

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

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

Answer: 0x140001170

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

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

To find the end address of the `.text` section in IDA, follow these steps:

1. Go to the "View" menu.

2. Select "Open subviews" and then choose "Segments".

3. In the Segments window, look for the `.text` section. This section contains the executable code.

4. The end address of the `.text` section will be listed in the corresponding column for that segment.

The address will be in the format `0x00000000`, as per the hint. Let me know if you need further clarification!

View Debugger Options Windows Help

Open subviews

Graphs

Toolbars

Calculator...

Full screen

Graph Overview

Recent scripts

Database snapshot manager...

Print segment registers

Print internal flags

Hide

Unhide

Hide all

Unhide all

Delete hidden range

Setup hidden items...

Quick view

Disassembly

Proximity browser

Generate pseudocode

Hex dump

Address details

Exports

Imports

Names

Functions

Strings

Segments

Segment registers

Selectors

Signatures

Ctrl+1

F5

Shift+F4

Shift+F3

Shift+F12

Shift+F7

Shift+F8

Shift+F5

IDA View-A

Segments

Hex View-1

Structures

Enums

Imports

Exports

Name	Start	End	R	W	X	D	L	Align	Base	Type	Class	AD	es	ss	ds	fs	gs
.text	0000000140001000	0000000140007000	R	.	X	.	L	para	0001	public	CODE	64	0000	0000	0003	FFFFFF...	FFFFFFFFFFFFFFFF
.idata	0000000140007000	0000000140007268	R	.	.	.	L	para	0005	public	DATA	64	0000	0000	0003	FFFFFF...	FFFFFFFFFFFFFFFF
.rdata	0000000140007268	000000014000A000	R	.	.	.	L	para	0002	public	DATA	64	0000	0000	0003	FFFFFF...	FFFFFFFFFFFFFFFF
.data	000000014000A000	000000014000D000	R	W	.	.	L	para	0003	public	DATA	64	0000	0000	0003	FFFFFF...	FFFFFFFFFFFFFFFF
.pdata	000000014000D000	000000014000E000	R	.	.	.	L	para	0004	public	DATA	64	0000	0000	0003	FFFFFF...	FFFFFFFFFFFFFFFF

Answer: 0x140007000

Task 3:

What is the IP address used to download the payload?

I investigate all the text and found the IP

```
.rdata:00000000140008E38 ; const WCHAR pszAgentW
.rdata:00000000140008E38 pszAgentW: ; DATA XREF: main+1Ffo
.rdata:00000000140008E38 text "UTF-16LE", 'WinHTTP Example/1.0',0
.rdata:00000000140008E60 ; const WCHAR pszVerb
.rdata:00000000140008E60 pszVerb: ; DATA XREF: sub_140001000+35fo
.rdata:00000000140008E60 text "UTF-16LE", 'GET',0
.rdata:00000000140008E68 aPayloadBin: ; DATA XREF: main+39fo
.rdata:00000000140008E68 text "UTF-16LE", '/payload.bin',0
.rdata:00000000140008E82 align 8
.rdata:00000000140008E88 a452499380: ; DATA XREF: main+18fo
.rdata:00000000140008E88 text "UTF-16LE", '45.249.93.80',0
```

Answer: 45.249.93.80

Task 4:

What is the name of the payload downloaded?

Same place like task 3

```
.rdata:00000000140008E38 ; const WCHAR pszAgentW
.rdata:00000000140008E38 pszAgentW: ; DATA XREF: main+1Ffo
.rdata:00000000140008E38 text "UTF-16LE", 'WinHTTP Example/1.0',0
.rdata:00000000140008E60 ; const WCHAR pszVerb
.rdata:00000000140008E60 pszVerb: ; DATA XREF: sub_140001000+35fo
.rdata:00000000140008E60 text "UTF-16LE", 'GET',0
.rdata:00000000140008E68 aPayloadBin: ; DATA XREF: main+39fo
.rdata:00000000140008E68 text "UTF-16LE", '/payload.bin',0
.rdata:00000000140008E82 align 8
.rdata:00000000140008E88 a452499380: ; DATA XREF: main+18fo
.rdata:00000000140008E88 text "UTF-16LE", '45.249.93.80',0
```

Answer: payload.bin

Task 5:

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

Same like task 3

```
.rdata:00000000140008E38 ; const WCHAR pszAgentW
.rdata:00000000140008E38 pszAgentW: ; DATA XREF: main+1Ffo
.rdata:00000000140008E38 text "UTF-16LE", 'WinHTTP Example/1.0',0
.rdata:00000000140008E60 ; const WCHAR pszVerb
.rdata:00000000140008E60 pszVerb: ; DATA XREF: sub_140001000+35fo
.rdata:00000000140008E60 text "UTF-16LE", 'GET',0
.rdata:00000000140008E68 aPayloadBin: ; DATA XREF: main+39fo
.rdata:00000000140008E68 text "UTF-16LE", '/payload.bin',0
.rdata:00000000140008E82 align 8
.rdata:00000000140008E88 a452499380: ; DATA XREF: main+18fo
.rdata:00000000140008E88 text "UTF-16LE", '45.249.93.80',0
```

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

```
.rdata:00000000140008EE8 LibFileName db 'dbghelp.dll',0 ; DATA XREF: main+116fo
.rdata:00000000140008EF4 ; Debug information (IMAGE_DEBUG_TYPE_CODEVIEW)
.rdata:00000000140008EF4 asc_140008EF4 db 'RSDS' ; DATA XREF: .rdata:000000001400072D4fo
.rdata:00000000140008EF4 ; CV signature
.rdata:00000000140008EF8 dd 656B49B0h ; Data1 ; GUID
.rdata:00000000140008EF8 dw 28ECh ; Data2
.rdata:00000000140008EF8 dw 4AC1h ; Data3
.rdata:00000000140008EF8 db 0B8h, 0D9h, 0F3h, 95h, 33h, 0D1h, 1, 0B3h ; Data4
.rdata:00000000140008F08 dd 1 ; Age
.rdata:00000000140008F0C text "UTF-8", 'd:\Documents\Visual Studio 2008\Projects\Project1\新WIN' ; PdbFileName
.rdata:00000000140008F0C text "UTF-8", '64\x64\Release\新WIN64.pdb',0
.rdata:00000000140008F60 unk_140008F60 db 1 ; DATA XREF: .rdata:000000001400072F0fo
```

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

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

```
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:WinHttpRequestReceiveResponse
test    eax, eax
jz      loc_140001151
```

Answer: WinHttpRequestReceiveResponse

Task 8:

What is the name of the function that establishes the HTTP request?

Same like task 7

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

Answer: sub_140001000