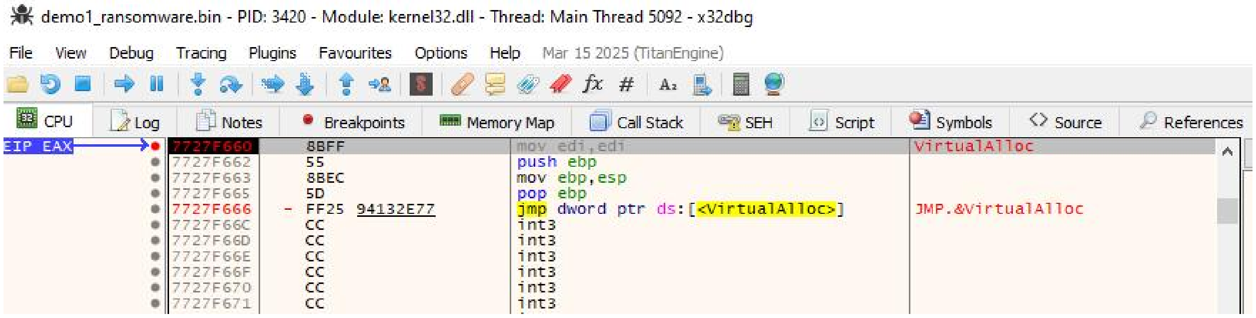
```
777510D0 9A 8B 13 35 96 5D BD 4F 8E 2D A2 44 02 25 F9
777510E0 06 00 01 00 70 7C 75 77 02 00 00 00 E3 28 2F
777510F0 B9 53 41 44 BA 9C D6 9D 4A 4A 6E 38 06 00 02
77751100 54 7C 75 77 03 00 00 00 76 6C 67 1F E1 80 39
```

Command: Commands are comma separated (like assembly i

Paused Breakpoint at 7727F660 set!



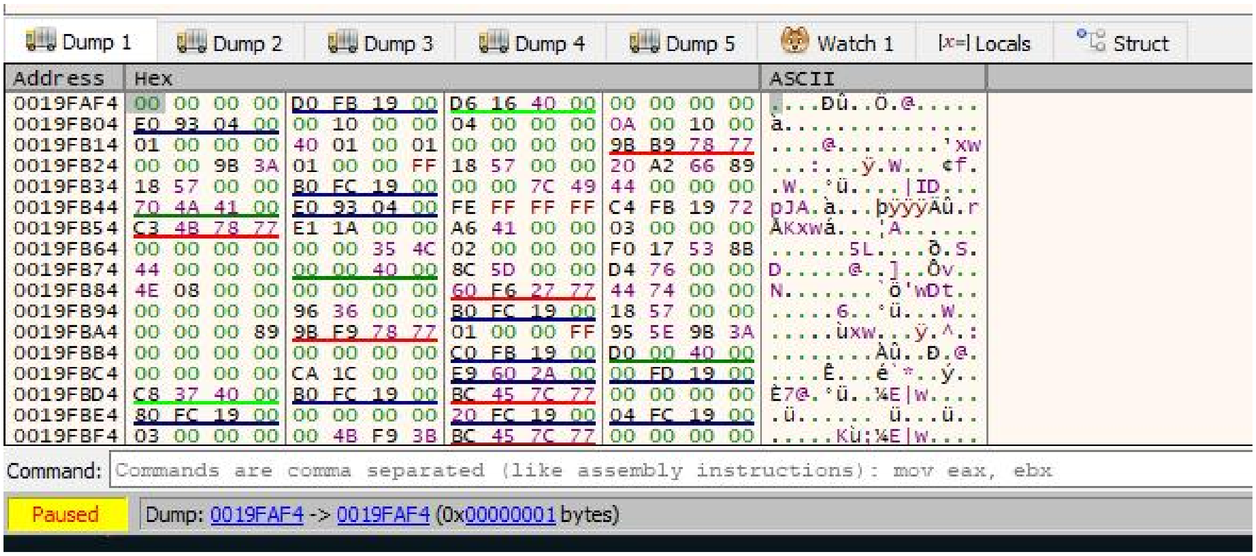
Type	Address	Module/Label/Exception	State	Disassembly
Software				
	7727F660	<kernel32.dll.VirtualAlloc>	Enabled	mov edi,edi
	77282370	<kernel32.dll.IsDebuggerPresent>	Enabled	jmp dword ptr ds:[<IsDebuggerPresent>]



demo1_ransomware.bin - PID: 3420 - Module: kernel32.dll - Thread: Main Thread 5092 - x32dbg

```
7727F660    8BFF            mov edi,edi                        VirtualAlloc
7727F662    55              push ebp
7727F663    8BEC            mov ebp,esp
7727F665    5D              pop ebp
7727F666  - FF25 94132E77   jmp dword ptr ds:[<VirtualAlloc>]  JMP.&VirtualAlloc
7727F66C    CC              int3
7727F66D    CC              int3
7727F66E    CC              int3
7727F66F    CC              int3
7727F670    CC              int3
7727F671    CC              int3
```

After follow in dump

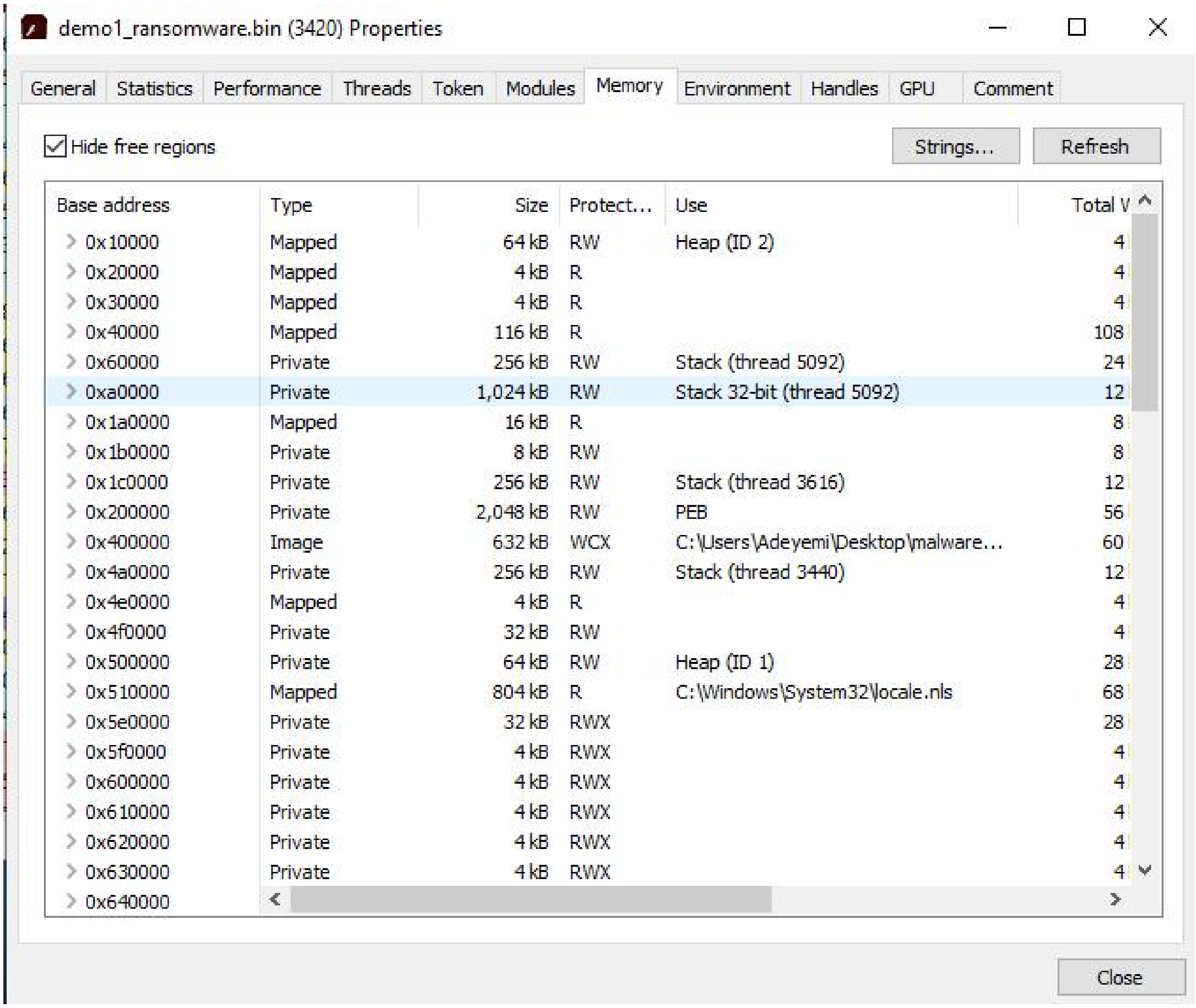


```
Address   Hex                                                ASCII
0019FAF4  00 00 00 00 D0 FB 19 00 D6 16 40 00 00 00 00 00  ....Ðû..Ö.@.....
0019FB04  E0 93 04 00 00 10 00 00 04 00 00 00 0A 00 10 00  à...............
0019FB14  01 00 00 00 40 01 00 01 00 00 00 00 9B B9 78 77  ....@........'xw
0019FB24  00 00 9B 3A 01 00 00 FF 18 57 00 00 20 A2 66 89  ...:...ÿ.W.. ¢f.
0019FB34  18 57 00 00 B0 FC 19 00 00 00 7C 49 44 00 00 00  .W..°ü....|ID...
0019FB44  70 4A 41 00 E0 93 04 00 FE FF FF FF C4 FB 19 72  pJA.à...þÿÿÿÄû.r
0019FB54  C3 4B 78 77 E1 1A 00 00 A6 41 00 00 03 00 00 00  ÃKxwá...¦A......
0019FB64  00 00 00 00 00 00 35 4C 02 00 00 00 F0 17 53 8B  ......5L....ð.S.
0019FB74  44 00 00 00 00 00 40 00 8C 5D 00 00 D4 76 00 00  D.....@..]..Ôv..
0019FB84  4E 08 00 00 00 00 00 00 60 F6 27 77 44 74 00 00  N.......`ö'wDt..
0019FB94  00 00 00 00 96 36 00 00 B0 FC 19 00 18 57 00 00  .....6..°ü...W..
0019FBA4  00 00 00 89 9B F9 78 77 01 00 00 FF 95 5E 9B 3A  .....ùxw...ÿ.^.:
0019FBB4  00 00 00 00 00 00 00 00 C0 FB 19 00 D0 00 40 00  ........Àû..Ð.@.
0019FBC4  00 00 00 00 CA 1C 00 00 E9 60 2A 00 00 FD 19 00  ....Ê...é`*..ý..
0019FBD4  C8 37 40 00 B0 FC 19 00 BC 45 7C 77 00 00 00 00  È7@.°ü..¼E|w....
0019FBE4  80 FC 19 00 00 00 00 00 20 FC 19 00 04 FC 19 00  .ü...... ü...ü..
0019FBF4  03 00 00 00 00 4B F9 3B BC 45 7C 77 00 00 00 00  .....Kù;¼E|w....
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused   Dump: 0019FAF4 -> 0019FAF4 (0x00000001 bytes)

Process hacker



☑ Hide free regions

Base address	Type	Size	Protect...	Use	Total V
0x10000	Mapped	64 kB	RW	Heap (ID 2)	4
0x20000	Mapped	4 kB	R		4
0x30000	Mapped	4 kB	R		4
0x40000	Mapped	116 kB	R		108
0x60000	Private	256 kB	RW	Stack (thread 5092)	24
0xa0000	Private	1,024 kB	RW	Stack 32-bit (thread 5092)	12
0x1a0000	Mapped	16 kB	R		8
0x1b0000	Private	8 kB	RW		8
0x1c0000	Private	256 kB	RW	Stack (thread 3616)	12
0x200000	Private	2,048 kB	RW	PEB	56
0x400000	Image	632 kB	WCX	C:\Users\Adeyemi\Desktop\malware...	60
0x4a0000	Private	256 kB	RW	Stack (thread 3440)	12
0x4e0000	Mapped	4 kB	R		4
0x4f0000	Private	32 kB	RW		4
0x500000	Private	64 kB	RW	Heap (ID 1)	28
0x510000	Mapped	804 kB	R	C:\Windows\System32\locale.nls	68
0x5e0000	Private	32 kB	RWX		28
0x5f0000	Private	4 kB	RWX		4
0x600000	Private	4 kB	RWX		4
0x610000	Private	4 kB	RWX		4
0x620000	Private	4 kB	RWX		4
0x630000	Private	4 kB	RWX		4
0x640000					

From which i dump the memory. It’s indeed an expirience