Proj 10: Analyzing Malicious Windows Programs (Lab 7-1) (15 pts.)

What you need:

- A Windows XP or Windows 7 machine with IDA PRO
- The textbook: "Practical Malware Analysis"

Purpose

You will practice the techniques in chapter 7.

You should already have the lab files, but if you don't, do this:

Downloading the Lab Files

In a Web browser, go here:

http://practicalmalwareanalysis.com/labs/

Download and unzip the lab files.

Analyzing the Malware

Follow the instructions for **Lab 7-1** in the textbook. There are more detailed solutions in the back of the book.

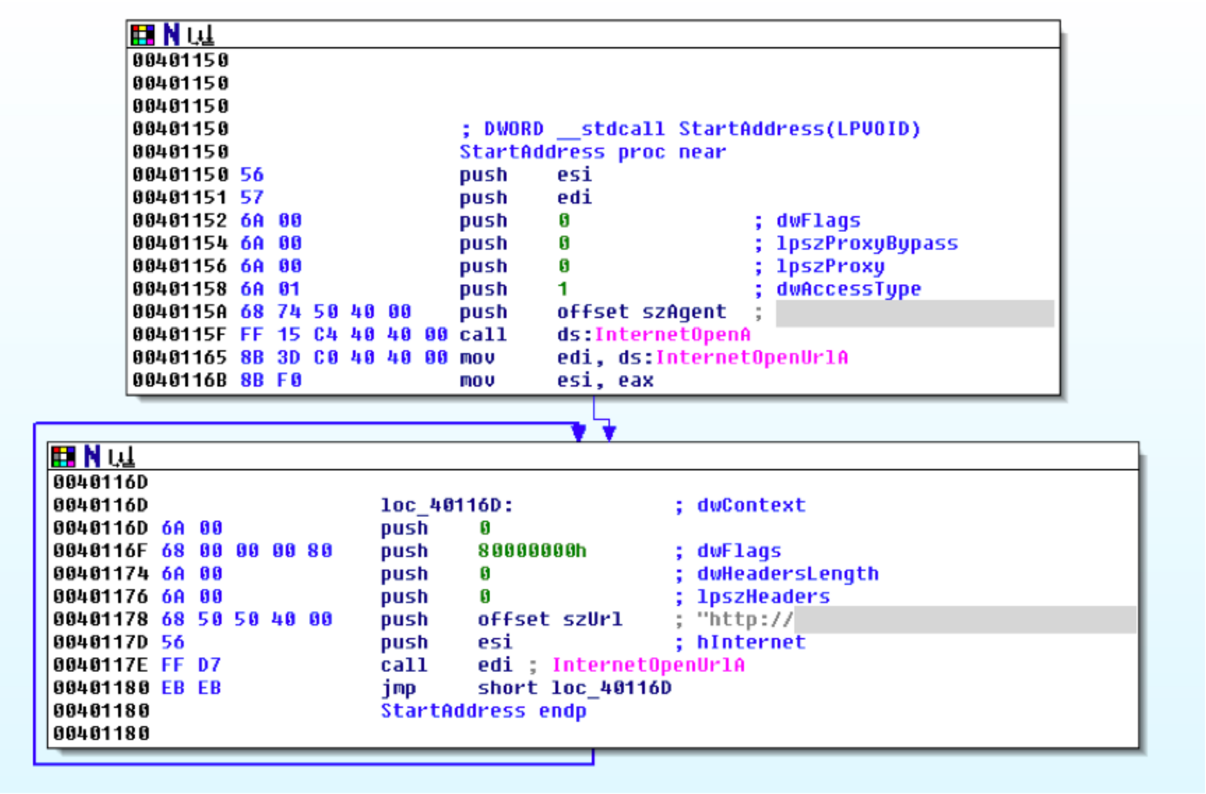
You will see these features:

1. A **persistence mechanism**
2. A **mutex**
3. A **host-based signature**
4. A **network-based signature**

This malware uses a function named StartAddress to perform a DDoS attack.

When answering Q: 4, you find the user agent it uses to perform the attack, and the URL it will attack.

Save a screen capture of the IDA Pro screen showing those two values, as shown below (with the important items grayed out).



```
00401150
00401150
00401150
00401150                         ; DWORD __stdcall StartAddress(LPVOID)
00401150                         StartAddress proc near
00401150 56                      push    esi
00401151 57                      push    edi
00401152 6A 00                   push    0                 ; dwFlags
00401154 6A 00                   push    0                 ; lpszProxyBypass
00401156 6A 00                   push    0                 ; lpszProxy
00401158 6A 01                   push    1                 ; dwAccessType
0040115A 68 74 50 40 00          push    offset szAgent    ; [redacted]
0040115F FF 15 C4 40 40 00 call  ds:InternetOpenA
00401165 8B 3D C0 40 40 00 mov   edi, ds:InternetOpenUrlA
0040116B 8B F0                   mov     esi, eax
```

```
0040116D
0040116D                   loc_40116D:               ; dwContext
0040116D 6A 00             push    0
0040116F 68 00 00 00 80    push    80000000h         ; dwFlags
00401174 6A 00             push    0                 ; dwHeadersLength
00401176 6A 00             push    0                 ; lpszHeaders
00401178 68 50 50 40 00    push    offset szUrl      ; "http://[redacted]
0040117D 56                push    esi               ; hInternet
0040117E FF D7             call    edi ; InternetOpenUrlA
00401180 EB EB             jmp     short loc_40116D
00401180                   StartAddress endp
00401180
```

Save this image with the filename "**Proj 10 from YOUR NAME**".

Turning in your Project

Email the image to cnit.126sam@gmail.com with the subject line: **Proj 10 from YOUR NAME**

Last modified 5-14-16