CSE 434S

Advanced Static Analysis with IDA

Overview

The purpose of this lab is to practice advanced static analysis using IDA. Please download the archive "IDA_malware_samples.7z" from our Canvas site on your Windows VM, extract the 4 sample files from the archive (password: "infected"), and answer the following questions about the samples.

Sample 1:

S1-Q1. What is the major code construct found in the only subroutine called by main?

Checking Internet connection cause I can see the string like 'Success: Internet Connection' or 'Error 1.1: No Internet₩n'.

S1-Q2. What is the subroutine located at 0x40105F?

I think it's trying to print out or write out something because of _stbuf and _ftbuf

----

S1-Q3. What is the purpose of this program?

I think this program is trying to check internet connection.

Sample 2:

S2-Q1. What operation does the first subroutine called by main perform?

Check internet connection!

S2-Q2. What is the subroutine located at 0x40117F?

I think it’s trying to print out or write out something because of _stbuf and _ftbuf

----

S2-Q3. What does the second subroutine called by main do?

It is trying to open the url, ‘http://www.practicalmalwareanalysis.com’. Because the code set the Agent and URL.

S2-Q4. What type of code construct is used in this subroutine?

Maybe it uses a character array filled with data from InternetReadFile.

S2-Q5. Are there any network-based indicators for this program?

HTTP User-Agent: Internet Explorer 7.5/pma
URL: http://www.practicalmalwareanalysis.com/

S2-Q6. What is the purpose of this malware?

I think it is trying to download a web page at
‘http://www.practicalmalwareanalysis.com/’

Sample 3:

S3-Q1. Compare the calls in main to Sample 2’s main method. What is the new function called from main?

Call sub_401130 is the different point.

S3-Q2. What parameters does this new function take?

From the source code, we can see it receives 2 parameters. One is a char and the oter is string pointer.
‘int __cdecl sub_401130(char,LPCSTR lpExistingFileName)’

S3-Q3. What major code construct does this function contain?

I think it is trying to jump somewhere. Because the source contains several the jump addresses. From the source code, I think it will handle its input parameters and it will do what the parameters indicate.

S3-Q4. What can this function do?

It can ‘create directory’ ‘copy a file’ ‘delete a file’ ‘open registry key value’ ‘set registry key value’ ‘sleep’

S3-Q5. Are there any host-based indicators for this malware?

In the address of ‘00401040’, we can see the same indicators like Sample2. Those are HTTP User-Agent: Internet Explorer 7.5/pma, URL: http://www.practicalmalwareanalysis.com/

S3-Q6. What is the purpose of this malware?

It is almost the same with the Sample 2. It tries to download a page(or program) at ‘http://www.practicalmalwareanalysis.com/’. The downloaded program can do 6 things that are ‘create directory’ ‘copy a file’ ‘delete a file’ ‘open registry key value’ ‘set registry key value’ ‘sleep’.

Sample 4:

S4-Q1. What is the difference between the calls made from the main method in Sample 3 and Sample 4?

In Lab 6-3,
sub_401000
sub_401040
sub_401271
sub_401130
Sleep

n Lab 6-4,

sub_401000

sub_401040

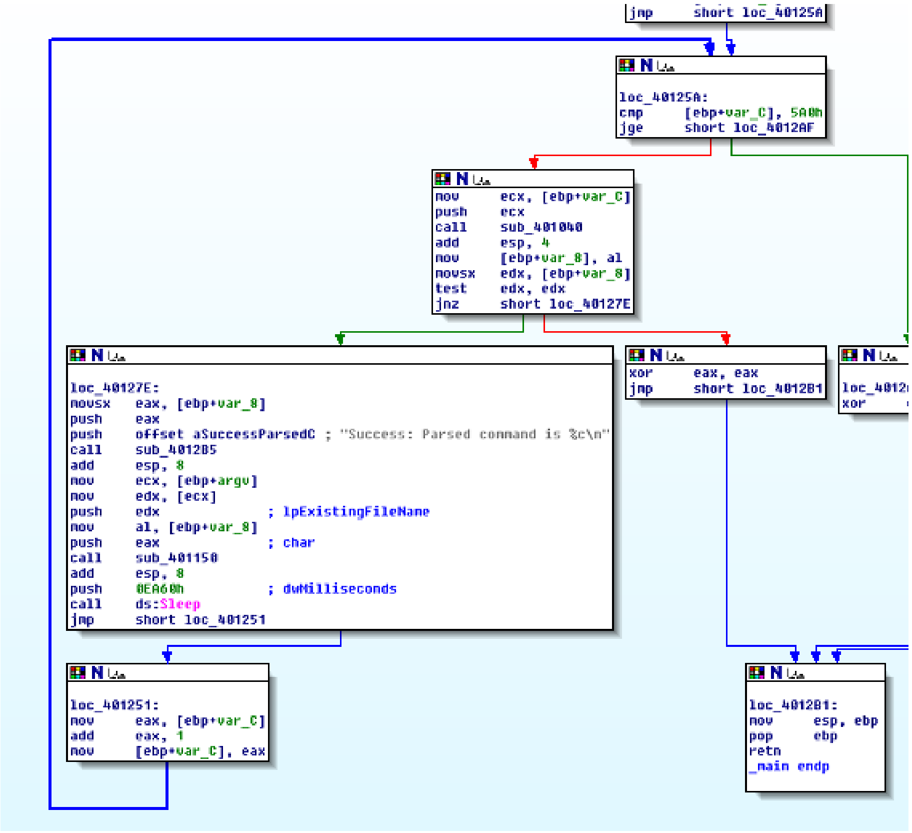
sub_4012B5 (not in Sample3)

sub_401150 (not in Sample3)

Sleep

S4-Q2. What new code construct has been added to main?

I think looping is added in this program. It sleep for a while and try to do again and again.



```
jmp     short loc_40125A
```

```
loc_40125A:
cmp     [ebp+var_C], 5A0h
jge     short loc_4012AF
```

```
mov     ecx, [ebp+var_C]
push    ecx
call    sub_401040
add     esp, 4
mov     [ebp+var_8], al
movsx   edx, [ebp+var_8]
test    edx, edx
jnz     short loc_40127E
```

```
loc_40127E:
movsx   eax, [ebp+var_8]
push    eax
push    offset aSuccessParsedC ; "Success: Parsed command is %c\n"
call    sub_4012B5
add     esp, 8
mov     ecx, [ebp+argv]
mov     edx, [ecx]
push    edx                 ; lpExistingFileName
mov     al, [ebp+var_8]
push    eax                 ; char
call    sub_401150
add     esp, 8
push    0EA60h              ; dwMilliseconds
call    ds:Sleep
jmp     short loc_401251
```

```
xor     eax, eax
jmp     short loc_4012B1
```

```
loc_4012
xor
```

```
loc_401251:
mov     eax, [ebp+var_C]
add     eax, 1
mov     [ebp+var_C], eax
```

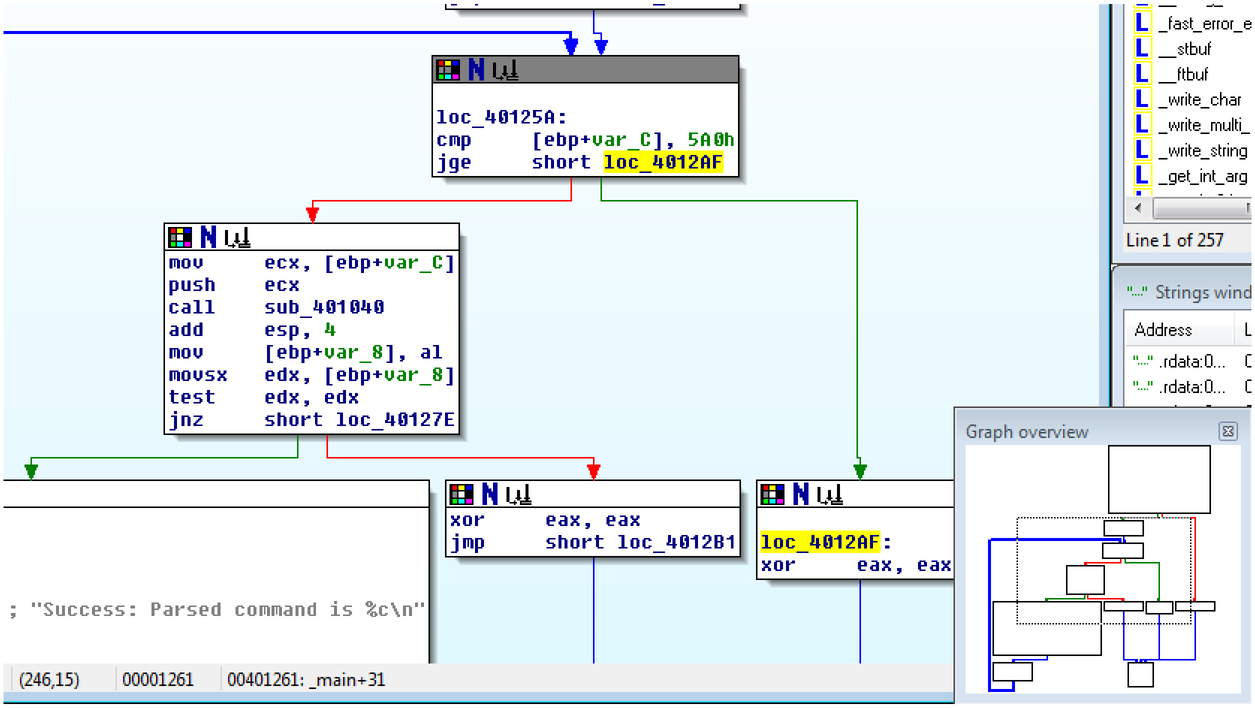
```
loc_4012B1:
mov     esp, ebp
pop     ebp
retn
_main endp
```

S4-Q3. What is the difference between this sample’s parse HTML function and those of the previous samples?

I think it takes an argument on the Agent type. For Sample 3, the agent string is like const ‘Internet Explorer 7.5/pma’. But, for Sample 4, the agent string can take a integer parameter like this ‘Internet Explorer 7.5/pma%d’

S4-Q4. How long will this program run? (Assume that it is connected to the Internet.)

In the main function, we can see branch to a call to ‘sleep’ for 0EA60h (60,000) milliseconds or to an end of main function. The comparison is var_C and 5a0h(hex) value. If the value is greater than 5A0h and then it will end the program or, it will sleep 60,000 millisecond(60 seconds) and it will do something again. Basically, if the condition does not meet, it will loop forever.



```
loc_40125A:
cmp     [ebp+var_C], 5A0h
jge     short loc_4012AF
```

```
mov     ecx, [ebp+var_C]
push    ecx
call    sub_401040
add     esp, 4
mov     [ebp+var_8], al
movsx   edx, [ebp+var_8]
test    edx, edx
jnz     short loc_40127E
```

```
; "Success: Parsed command is %c\n"
```

```
xor     eax, eax
jmp     short loc_4012B1
```

```
loc_4012AF:
xor     eax, eax
```

(246,15) 00001261 00401261: _main+31

S4-Q5. Are there any new network-based indicators for this malware?

In the address of ‘00401040’, we can see the same indicators like Sample2. Those are HTTP User-Agent: Internet Explorer 7.5/pma%, URL: http://www.practicalmalwareanalysis.com/
But we need to notice that there is %d at the end of the Agent type which shows us that it can take input parameter.

S4-Q6. What is the purpose of this malware?

Basically, it is almost the same program with Sample 3. But it has a function that sleeping 60 seconds and do it again. All these thing together, the program tries to download a page(or program) at ‘http://www.practicalmalwareanalysis.com/’. The downloaded program can do 6 things that are ‘create directory’ ‘copy a file’ ‘delete a file’ ‘open registry key value’ ‘set registry key value’ ‘sleep’. However, if it fails to download the page(or program) it will try to again after 60 seconds.
