

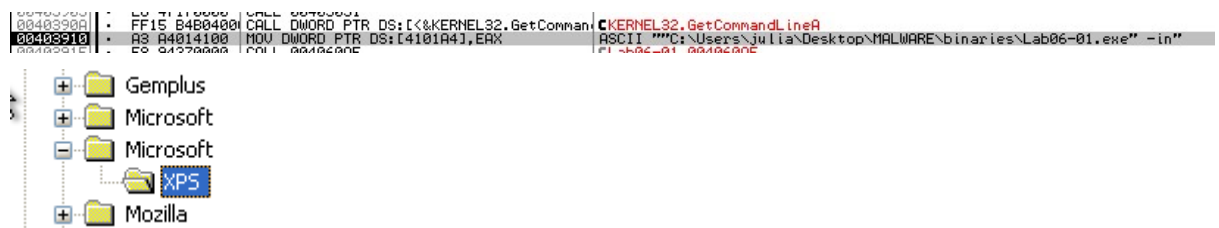
Laboratorium 5 – Zaawansowana analiza dynamiczna

Julia Sadecka, Cyberbezpieczeństwo

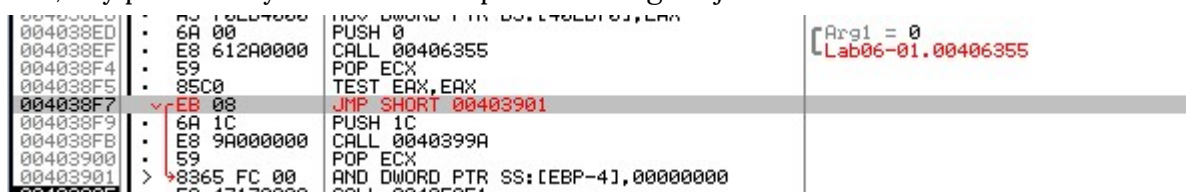
Laboratorium 5.1

1. Zmuszenie malware do instalacji

Aby malware się zainstalowało można albo wprowadzić argument '-in' i wpisać hasło. Takim sposobem możemy zobaczyć, że w rejestrach malware stworzyło nam w SOFTWARE folder Microsoft z folderem XPS.



Można też gdy nie zna się hasła zmienić plik binarny np. zamiast JNZ wprowadzić JNB, aby przeskoczyło od razu do wprowadzanego rejestru



2. Argumenty wiersza poleceń

Funkcja -cc posiada 8 argumentów, które następnie wypisuje w postaci: "k: h: p: pre: ". Są to informacje o konfiguracji:

k=ups

h=host:<http://www.practicalmalwareanalysis.com>

p=port:80

per=60

00402CE5	. 68 64C14000	PUSH Lab06-01.0040C164	ASCII "-cc"
00402CEA	. 8B8D D4E7FFFF	MOV ECX,DWORD PTR SS:[EBP	
00402CF0	. 51	PUSH ECX	
00402CF1	. E8 190B0000	CALL Lab06-01.004033AF	
00402CF6	. 83C4 08	ADD ESP,8	
00402CF9	. 85C0	TEST EAX,EAX	
00402CFB	. 75 74	JNZ SHORT Lab06-01.00402D	
00402CFD	. 837D 08 03	CMP DWORD PTR SS:[EBP+8],	
00402D01	. 75 67	JNZ SHORT Lab06-01.00402D	
00402D03	. 68 00040000	PUSH 400	Arg8 = 00000400
00402D08	. 8D95 E4F3FFFF	LEA EDX,DWORD PTR SS:[EBP	Arg7
00402D0E	. 52	PUSH EDX	Arg6 = 00000400
00402D0F	. 68 00040000	PUSH 400	Arg5
00402D14	. 8D85 E4E7FFFF	LEA EAX,DWORD PTR SS:[EBP	Arg4 = 00000400
00402D1A	. 50	PUSH EAX	Arg3
00402D1B	. 68 00040000	PUSH 400	Arg2 = 00000400
00402D20	. 8D8D E4EFFFFF	LEA ECX,DWORD PTR SS:[EBP	Arg1
00402D26	. 51	PUSH ECX	Lab06-01.00401280
00402D27	. 68 00040000	PUSH 400	
00402D2C	. 8D95 E4EBFFFF	LEA EDX,DWORD PTR SS:[EBP	
00402D32	. 52	PUSH EDX	
00402D33	. E8 48E5FFFF	CALL Lab06-01.00401280	

.text:00402D5B 1840 push^{wt} offset AKSHSPSPerS ; "k:%s h:%s p:%s per:%s\n"

00402D5B	. 68 01000000	MOV EAX,1	
00402D6A	. EB 29	JMP SHORT Lab06-01.00402D8F	
00402D8C	. 68 14C14000	PUSH Lab06-01.0040C114	Arg4 = 0040C114 ASCII "60"
00402D8D	. 68 10C14000	PUSH Lab06-01.0040C110	Arg3 = 0040C110 ASCII "80"
00402D9D	. 68 E8C04000	PUSH Lab06-01.0040C0E8	Arg2 = 0040C0E8 ASCII "http://www.practicalmalwa
00402D9E	. 68 E4C04000	PUSH Lab06-01.0040C0E4	Arg1 = 0040C0E4 ASCII "ups"
00402D9F	. E8 8BE7FFFF	CALL Lab06-01.00401070	Lab06-01.00401070
00402DA5	. 83C4 10	ADD ESP,10	
00402DA6	. 85C0	TEST EAX,EAX	

Funkcja -c pobiera 4 argumenty. Jeżeli nie istnieje to funkcja tworzy klucz rejestru.

00402C5B	. 68 68C14000	PUSH Lab06-01.0040C168	ASCII "-c"
00402C60	. 8B8D D8E7FFFF	MOV ECX,DWORD PTR SS:[EBP	
00402C66	. 51	PUSH ECX	
00402C67	. E8 A30B0000	CALL Lab06-01.0040380F	
00402C6C	. 83C4 08	ADD ESP,8	
00402C6F	. 85C0	TEST EAX,EAX	
00402C71	. 75 66	JNZ SHORT Lab06-01.00402C	
00402C73	. 837D 08 07	CMP DWORD PTR SS:[EBP+8],	
00402C77	. 75 56	JNZ SHORT Lab06-01.00402C	
00402C79	. 8B55 0C	MOV EDX,DWORD PTR SS:[EBP	
00402C7C	. 8B42 08	MOV EAX,DWORD PTR DS:[EDX	
00402C7F	. 8985 E8F7FFFF	MOV DWORD PTR SS:[EBP-818	
00402C85	. 8B4D 0C	MOV ECX,DWORD PTR SS:[EBP	
00402C88	. 8B51 0C	MOV EDX,DWORD PTR DS:[ECX	
00402C8B	. 8995 ECF7FFFF	MOV DWORD PTR SS:[EBP-814	
00402C91	. 8B45 0C	MOV EAX,DWORD PTR SS:[EBP	
00402C94	. 8B48 10	MOV ECX,DWORD PTR DS:[EAX	
00402C97	. 898D E4F7FFFF	MOV DWORD PTR SS:[EBP-81C	
00402C9D	. 8B55 0C	MOV EDX,DWORD PTR SS:[EBP	
00402CA0	. 8B42 14	MOV EAX,DWORD PTR DS:[EDX	
00402CA3	. 8985 F0F7FFFF	MOV DWORD PTR SS:[EBP-810	
00402CA9	. 8B8D F0F7FFFF	MOV ECX,DWORD PTR SS:[EBP	
00402CAF	. 51	PUSH ECX	Arg4
00402CB0	. 8B95 E4F7FFFF	MOV EDX,DWORD PTR SS:[EBP	Arg3
00402CB6	. 52	PUSH EDX	Arg2
00402CB7	. 8B85 ECF7FFFF	MOV EAX,DWORD PTR SS:[EBP	Arg1
00402CBD	. 50	PUSH EAX	Lab06-01.00401070
00402CBE	. 8B8D E8F7FFFF	MOV ECX,DWORD PTR SS:[EBP	
00402CC4	. 51	PUSH ECX	
00402CC5	. E8 A6E3FFFF	CALL Lab06-01.00401070	
00402CCA	. 83C4 10	ADD ESP,10	

Funkcja -re usuwa usługę, a także wpis w rejestrze

push offset aRe ; "-re"

3. Zmiany w malware

Tak jak w punkcie pierwszym można zmienić funkcję JNB (jump if not equal) na JMP (jump)

4. Indykatory hostowe

Klucz rejestru który jest tworzony:

0000C040	ASCII	SOFTWARE\Microsoft\XPS
----------	-------	------------------------

5. Wykorzystanie przy pomocy Internetu

Oprogramowanie może dostać instrukcję przez sieć, aby zrobić którąś z poniższych funkcji:

- SLEEP - przez określony czas malware nic nie wykonuje
- UPLOAD - odczytuje plik z sieci
- NOTHING - malware dostaje informację, że ma nic nie robić
- CMD - otwiera terminal wiersza poleceń
- DOWNLOAD - wysyła przez sieć plik do lokalnego hosta

30402042	• B8 01000000	MOV EAX,1	
30402047	• E9 0C030000	JMP Lab06-01.00402358	
3040204C	• BF C4C04000	MOV EDI,Lab06-01.0040C0C4	ASCII "SLEEP"
30402051	• 83C9 FF	OR ECX,FFFFFFFF	
30402054	• 33C0	XOR EAX,EAX	
30402056	• F2:AE	REPNE SCAS BYTE PTR ES:IE	
30402058	• F7D1	NOT ECX	
304020D2	• BF B8C04000	MOV EDI,Lab06-01.0040C0B8	ASCII "UPLOAD"
304020D7	• 83C9 FF	OR ECX,FFFFFFFF	
304020DA	• 33C0	XOR EAX,EAX	
304020DC	• F2:AE	REPNE SCAS BYTE PTR ES:IE	
304020DF	• F7D1	NOT ECX	
3040232E	• EB 26	JMP SHORT Lab06-01.004023	
30402330	• BF 98C04000	MOV EDI,Lab06-01.0040C098	ASCII "NOTHING"
30402335	• 83C9 FF	OR ECX,FFFFFFFF	
30402338	• 33C0	XOR EAX,EAX	
3040233A	• F2:AE	REPNE SCAS BYTE PTR ES:IE	
3040233C	• F7D1	NOT ECX	
3040223A	• BF A8C04000	MOV EDI,Lab06-01.0040C0A8	ASCII "CMD"
3040223F	• 83C9 FF	OR ECX,FFFFFFFF	
30402242	• 33C0	XOR EAX,EAX	
30402244	• F2:AE	REPNE SCAS BYTE PTR ES:IE	
30402246	• F7D1	NOT ECX	
30402186	• BF ACC04000	MOV EDI,Lab06-01.0040C0AC	ASCII "DOWNLOAD"
3040218B	• 83C9 FF	OR ECX,FFFFFFFF	
3040218E	• 33C0	XOR EAX,EAX	

6. Wskaźniki sieciowe

- Strona www.practicalmalwareanalysis.com

0000C0E8	ASCII	http://www.practicalmalwareanalysis.com
----------	-------	---

- Malware łączy się przez port 80

Laboratorium 5.2

1. Łańcuchy znaków

Jesteśmy w stanie odnaleźć dwa zaciemnione łańcuchy znaków. Znajduje się także string cmd

```
|cmd |
31h ; '1'
71h ; 'q'
61h ; 'a'
7Ah ; 'z'
32h ; '2'
77h ; 'w'
73h ; 's'
78h ; 'x'
33h ; '3'
65h ; 'e'
64h ; 'd'
63h ; 'c'
0
1 ; 'o'
63h ; 'c'
6Ch ; 'l'
2Eh ; '.'
65h ; 'e'
78h ; 'x'
65h ; 'e'
0
1qaz2wsx3edc
ocl.exe
```

2. Wyniki programu

Funkcja najpierw używa funkcji GetVersion. Następnie pobiera ścieżkę do uruchomionego pliku i zapisuje ją w rejestrach.

```
Registers (FPU)
EAX 005F40F8 ASCII ""C:\Users\julia\Desktop\MALWARE\binaries\Ls
FCX 00750F56
```

Odczytuje końcówkę ścieżki i porównuje ją z ocl.exe. Jeżeli nie są takie same kończy swoje działanie.

```
EAX 00000001
ECX 0019FC58 ASCII "Lab06-02.exe"
EDX 0019FD90 ASCII "ocl.exe"
EBX 0039F000
```

3. Uruchomienie szkodliwej zawartości

Aby plik uruchomił szkodliwą zawartość należy zatem zmienić jego nazwę na ocl.exe. Program porówna nazwę, a następnie zacznie wykonywać dalej program

```

00401400 74 26 JZ SHORT 00401500
0040140A 3A61 01 CMP AH, BYTE PTR DS:[ECX+1]
004014D0 75 25 JNE SHORT 00401504
004014DF 0AE4 OR AH, AH
004014E1 74 1D JZ SHORT 00401500
004014E3 C1E8 10 SHR EAX, 10
004014E6 3A41 02 CMP AL, BYTE PTR DS:[ECX+2]
004014E9 75 19 JNE SHORT 00401504
004014EB 0AC0 OR AL, AL
004014ED 74 11 JZ SHORT 00401500
004014EF 3A61 03 CMP AH, BYTE PTR DS:[ECX+3]
004014F2 75 10 JNE SHORT 00401504
004014F4 83C1 04 ADD ECX, 4
004014F7 83C2 04 ADD EDX, 4
004014FA 0AE4 OR AH, AH
004014FC 75 02 JNZ SHORT 004014D0
004014FE 8BFF MOV EDI, EDI
00401500 33C0 XOR EAX, EAX
Stack [0019FC5E]=65 ('e')
AL=65 ('e')

```

4. Działanie pod adresem 0x00401133

Znajduje się tu zaciemniony string 1qaz2wsx3edc. Zaciemniony jest ponieważ jest zapisany znak po znaku (screen z podpunktu 1).

5. Argumenty 0x00401089

Jest wprowadzony ciąg znaków z adresu 0x00401133 i wskaźnik do bufora danych. Następnie ten ciąg jest XORowany kilka razy. Po tym powstaje domena www.practicalmalwareanalysis.com

```

004010B9 50 PUSH EAX Arg1 = ASCII "1qaz2wsx3edc"
004010D2 EB 0F JMP SHORT 004010E3
004010D4 8B8D F8FFFFFF MOV ECX, DWORD PTR SS:[LOCAL.66]
004010DA 83C1 01 ADD ECX, 1
004010DD 898D F8FFFFFF MOV DWORD PTR SS:[LOCAL.66], ECX
004010E3 83BD F8FFFFFF CMP DWORD PTR SS:[LOCAL.66], 20
004010EA 7D 31 JGE SHORT 0040111D
004010EC 8B55 0C MOV EDX, DWORD PTR SS:[ARG.2]
004010EF 0395 F8FFFFFF ADD EDX, DWORD PTR SS:[LOCAL.66]
004010F5 0FBE0A MOVSX ECX, BYTE PTR DS:[EDX]
004010F8 8B85 F8FFFFFF MOV EAX, DWORD PTR SS:[LOCAL.66]
004010FE 99 CDQ
004010FF F7BD FCFEFFFF IDIV DWORD PTR SS:[LOCAL.65]
00401105 8B45 08 MOV EAX, DWORD PTR SS:[ARG.1]
00401108 0FBE1410 MOVSX EDX, BYTE PTR DS:[EDX+EAX]
0040110C 33CA XOR ECX, ECX
0040110E 8B85 F8FFFFFF MOV EAX, DWORD PTR SS:[LOCAL.66]
00401114 8B8C05 00FFFF MOV BYTE PTR SS:[EAX+EBP-100], CL
0040111B EB B7 JMP SHORT 004010D4
0040111D 8D85 00FFFFFF LEA EAX, [LOCAL.64]
00401123 5F POP EDI
CL=70 ('p')
Stack [0019FB18]=00
EAX 0019FB14 ASCII "www.practicalmalwareanalysis.com"

```

6. Domena

Malware wykorzystuje domenę www.practicalmalwareanalysis.com

7. Procedura kodowania

Do zaciemnienia domeny została zastosowana operacja XOR z łańcuchem 1qaz2wsx3edc.

8. CreateProcessA

Proces ten najpierw szuka adresu IP domeny (www.practicalmalwareanalysis.com). Włącza command line (nie pokazując

okienka na monitorze) i następnie pobierając instrukcje ze strony wykonuje je w cmd.

```
06/06/23 06:13:20 PM [ DNS Server] Received A request for domain 'www.practicalmalwareanalysis.com'.
06/06/23 06:13:21 PM [ Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
06/06/23 06:13:25 PM [ Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
06/06/23 06:13:28 PM [ Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103
06/06/23 06:13:33 PM [ Diverter] ICMP type 3 code 1 192.168.56.103->192.168.56.103

.text:0040103B 05C mov [ebp+StartupInfo.wShowWindow], 0
```

8. Opisz znaczenie wywołania CreateProcessA znajdującego się pod adresem 0x0040106E w nawiązaniu do tego malware?

Laboratorium 5.3

1. Biblioteki dll

Ładują się 4 biblioteki dll (program PPEE). Dynamicznie ładuje się biblioteka user32.dll

000055BC	KERNEL32.dll	000054CC	00000000	00000000	00005014
000055DE	NETAPI32.dll	00005570	00000000	00000000	000050B8
000055F8	DLL1.dll	000054B8	00000000	00000000	00005000
0000561C	DLL2.dll	000054C0	00000000	00000000	00005008

```
.text:00403B81 00C push offset aUser32Dll ; "user32.dll"
.text:00403B86 010 call ds:LoadLibraryA ; Indirect Call Near Procedure
.text:00403B8C 00C mov [ebp+LibFileName], offset aLibFileName ; "DLL3.dll"
.text:0040103C 020 push offset LibFileName ; "DLL3.dll"
.text:00401041 024 call ds:LoadLibraryA ; Indirect Call Near Procedure
```

2. Wymagany adres bazowy

Adres bazowy wymagany przez biblioteki DLL1.dll, DLL2.dll i DLL3.dll to 0x10000000

pFile	Data	Description
000000F8	010B	Magic
000000FA	06	Major Linker Version
000000FB	00	Minor Linker Version
000000FC	00006000	Size of Code
00000100	00007000	Size of Initialized Data
00000104	00000000	Size of Uninitialized Data
00000108	00001152	Address of Entry Point
0000010C	00001000	Base of Code
00000110	00007000	Base of Data
00000114	10000000	Image Base

3. Przypisany adres bazowy

DLL1 - 10000000

DLL2 - 001D0000

DLL3 - 001E0000

Base	Size	Entry	Name
001D0000	0000E000	001D1174	DLL2
00400000	00009000	004010A2	Lab06-03
10000000	0000E000	10001152	DLL1
73070000	00014000	730710FA	NFTAPI32

Base	Size	Entry	Name
001D0000	0000E000	001D1174	DLL2
001E0000	0000E000	001E11A1	DLL3
00400000	00009000	004010A2	Lab06-03

4. Działanie funkcji z DLL1.dll

Biblioteka DD1.dll ma dwie funkcje: DLL1Print i DLLMain. Ta pierwsza pokaże napis "DLL 1 mystery data" a także numer procesu. Po sprawdzeniu rzeczywiście taki proces istnieje .

```

-----
PUSH EAX
PUSH OFFSET 10008034
CALL 10001038
ADD ESP, 8

```

ASCII "DLL 1 mystery data %d"

DLL 1 mystery data 1080

```

C:\Users\julia>tasklist | findstr "1080"
Lab06-03.exe           1080 Console           1           5 152 K

```

5. Nazwa pliku

Funkcja WriteFile wykorzystuje nazwę pliku temp.txt

```

.data:10008030          CHAR FileName[]
.data:10008030          FileName          db 'temp.txt',0          ; DATA XREF
.data:10008039                                     align 4

```

6. Dane drugiego parametru NetScheduleJobAdd

Dane do drugiego parametru z funkcji NetScheduleJobAdd pobiera się z DLL3.DLL3GetStructure.

7. Mystery Data

Po wykonaniu program wyświetla w terminalu 3 informacje Mystery Data. Razem z nimi są identyfikatory PID procesów.

```
DLL 1 mystery data 3500
DLL 2 mystery data 232
DLL 3 mystery data 2011328
```

DLL1 jest związane z identyfikatorem bieżącego procesu

```
C:\Users\julia>tasklist | findstr "1080"
Lab06-03.exe                1080 Console                1          5 152 K
```

DLL 2 jest związany z plikiem temp.txt

```
.data:10008030 db 'temp.txt',0 ; DATA XREF
.data:10008030 FileName
.data:10008039 align 4
```

DLL 3 jest związany z łańcuchem znaków ping www.malwareanalysisbook.com

00008038	ASCII	ping www.malwareanalysisbook.com
----------	-------	----------------------------------

8. Ładowanie DLL2.dll

Aby załadować DLL2.dll do IDA, aby było to zgodne z adresem ładowania zastosowanym przez OllyDbg należy w IDA wybrać Manual Load, a następnie adres bazowy tej biblioteki. W moim przypadku adresem bazowym jest 001D0000.