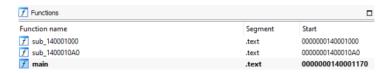
Downloader Challenge

Our organization's Security Operations Center (SOC) has detected suspicious activity related to downloader malware. The malware is designed to retrieve and execute additional payloads from remote servers, potentially leading to further compromise of the network. Please help us answer these questions.

Task 1: What is the address of the function "main"?

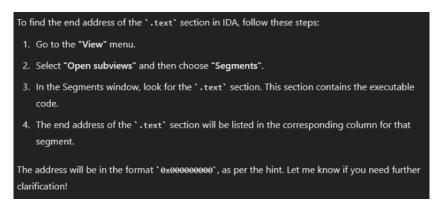
First when we open the file with IDA we can see the main function

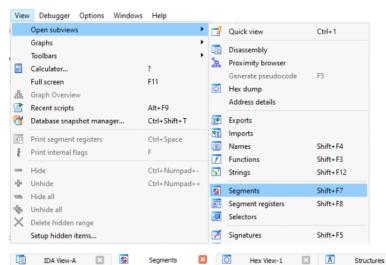


Answer: 0x140001170

Task 2: What is the end address of the .text section?

I asked the ChatGPT about how to see the .text section





Task 3: What is the IP address used to download the payload?

I investigate all the text and found the IP

Answer: 45.249.93.80

Task 4

What is the name of the payload downloaded?

Same place like task 3

```
.rdata:0000000140008E38 ; const WCHAR pszAgentW
.rdata:0000000140008E38 pszAgentW:
                                                           ; DATA XREF: main+1F↑o
                                    text "UTF-16LE", 'WinHTTP Example/1.0',0
.rdata:0000000140008F38
.rdata:0000000140008E60 ; const WCHAR pwszVerb
rdata:0000000140008E60 pwszVerb:
                                    text "UTF-16LE", 'GET',0
; DATA XREF: main+39fo
                                                           ; DATA XREF: sub_140001000+35↑o
.rdata:0000000140008E60
rdata:0000000140008E68 aPayloadBin:
.rdata:0000000140008E68
                                    text "UTF-16LE", '/payload.bin',0
.rdata:0000000140008E82
                                                    ; DATA XREF: main+18↑o
.rdata:0000000140008E88 a452499380:
                                    text "UTF-16LE", '45.249.93.80',0
.rdata:0000000140008E88
```

Answer: payload.bin

Task 5:

What is the name of the user agent used by the downloader?

Same like task 3

```
.rdata:0000000140008E38 ; const WCHAR pszAgentW
.rdata:0000000140008E38 pszAgentW:
.rdata:0000000140008E38
                                                                : DATA XREF: main+1F1o
                                       text "UTF-16LE", 'WinHTTP Example/1.0',0
rdata:0000000140008E60 ; const WCHAR pwszVerb
.rdata:0000000140008E60 pwszVerb:
                                      ; DATA XREF: sub_140001000+3510
text "UTF-16LE", 'GET',0
; DATA XREF: main+3910
.rdata:0000000140008E60
.rdata:0000000140008E68 aPayloadBin:
.rdata:0000000140008E68
                                       text "UTF-16LE", '/payload.bin',0
.rdata:0000000140008E82
                                      align 8
                                                                ; DATA XREF: main+18†o
.rdata:0000000140008E88 a452499380:
                                       text "UTF-16LE", '45.249.93.80',0
.rdata:0000000140008E88
```

Answer: WinHTTP Example/1.0

Task 6:

What is the name of the DLL loaded by the downloader?

While scrolling a little bit more after finding the answers for task 3-5 and found the DLL

```
; DATA XREF: main+116↑o
                                                       ; DATA XREF: .rdata:00000001400072D4†o
; CV signature
.rdata:0000000140008EF4
                                                                              ; GUID
.rdata:0000000140008EF8
                                           dd 656B49B0h
.rdata:0000000140008EF8
                                           dw 2BECh
                                                      ; Data2
                                          dw 2BELn ; Data2
dw 4AClh ; Data3
db 08Bh, 0D9h, 0F3h, 95h, 33h, 0D1h, 1, 0B3h; Data4
dd 1 ; Age : "UTF-8", 'd:\Documents\Visual Studio 2008\Projects\Project1\新wIN'; PdbFileName
text "UTF-8", '64\x64\Release\新wIN64.pdb', 0
.rdata:0000000140008EF8
.rdata:0000000140008EF8
.rdata:0000000140008F08
.rdata:0000000140008F0C
.rdata:0000000140008F0C
.rdata:0000000140008F60 unk 140008F60 db
                                                                     ; DATA XREF: .rdata:00000001400072F01o
```

Answer: dbghelp.dll

Task 7:

What is the first API used during the function that retrieves data from the HTTP response?

Above the main functions there is two more functions. One of them is $sub_1400010A0$ which contains an API



sub_1400010A0 proc near

```
dwNumberOfBytesAvailable= dword ptr 8
dwNumberOfBytesRead= dword ptr 10h
arg_10= qword ptr 18h
arg_18= qword ptr 20h

mov [rsp+arg_18], rbx
push rbp
push rsi
push r12
sub rsp, 20h
mov rbp, rcx
mov rcx, [rcx+8] ; hRequest
xor r12d, r12d
xor edx, edx ; lpReserved
mov rbx, r12
mov esi, r12d
call cs:WinHttpReceiveResponse
test eax, eax
jz loc_140001151
```

Answer: WinHttpReceiveResponse

Task 8: What is the name of the function that establishes the HTTP request?

Same like task 7

f main	.text	0000000140001170
f sub_1400010A0	.text	00000001400010A0
f sub_140001000	.text	0000000140001000
Function name	Segment	Start

Answer: sub_140001000