Kraków, 10.05..23

Laboratorium 4 - Zaawansowana Analiza Statyczna

Julia Sadecka, Cyberbezpieczeństwo

Laboratorium 4.1

1. Adres DllMain

   DllMain znajduje się pod adresem 0x1001516D

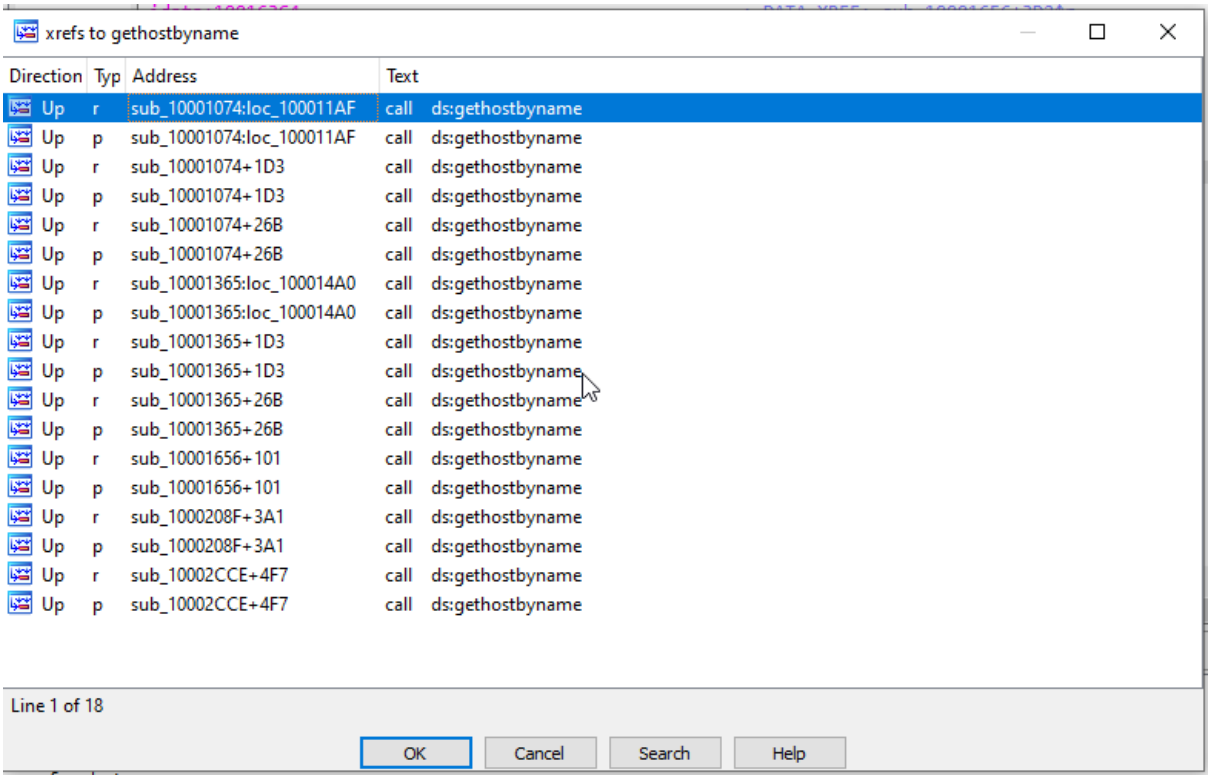
```
.text:1001516D ; BOOL __stdcall DllEntryPoint(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpReserved)
.text:1001516D public DllEntryPoint
.text:1001516D DllEntryPoint proc near
.text:1001516D
```

2. Funkcja gethostbyname

   Znajduje się pod adresem 0x100163CC

3. Jest wywoływany

   9 razy



4. Żądanie DNS

   Pod adresem 0x10001757 zostanie wysłane żądanie DNS pod adres pics.practicalmalwareanalysis.com

```
.data:10019040 off_10019040    dd offset aThisIsRdoPicsP
.data:10019040                                          ; DATA XREF: sub_10001656:loc_10001722↑r
.data:10019040                                          ; sub_10001656+F8↑r ...
.data:10019040                                          ; "[This is RDO]pics.praticalmalwareanalys"...
```

5. Zmienne lokalne

   Program rozpoznał 23 zmienne lokalne

6. Liczba parametrów

   Rozpoznał 1 parametr dla adresu 0x10001656 (offset +)

7. Łańcuch \cmd /c

   cmd.exe znajduje się pod adresem 10095B34

```
kdoors_d:10095B34     aCmdExeC        db '\cmd.exe /c ',0     ; DATA XREF: sub_1000FF58+278↑o
```

8. Działanie \cmd.exe

   Analizując graf widać dużo odwołań do funkcji memcmp, może ona porównywać łańcuchy znaków. Znajduje się tu też tekst “This remote shell session”. Może to oznaczać, że malware próbuje zainstalować backdoora.

9. Zmienna dword_1008E5C4

   W tej zmiennej przechowywane jest wersja systemu operacyjnego.

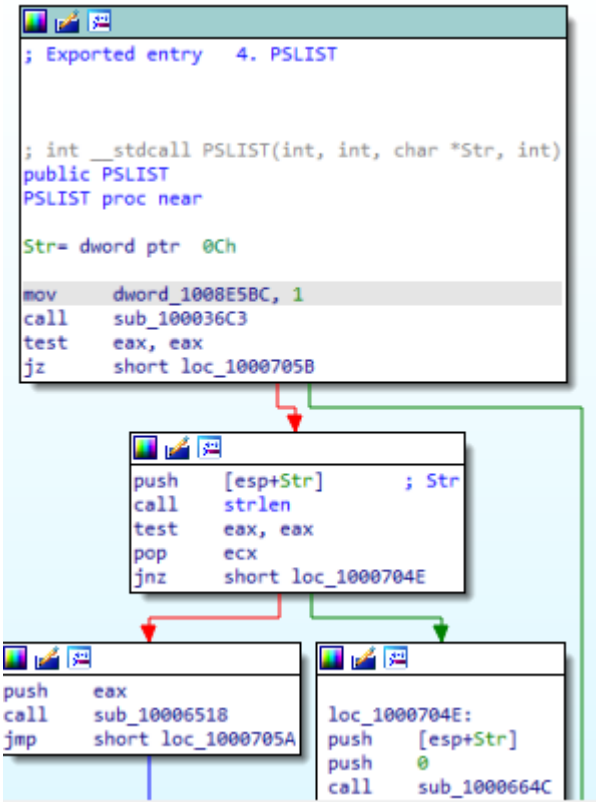
```
.text:10003695     ; Attributes: bp-based frame
.text:10003695
.text:10003695     sub_10003695 proc near
.text:10003695
.text:10003695     VersionInformation= _OSVERSIONINFOA ptr -94h
.text:10003695
.text:10003695 000 push    ebp
.text:10003696 004 mov     ebp, esp
.text:10003698 004 sub     esp, 94h        ; Integer Subtraction
.text:1000369E 098 lea     eax, [ebp+VersionInformation] ; Load Effective Address
.text:100036A4 098 mov     [ebp+VersionInformation.dwOSVersionInfoSize], 94h
.text:100036AE 098 push    eax             ; lpVersionInformation
.text:100036AF 09C call    ds:GetVersionExA ; Indirect Call Near Procedure
.text:100036AF
.text:100036B5 098 xor     eax, eax        ; Logical Exclusive OR
.text:100036B7 098 cmp     [ebp+VersionInformation.dwPlatformId], 2 ; Compare Two Operands
.text:100036BE 098 setz    al              ; Set Byte if Zero (ZF=1)
.text:100036C1 098 leave                   ; High Level Procedure Exit
.text:100036C2 000 retn                    ; Return Near from Procedure
.text:100036C2
.text:100036C2     sub_10003695 endp
.text:100036C2
```

10.

    Informacja jest wysyłana przez Socketa. Wywoływana jest funkcja sub_100052A2

11. PSLIST

    Funkcja PSLIST wywołuje funkcję sub_100036C3.



Funkcja ta sprawdza i porównuje wersję systemu

.dwOSVersionInfoSize = 94h (148) oznacza system operacyjny Windows 95/98/Me

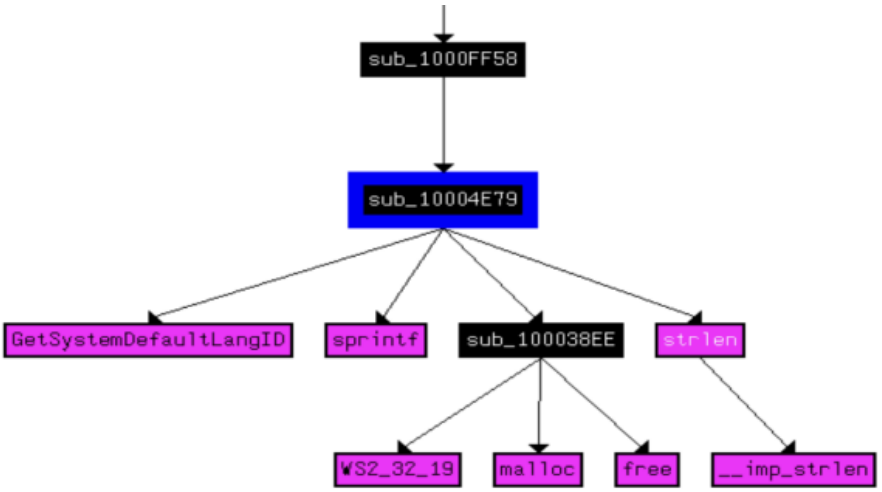
.dwPlatformId = 2 oznacza Windows NT lub nowszy

.dwMajorVersion = 5 oznacza Windows XP/Windows 2003/Windows 2000

Funkcja PSLIST wykorzystuje też funkcję sub_1000664C, która wywołuje CreateToolhelp32Snapshot, która wykonuje migawkę określonych procesów, a także sterty, moduły i wątki używane przez te procesy.

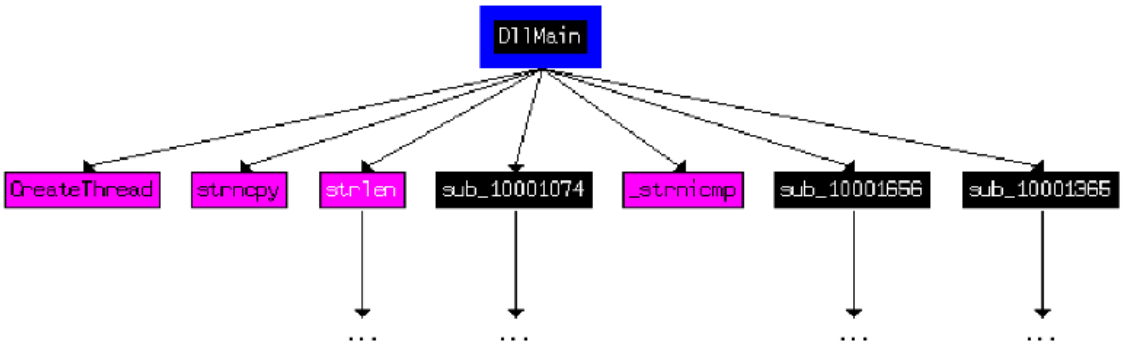
```
push    2               ; dwFlags
stosb
call    CreateToolhelp32Snapshot
mov     esi, ds:CloseHandle
cmp     eax, 0FFFFFFFFh
mov     [ebp+hSnapshot], eax
jz      loc_10006640
```

12. Funkcje API w sub_10004E79



Na grafie widzimy, że wywoływana jest funkcja GetSystemDefaultLangID. Można ją nazwać np. getLanguage

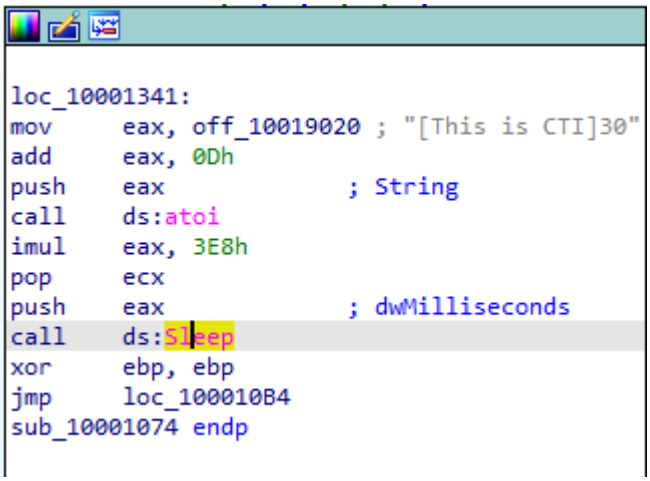
13. Funkcje wywołane przez DllMain



Funkcja bezpośrednio 7 funkcji. Na głębokości 2 jest ich ponad 60.

14. Długość uśpienia

Funkcja wywołuje rejestr eax, który na początku jest stringiem [This is CTI]30 wcześniej jest dodawane 0Dh (13), czyli ze stringu zostaje 30. Następnie mnożony jest przez 3E8 (1000).
Oznacza to, że jest uśpiony na 30000 milisekund.



15. Parametry socket

    Są to: protocol, type, af

16. Funkcja in

    Jest używana do wykrywania maszyn wirtualnych.

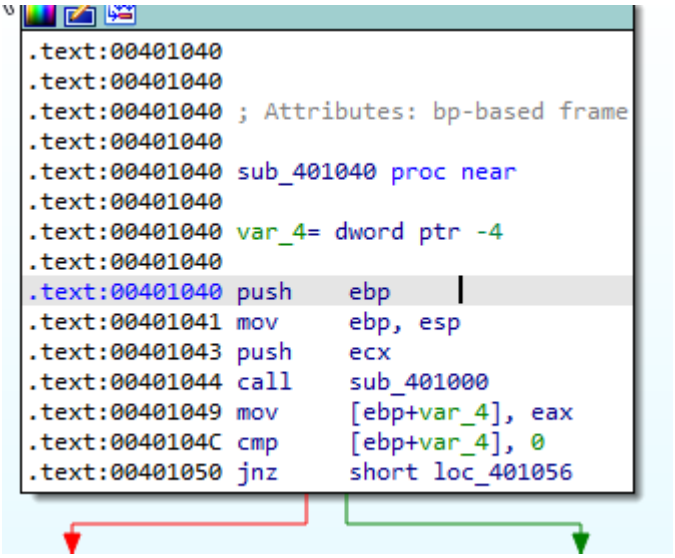
17. Adres 0x1001D988

Znajdują się losowe dane

Laboratorium 4.2

1. Konstrukcja w main

   Przez main wywoływany jest program 0x401000



Wywołuje on funkcje InternetGetConnectedState, która jest funkcją API systemu Windows, która służy do sprawdzenia, czy komputer jest obecnie połączony z Internetem czy nie.

```
.text:00401006 push    0               ; lpdwFlags
.text:00401008 call    ds:InternetGetConnectedState
```

2. Podprogram pod adresem 0x40105F

   Jest to funkcja printf. Ponieważ odkłada na stos łańcuchy znaków.

3. Działanie programu

   Program funkcją InternetGetConnectedState sprawdza połącznie z internetem.

Laboratorium 4.3

1. Operacja w main

   Pierwszym wywoływanym programem jest funkcja InternetGetConnectedState

```
.text:00401000 push    ebp
.text:00401001 mov     ebp, esp
.text:00401003 push    ecx
.text:00401004 push    0               ; dwReserved
.text:00401006 push    0               ; lpdwFlags
.text:00401008 call    ds:InternetGetConnectedState
.text:0040100E mov     [ebp+var_4], eax
```

2. Podprogram pod adresem 0x40117F

   Jest to funkcja print, ponieważ wcześniej dostajemy argumenty, które zostaną wyświetlone w formie łańcucha.

```
.text:0040117F sub_40117F proc near
.text:0040117F
.text:0040117F arg_0= dword ptr  4
.text:0040117F arg_4= byte ptr  8
.text:0040117F
.text:0040117F push    ebx
.text:00401180 push    esi
```

3. Podprogram w main

   Podprogram 401040 wykonuje sporo funkcji związanych z Internetem: InternetOpenA (która otwiera przeglądarkę Internet Explorer 7.5), InternetOpenURLA (która otwiera stronę www.practicalmalwareanalysis.com), InternetReadFile (odczytująca zawartość strony i zapisywana w [ebp+Buffer]), InternetCloseHandle,

```
.text:00401040 push    ebp
.text:00401041 mov     ebp, esp
.text:00401043 sub     esp, 210h
.text:00401049 push    0               ; dwFlags
.text:0040104B push    0               ; lpszProxyBypass
.text:0040104D push    0               ; lpszProxy
.text:0040104F push    0               ; dwAccessType
.text:00401051 push    offset szAgent  ; "Internet Explorer 7.5/pma"
.text:00401056 call    ds:InternetOpenA
.text:0040105C mov     [ebp+hInternet], eax
.text:0040105F push    0               ; dwContext
.text:00401061 push    0               ; dwFlags
.text:00401063 push    0               ; dwHeadersLength
.text:00401065 push    0               ; lpszHeaders
.text:00401067 push    offset szUrl    ; "http://www.practicalmalware
.text:0040106C mov     eax, [ebp+hInternet]
.text:0040106F push    eax             ; hInternet
.text:00401070 call    ds:InternetOpenUrlA
.text:00401076 mov     [ebp+hFile], eax
```

4. Indykatory sieciowe

   Jak w poprzednim zadaniu, są to:
   - www.practicalmalwareanalysis.com
   - Internet Explorer 7.5

5. Cel złośliwego pliku

   Program sprawdza połączenie z Internetem. Jeżeli próba się powiedzie to następnie łączy się ze stroną www.practicalmalwareanalysis.com i odczytuje z niej zawartość i wypisuje ją. Po tym program się usypia na minutę.