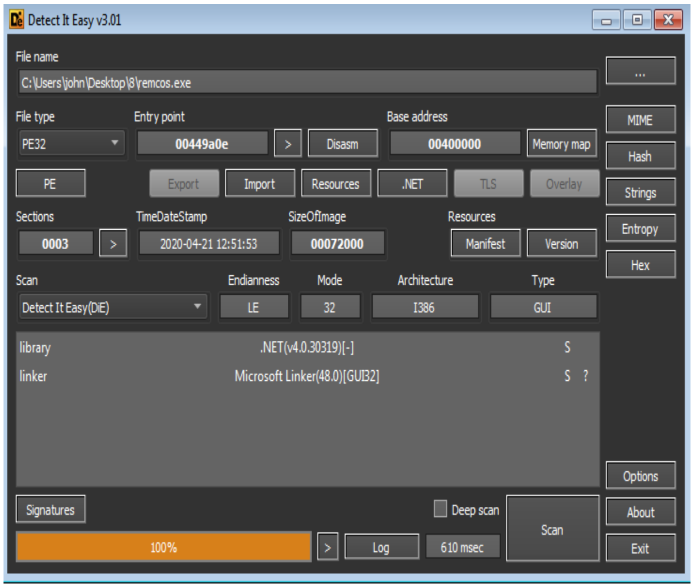
Here initially we uploaded the sample in Detect It Easy to check whether the sample is packed or not , here click on entropy tab we will be able to view the entropy which is high 7.38 and also it is also showing the status as packed.



Detect It Easy v3.01

File name: C:\Users\john\Desktop\8\remcos.exe

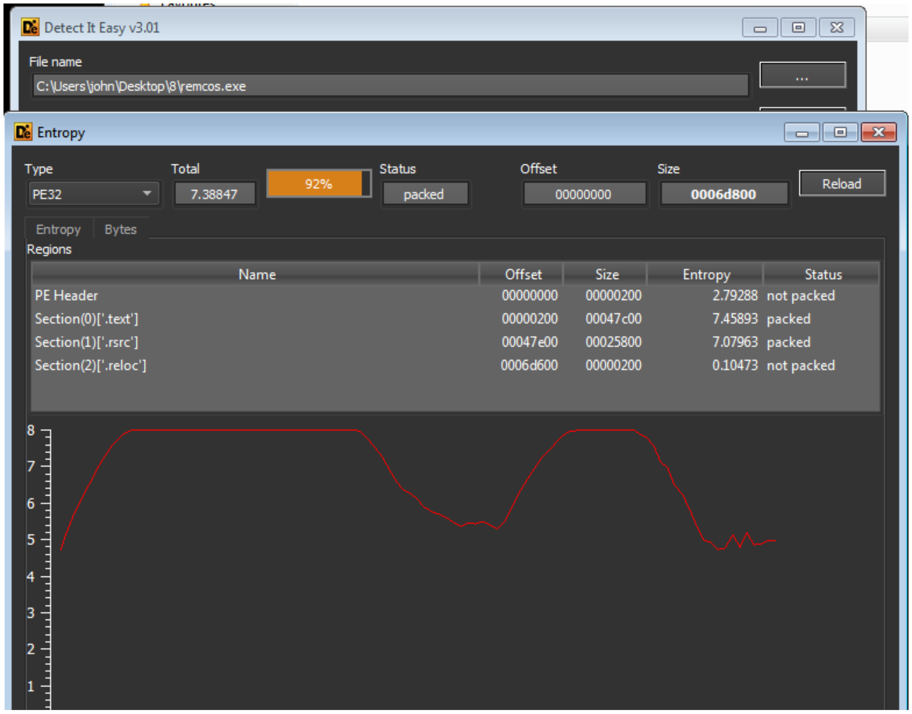
File type: PE32 | Entry point: 00449a0e | Base address: 00400000

Sections: 0003 | TimeDateStamp: 2020-04-21 12:51:53 | SizeOfImage: 00072000

Scan: Detect It Easy(DiE) | Endianness: LE | Mode: 32 | Architecture: I386 | Type: GUI

```
library     .NET(v4.0.30319)[-]              S
linker      Microsoft Linker(48.0)[GUI32]    S  ?
```

100% | 610 msec



Detect It Easy v3.01

File name: C:\Users\john\Desktop\8\remcos.exe

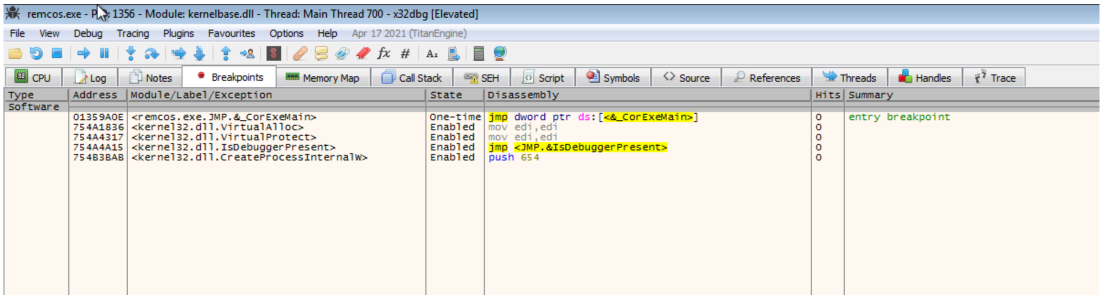
Entropy

Type: PE32 | Total: 7.38847 | 92% | Status: packed | Offset: 00000000 | Size: 0006d800

Regions

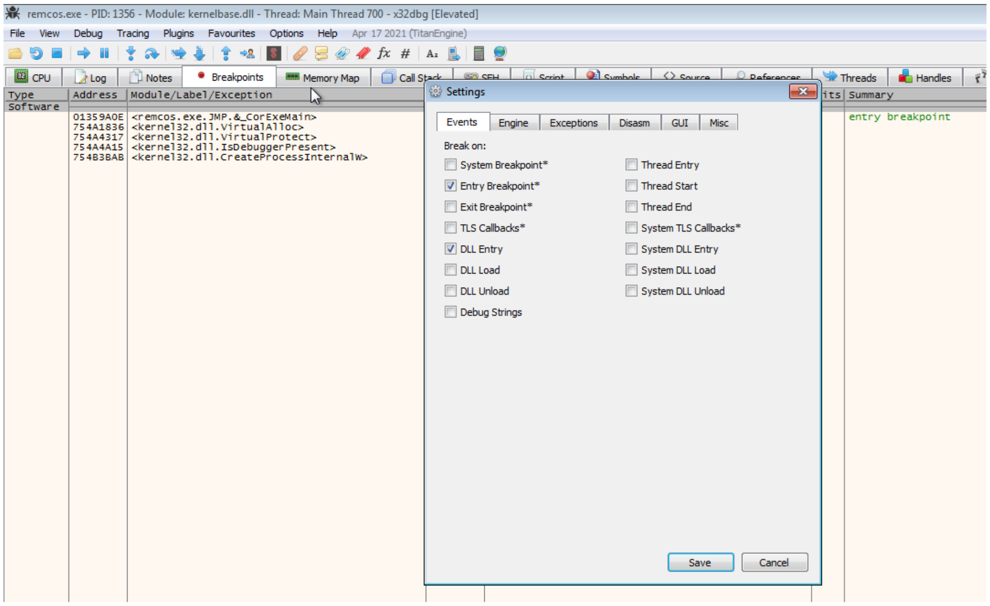
Name	Offset	Size	Entropy	Status
PE Header	00000000	00000200	2.79288	not packed
Section(0)['.text']	00000200	00047c00	7.45893	packed
Section(1)['.rsrc']	00047e00	00025800	7.07963	packed
Section(2)['.reloc']	0006d600	00000200	0.10473	not packed

Now we uploaded the sample in x32dbg and put breakpoint VirtualAlloc, VirtualProtect, IsDebuggerPresent, CreateProcessInternalW.


remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace

```
Type      Address  Module/Label/Exception                 State    Disassembly                          Hits Summary
Software
          01359A0E <remcos.exe.JMP.&_CorExeMain>          One-time jmp dword ptr ds:[<&_CorExeMain>]    0    entry breakpoint
          754A1836 <kernel32.dll.VirtualAlloc>            Enabled  mov edi,edi                          0
          754A4317 <kernel32.dll.VirtualProtect>          Enabled  mov edi,edi                          0
          754A4A15 <kernel32.dll.IsDebuggerPresent>       Enabled  jmp <JMP.&IsDebuggerPresent>         0
          754B3BAB <kernel32.dll.CreateProcessInternalW>  Enabled  push 654                             0
```

Click on Options->Preferences->Event tabs Mark the option i.e. Break on DLL Entry and press f9.

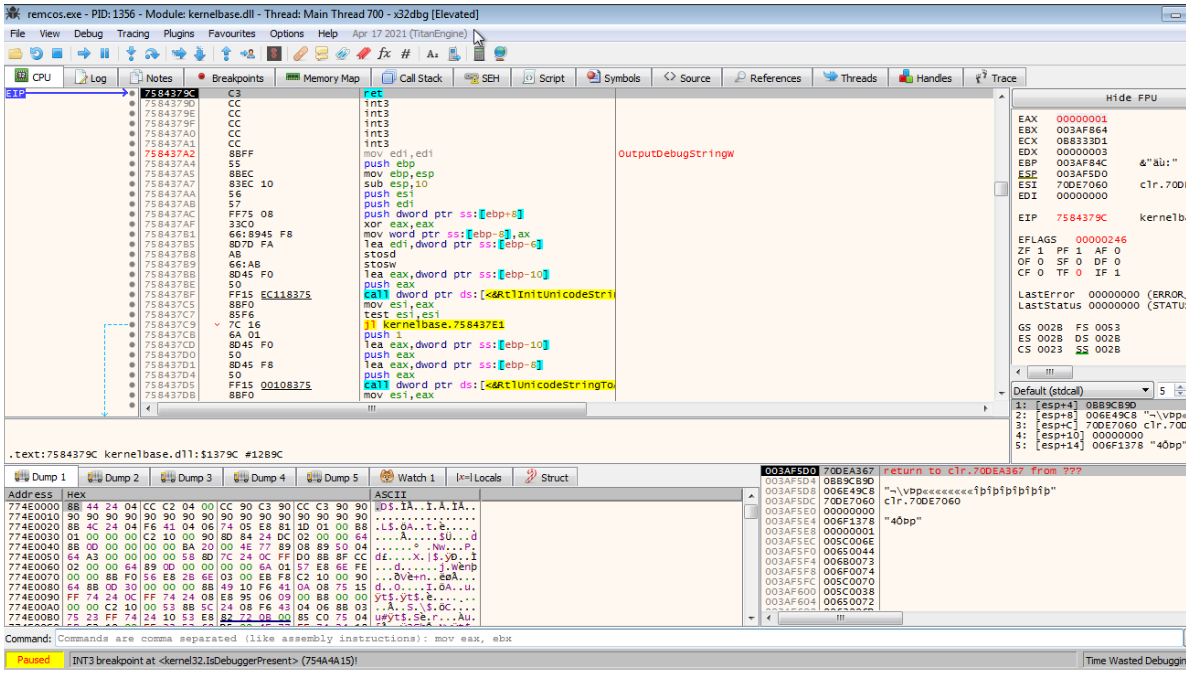

remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles
Settings
Events Engine Exceptions Disasm GUI Misc
Save
Cancel

```
Type      Address  Module/Label/Exception
Software
          01359A0E <remcos.exe.JMP.&_CorExeMain>
          754A1836 <kernel32.dll.VirtualAlloc>
          754A4317 <kernel32.dll.VirtualProtect>
          754A4A15 <kernel32.dll.IsDebuggerPresent>
          754B3BAB <kernel32.dll.CreateProcessInternalW>
```

Break on:

☐ System Breakpoint*	☐ Thread Entry
☑ Entry Breakpoint*	☐ Thread Start
☐ Exit Breakpoint*	☐ Thread End
☐ TLS Callbacks*	☐ System TLS Callbacks*
☑ DLL Entry	☐ System DLL Entry
☐ DLL Load	☐ System DLL Load
☐ DLL Unload	☐ System DLL Unload
☐ Debug Strings	

Here we hit our first breakpoint at IsDebuggerPresent and we change its return value from 1 to 0 and press f9.


remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Default (stdcall) 5
Time Wasted Debuggin

```
EIP --> 7584379C  C3           ret
        7584379D  CC           int3
        7584379E  CC           int3
        7584379F  CC           int3
        758437A0  CC           int3
        758437A1  CC           int3
        758437A2  8BFF         mov edi,edi                                  OutputDebugStringW
        758437A4  55           push ebp
        758437A5  8BEC         mov ebp,esp
        758437A7  83EC 10      sub esp,10
        758437AA  56           push esi
        758437AB  57           push edi
        758437AC  FF75 08      push dword ptr ss:[ebp+8]
        758437AF  33C0         xor eax,eax
        758437B1  66:8945 F8   mov word ptr ss:[ebp-8],ax
        758437B5  8D7D FA      lea edi,dword ptr ss:[ebp-6]
        758437B8  AB           stosd
        758437B9  66:AB        stosw
        758437BB  8D45 F0      lea eax,dword ptr ss:[ebp-10]
        758437BE  50           push eax
        758437BF  FF15 EC118375 call dword ptr ds:[<&RtlInitUnicodeStri
        758437C5  8BF0         mov esi,eax
        758437C7  85F6         test esi,esi
        758437C9  7C 16        jl kernelbase.758437E1
        758437CB  6A 01        push 1
        758437CD  8D45 F0      lea eax,dword ptr ss:[ebp-10]
        758437D0  50           push eax
        758437D1  8D45 F8      lea eax,dword ptr ss:[ebp-8]
        758437D4  50           push eax
        758437D5  FF15 00108375 call dword ptr ds:[<&RtlUnicodeStringTo
        758437DB  8BF0         mov esi,eax

.text:7584379C kernelbase.dll:$1379C #12B9C
```

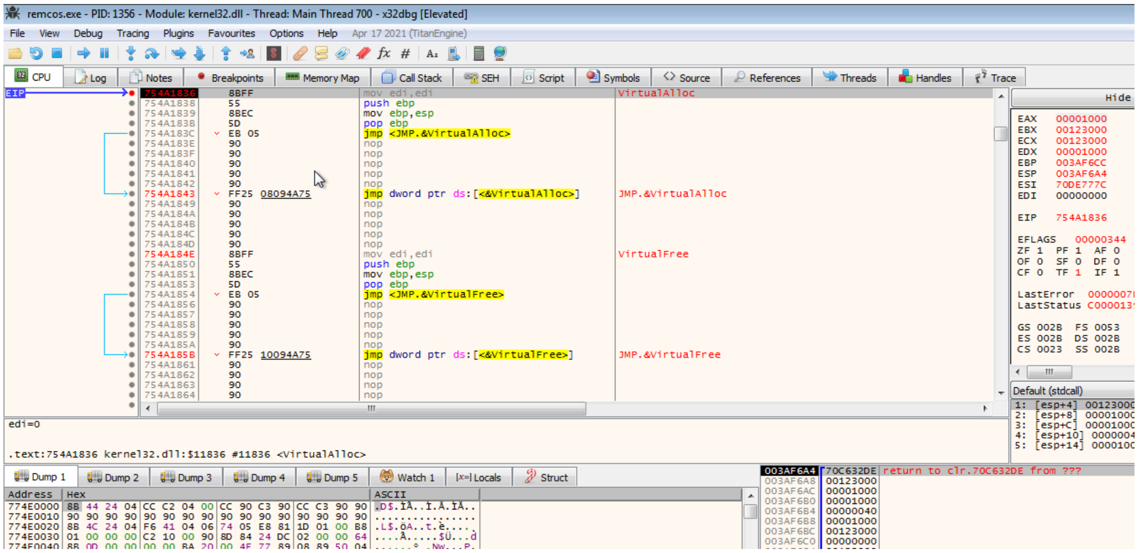
```
EAX   00000001
EBX   003AF864
ECX   0B8333D1
EDX   00000003
EBP   003AF84C     &"äù:"
ESP   003AF5D0
ESI   70DE7060     clr.70DI
EDI   00000000

EIP   7584379C     kernelba

EFLAGS   00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_
LastStatus 00000000 (STATU:

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

1: [esp+4] 0BB9CB9D
2: [esp+8] 006E49C8 "¬\vÞp«
3: [esp+C] 70DE7060 clr.70D
4: [esp+10] 00000000
5: [esp+14] 006F1378 "4ÕÞp"
```

```
Address   Hex                                              ASCII
774E0000  8B 44 24 04 CC C2 04 00 CC 90 C3 90 CC C3 90 90  .D$.ÌÂ..Ì.Ã.ÌÃ..
774E0010  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
774E0020  8B 4C 24 04 F6 41 04 06 74 05 E8 81 1D 01 00 B8  .L$.öA..t.è.....
774E0030  01 00 00 00 C2 10 00 90 8D 84 24 DC 02 00 00 64  ....Â.....$Ü...d
774E0040  8B 0D 00 00 00 00 BA 20 00 4E 77 89 08 89 50 04  ......º .Nw...P.
774E0050  64 A3 00 00 00 00 58 8D 7C 24 0C FF D0 8B 8F CC  d£....X.|$.ÿÐ..Ì
774E0060  02 00 00 64 89 0D 00 00 00 00 6A 01 57 E8 6E FE  ...d......j.Wènþ
774E0070  00 00 8B F0 56 E8 2B 6E 03 00 EB F8 C2 10 00 90  ...ðVè+n..ëøÂ...
774E0080  64 8B 0D 30 00 00 00 8B 49 10 F6 41 0A 08 75 15  d..0....I.öA..u.
774E0090  FF 74 24 0C FF 74 24 08 E8 95 06 09 00 B8 00 00  ÿt$.ÿt$.è.......
774E00A0  00 00 C2 10 00 53 8B 5C 24 08 F6 43 04 06 8B 03  ..Â..S.\$.öC....
774E00B0  75 23 FF 74 24 10 53 E8 82 72 0B 00 85 C0 75 04  u#ÿt$.Sè.r...Àu.
```

```
003AF5D0  70DEA367  return to clr.70DEA367 from ???
003AF5D4  0BB9CB9D
003AF5D8  006E49C8  "¬\vÞp«««««««««îþîþîþîþîþîþ"
003AF5DC  70DE7060  clr.70DE7060
003AF5E0  00000000
003AF5E4  006F1378  "4ÕÞp"
003AF5E8  00000001
003AF5EC  005C006E
003AF5F0  00650044
003AF5F4  006B0073
003AF5F8  006F0074
003AF5FC  005C0070
003AF600  005C0038
003AF604  00650072
```

```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused   INT3 breakpoint at <kernel32.IsDebuggerPresent> (754A4A15)!
```

Now we hit breakpoint at VirtualAlloc just step over it.


remcos.exe - PID: 1356 - Module: kernel32.dll - Thread: Main Thread 700 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Default (stdcall)

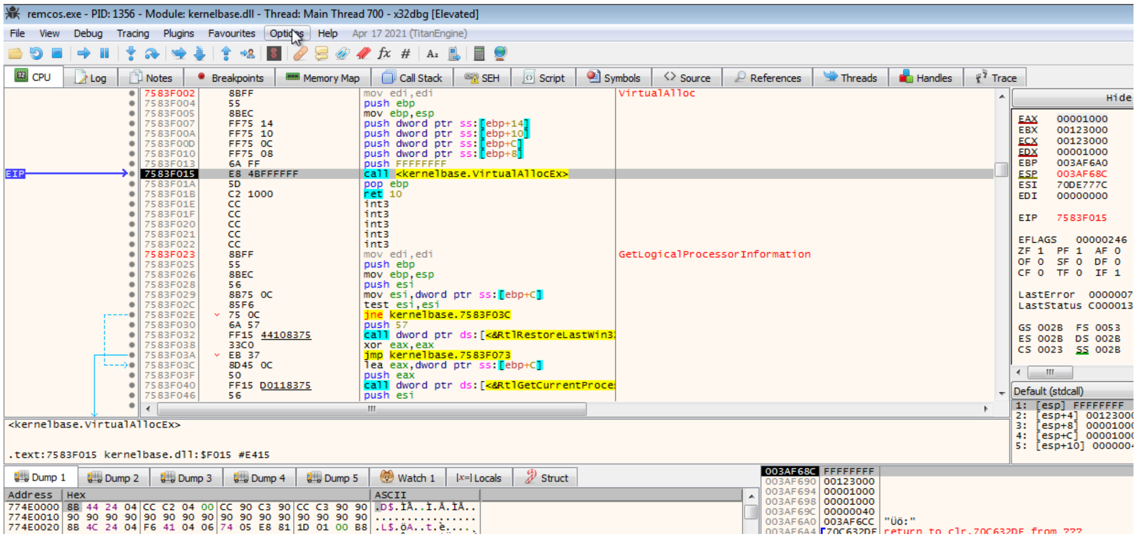
```
EIP --> 754A1836  8BFF          mov edi,edi                          VirtualAlloc
        754A1838  55            push ebp
        754A1839  8BEC          mov ebp,esp
        754A183B  5D            pop ebp
        754A183C  EB 05         jmp <JMP.&VirtualAlloc>
        754A183E  90            nop
        754A183F  90            nop
        754A1840  90            nop
        754A1841  90            nop
        754A1842  90            nop
        754A1843  FF25 08094A75 jmp dword ptr ds:[<&VirtualAlloc>]   JMP.&VirtualAlloc
        754A1849  90            nop
        754A184A  90            nop
        754A184B  90            nop
        754A184C  90            nop
        754A184D  90            nop
        754A184E  8BFF          mov edi,edi                          VirtualFree
        754A1850  55            push ebp
        754A1851  8BEC          mov ebp,esp
        754A1853  5D            pop ebp
        754A1854  EB 05         jmp <JMP.&VirtualFree>
        754A1856  90            nop
        754A1857  90            nop
        754A1858  90            nop
        754A1859  90            nop
        754A185A  90            nop
        754A185B  FF25 10094A75 jmp dword ptr ds:[<&VirtualFree>]    JMP.&VirtualFree
        754A1861  90            nop
        754A1862  90            nop
        754A1863  90            nop
        754A1864  90            nop

edi=0

.text:754A1836 kernel32.dll:$11836 #11836 <VirtualAlloc>
```

```
EAX   00001000
EBX   00123000
ECX   00123000
EDX   00001000
EBP   003AF6CC
ESP   003AF6A4
ESI   70DE777C
EDI   00000000

EIP   754A1836

EFLAGS   00000344
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1

LastError  0000007
LastStatus C000013

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

1: [esp+4] 0012300
2: [esp+8] 0000100
3: [esp+C] 0000100
4: [esp+10] 000000
5: [esp+14] 000010
```

```
Address   Hex                                              ASCII
774E0000  8B 44 24 04 CC C2 04 00 CC 90 C3 90 CC C3 90 90  .D$.ÌÂ..Ì.Ã.ÌÃ..
774E0010  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
774E0020  8B 4C 24 04 F6 41 04 06 74 05 E8 81 1D 01 00 B8  .L$.öA..t.è.....
774E0030  01 00 00 00 C2 10 00 90 8D 84 24 DC 02 00 00 64  ....Â.....$Ü...d
```

```
003AF6A4  70C632DE  return to clr.70C632DE from ???
003AF6A8  00123000
003AF6AC  00001000
003AF6B0  00001000
003AF6B4  00000040
003AF6B8  00001000
003AF6BC  00123000
003AF6C0  00000000
```

Here we just step over this and we can see the return address after this call in eax register.


remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Hide
Default (stdcall)

```
     7583F002   8BFF            mov edi,edi                                VirtualAlloc
     7583F004   55              push ebp
     7583F005   8BEC            mov ebp,esp
     7583F007   FF75 14         push dword ptr ss:[ebp+14]
     7583F00A   FF75 10         push dword ptr ss:[ebp+10]
     7583F00D   FF75 0C         push dword ptr ss:[ebp+C]
     7583F010   FF75 08         push dword ptr ss:[ebp+8]
     7583F013   6A FF           push FFFFFFFF
EIP  7583F015   E8 4BFFFFFF     call <kernelbase.VirtualAllocEx>
     7583F01A   5D              pop ebp
     7583F01B   C2 1000         ret 10
     7583F01E   CC              int3
     7583F01F   CC              int3
     7583F020   CC              int3
     7583F021   CC              int3
     7583F022   CC              int3
     7583F023   8BFF            mov edi,edi                                GetLogicalProcessorInformation
     7583F025   55              push ebp
     7583F026   8BEC            mov ebp,esp
     7583F028   56              push esi
     7583F029   8B75 0C         mov esi,dword ptr ss:[ebp+C]
     7583F02C   85F6            test esi,esi
     7583F02E   75 0C           jne kernelbase.7583F03C
     7583F030   6A 57           push 57
     7583F032   FF15 44108375   call dword ptr ds:[<&RtlRestoreLastWin3
     7583F038   33C0            xor eax,eax
     7583F03A   EB 37           jmp kernelbase.7583F073
     7583F03C   8D45 0C         lea eax,dword ptr ss:[ebp+C]
     7583F03F   50              push eax
     7583F040   FF15 D0118375   call dword ptr ds:[<&RtlGetCurrentProce
     7583F046   56              push esi
```

```
EAX     00001000
EBX     00123000
ECX     00123000
EDX     00001000
EBP     003AF6A0
ESP     003AF68C
ESI     70DE777C
EDI     00000000

EIP     7583F015

EFLAGS    00000246
ZF 1   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1

LastError   0000007
LastStatus C000013

GS 002B   FS 0053
ES 002B   DS 002B
CS 0023   SS 002B
```

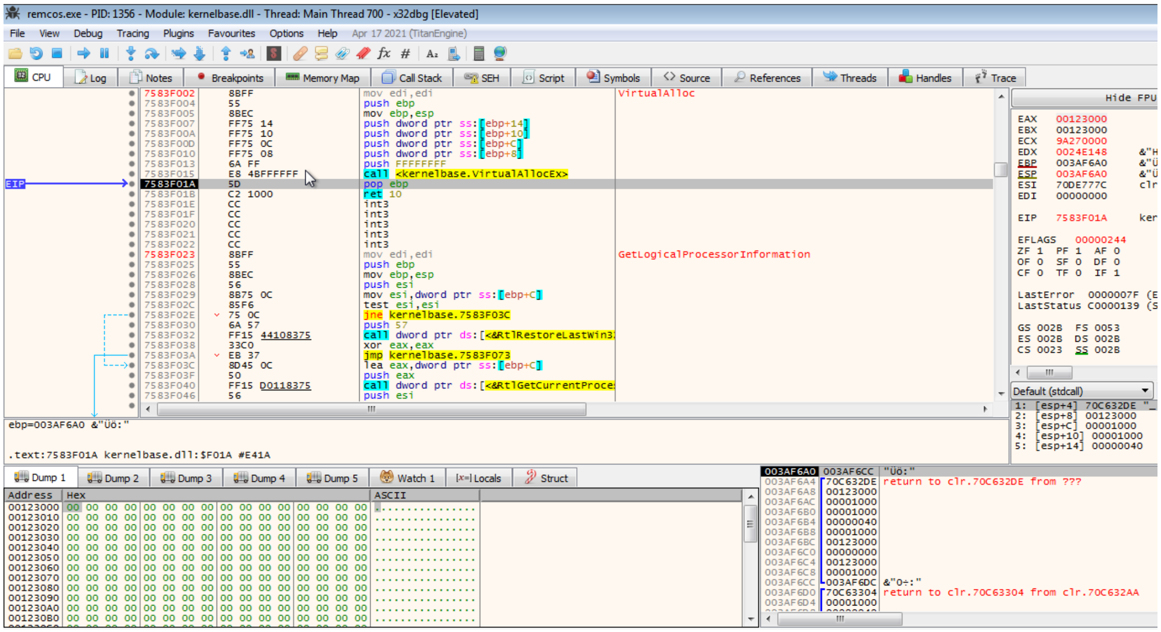
```
1:  [esp] FFFFFFFF
2:  [esp+4]  0012300
3:  [esp+8]  0000100
4:  [esp+C]  0000100
5:  [esp+10] 000000
```

```
<kernelbase.VirtualAllocEx>

.text:7583F015 kernelbase.dll:$F015 #E415
```

```
Address   Hex                                               ASCII
774E0000  8B 44 24 04 CC C2 04 00 CC 90 C3 90 CC C3 90 90  .D$.ÌÂ..Ì.Ã.ÌÃ..
774E0010  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
774E0020  8B 4C 24 04 F6 41 04 06 74 05 E8 81 1D 01 00 B8  .L$.öA..t.è.....
```

```
003AF68C  FFFFFFFF
003AF690  00123000
003AF694  00001000
003AF698  00001000
003AF69C  00000040
003AF6A0  003AF6CC  "Üö:"
003AF6A4  70C632DE  return to clr.70C632DE from ???
```

Here the return address is 123000 , so we follow this in dump1


remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Hide FPU
Default (stdcall)

```
     7583F002   8BFF            mov edi,edi                                VirtualAlloc
     7583F004   55              push ebp
     7583F005   8BEC            mov ebp,esp
     7583F007   FF75 14         push dword ptr ss:[ebp+14]
     7583F00A   FF75 10         push dword ptr ss:[ebp+10]
     7583F00D   FF75 0C         push dword ptr ss:[ebp+C]
     7583F010   FF75 08         push dword ptr ss:[ebp+8]
     7583F013   6A FF           push FFFFFFFF
     7583F015   E8 4BFFFFFF     call <kernelbase.VirtualAllocEx>
EIP  7583F01A   5D              pop ebp
     7583F01B   C2 1000         ret 10
     7583F01E   CC              int3
     7583F01F   CC              int3
     7583F020   CC              int3
     7583F021   CC              int3
     7583F022   CC              int3
     7583F023   8BFF            mov edi,edi                                GetLogicalProcessorInformation
     7583F025   55              push ebp
     7583F026   8BEC            mov ebp,esp
     7583F028   56              push esi
     7583F029   8B75 0C         mov esi,dword ptr ss:[ebp+C]
     7583F02C   85F6            test esi,esi
     7583F02E   75 0C           jne kernelbase.7583F03C
     7583F030   6A 57           push 57
     7583F032   FF15 44108375   call dword ptr ds:[<&RtlRestoreLastWin3
     7583F038   33C0            xor eax,eax
     7583F03A   EB 37           jmp kernelbase.7583F073
     7583F03C   8D45 0C         lea eax,dword ptr ss:[ebp+C]
     7583F03F   50              push eax
     7583F040   FF15 D0118375   call dword ptr ds:[<&RtlGetCurrentProce
     7583F046   56              push esi
```

```
EAX     00123000
EBX     00123000
ECX     9A270000
EDX     0024E148     &"H
EBP     003AF6A0     &"Ü
ESP     003AF6A0     &"Ü
ESI     70DE777C     clr
EDI     00000000

EIP     7583F01A     ker

EFLAGS    00000244
ZF 1   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1

LastError   0000007F (E
LastStatus C0000139 (S

GS 002B   FS 0053
ES 002B   DS 002B
CS 0023   SS 002B
```

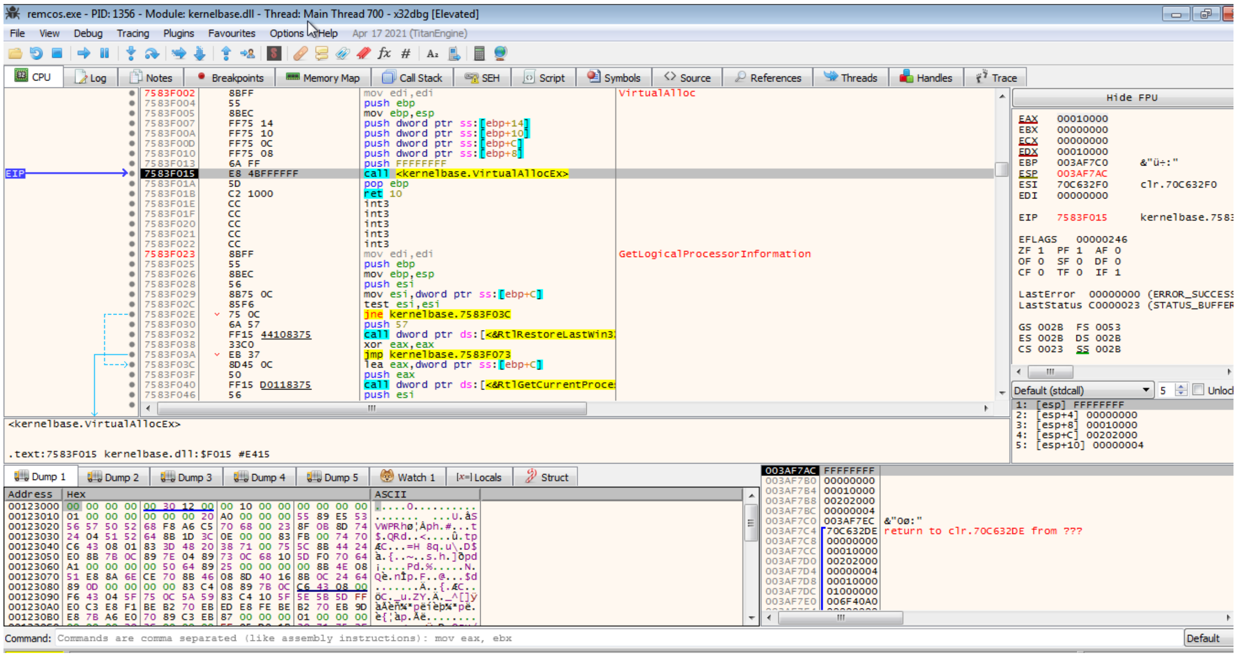
```
1:  [esp+4]  70C632DE "_
2:  [esp+8]  00123000
3:  [esp+C]  00001000
4:  [esp+10]  00001000
5:  [esp+14]  00000040
```

```
ebp=003AF6A0 &"Üö:"

.text:7583F01A kernelbase.dll:$F01A #E41A
```

```
Address   Hex                                               ASCII
00123000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00123010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00123020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00123030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00123040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00123050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00123060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00123070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00123080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00123090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
001230A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
001230B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
003AF6A0  003AF6CC  "Üö:"
003AF6A4  70C632DE  return to clr.70C632DE from ???
003AF6A8  00123000
003AF6AC  00001000
003AF6B0  00001000
003AF6B4  00000040
003AF6B8  00001000
003AF6BC  00123000
003AF6C0  00000000
003AF6C4  00123000
003AF6C8  00001000
003AF6CC  003AF6DC  &"0÷:"
003AF6D0  70C63304  return to clr.70C63304 from clr.70C632AA
003AF6D4  00001000
```

Here we hit breakpoint at VirtualAlloc and step over it, and here the there are some values filled in dump1.


remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace

```
     7583F002   8BFF          mov edi,edi                                    VirtualAlloc
     7583F004   55            push ebp
     7583F005   8BEC          mov ebp,esp
     7583F007   FF75 14       push dword ptr ss:[ebp+14]
     7583F00A   FF75 10       push dword ptr ss:[ebp+10]
     7583F00D   FF75 0C       push dword ptr ss:[ebp+C]
     7583F010   FF75 08       push dword ptr ss:[ebp+8]
     7583F013   6A FF         push FFFFFFFF
EIP  7583F015   E8 4BFFFFFF   call <kernelbase.VirtualAllocEx>
     7583F01A   5D            pop ebp
     7583F01B   C2 1000       ret 10
     7583F01E   CC            int3
     7583F01F   CC            int3
     7583F020   CC            int3
     7583F021   CC            int3
     7583F022   CC            int3
     7583F023   8BFF          mov edi,edi                                    GetLogicalProcessorInformation
     7583F025   55            push ebp
     7583F026   8BEC          mov ebp,esp
     7583F028   56            push esi
     7583F029   8B75 0C       mov esi,dword ptr ss:[ebp+C]
     7583F02C   85F6          test esi,esi
     7583F02E   75 0C         jne kernelbase.7583F03C
     7583F030   6A 57         push 57
     7583F032   FF15 44108375 call dword ptr ds:[<&RtlRestoreLastWin3
     7583F038   33C0          xor eax,eax
     7583F03A   EB 37         jmp kernelbase.7583F073
     7583F03C   8D45 0C       lea eax,dword ptr ss:[ebp+C]
     7583F03F   50            push eax
     7583F040   FF15 D0118375 call dword ptr ds:[<&RtlGetCurrentProce
     7583F046   56            push esi

<kernelbase.VirtualAllocEx>

.text:7583F015 kernelbase.dll:$F015 #E415
```

```
Hide FPU

EAX     00010000
EBX     00000000
ECX     00000000
EDX     00010000
EBP     003AF7C0     &"ü÷:"
ESP     003AF7AC
ESI     70C632F0     clr.70C632F0
EDI     00000000

EIP     7583F015     kernelbase.7583

EFLAGS   00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS
LastStatus C0000023 (STATUS_BUFFER

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

Default (stdcall)  5  Unlock
1: [esp] FFFFFFFF
2: [esp+4] 00000000
3: [esp+8] 00010000
4: [esp+C] 00202000
5: [esp+10] 00000004
```

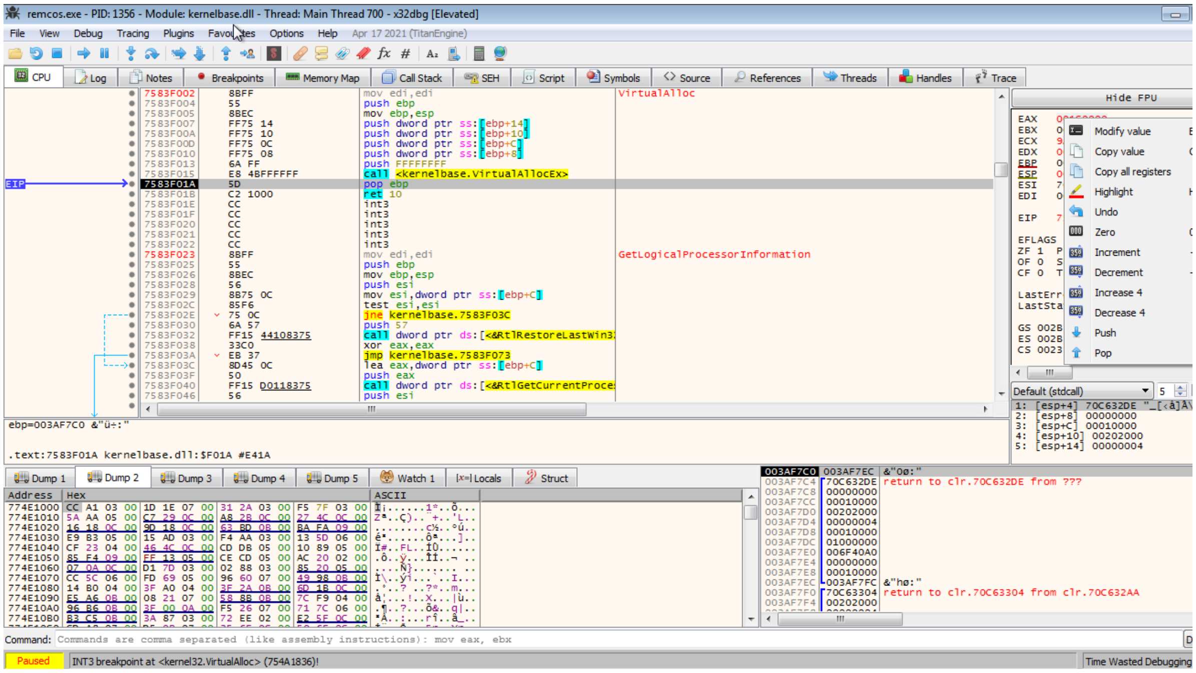
```
Address  Hex                                              ASCII
00123000 00 00 00 00 00 30 12 00 00 10 00 00 00 00 00 00  .....0..........
00123010 01 00 00 00 00 00 00 20 A0 00 00 00 55 89 E5 53  ....... ....U.åS
00123020 56 57 50 52 68 F8 A6 C5 70 68 00 23 8F 0B 8D 74  VWPRhø¦Åph.#...t
00123030 24 04 51 52 64 8B 1D 3C 0E 00 00 83 FB 00 74 70  $.QRd..<....û.tp
00123040 C6 43 08 01 83 3D 48 20 38 71 00 75 5C 8B 44 24  ÆC...=H 8q.u\.D$
00123050 E0 8B 7B 0C 89 7E 04 89 73 0C 68 10 5D F0 70 64  à.{..~..s.h.]ðpd
00123060 A1 00 00 00 00 50 64 89 25 00 00 00 00 8B 4E 08  ¡....Pd.%.....N.
00123070 51 E8 8A 6E CE 70 8B 46 08 8D 40 16 8B 0C 24 64  Qè.nÎp.F..@...$d
00123080 89 0D 00 00 00 00 83 C4 08 89 7B 0C C6 43 08 00  .......Ä..{.ÆC..
00123090 F6 43 04 5F 75 0C 5A 59 83 C4 10 5F 5E 5B 5D FF  öC._u.ZY.Ä._^[]ÿ
001230A0 E0 C3 E8 F1 BE B2 70 EB ED E8 FE BE B2 70 EB 9D  àÃèñ¾²pëíèþ¾²pë.
001230B0 E8 7B A6 E0 70 89 C3 EB 87 00 00 00 01 00 00 00  è{¦àp.Ãë........
```

```
003AF7AC  FFFFFFFF
003AF7B0  00000000
003AF7B4  00010000
003AF7B8  00202000
003AF7BC  00000004
003AF7C0  003AF7EC  &"Oø:"
003AF7C4  70C632DE  return to clr.70C632DE from ???
003AF7C8  00000000
003AF7CC  00010000
003AF7D0  00202000
003AF7D4  00000004
003AF7D8  00010000
003AF7DC  01000000
003AF7E0  006F40A0
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Default

Here we got the return address in eax, but here we are not able to dump it.


remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace

```
     7583F002   8BFF          mov edi,edi                                    VirtualAlloc
     7583F004   55            push ebp
     7583F005   8BEC          mov ebp,esp
     7583F007   FF75 14       push dword ptr ss:[ebp+14]
     7583F00A   FF75 10       push dword ptr ss:[ebp+10]
     7583F00D   FF75 0C       push dword ptr ss:[ebp+C]
     7583F010   FF75 08       push dword ptr ss:[ebp+8]
     7583F013   6A FF         push FFFFFFFF
     7583F015   E8 4BFFFFFF   call <kernelbase.VirtualAllocEx>
EIP  7583F01A   5D            pop ebp
     7583F01B   C2 1000       ret 10
     7583F01E   CC            int3
     7583F01F   CC            int3
     7583F020   CC            int3
     7583F021   CC            int3
     7583F022   CC            int3
     7583F023   8BFF          mov edi,edi                                    GetLogicalProcessorInformation
     7583F025   55            push ebp
     7583F026   8BEC          mov ebp,esp
     7583F028   56            push esi
     7583F029   8B75 0C       mov esi,dword ptr ss:[ebp+C]
     7583F02C   85F6          test esi,esi
     7583F02E   75 0C         jne kernelbase.7583F03C
     7583F030   6A 57         push 57
     7583F032   FF15 44108375 call dword ptr ds:[<&RtlRestoreLastWin3
     7583F038   33C0          xor eax,eax
     7583F03A   EB 37         jmp kernelbase.7583F073
     7583F03C   8D45 0C       lea eax,dword ptr ss:[ebp+C]
     7583F03F   50            push eax
     7583F040   FF15 D0118375 call dword ptr ds:[<&RtlGetCurrentProce
     7583F046   56            push esi

ebp=003AF7C0 &"ü÷:"

.text:7583F01A kernelbase.dll:$F01A #E41A
```

```
Hide FPU

EAX     0
EBX     0
ECX     9
EDX     0
EBP     0
ESP     0
ESI     7
EDI     0

EIP     7

EFLAGS
ZF 1  P
OF 0  S
CF 0  T

LastErr
LastSta

GS 002B
ES 002B
CS 0023

Default (stdcall)  5
1: [esp+4] 70C632DE "_[‹å]Å\
2: [esp+8] 00000000
3: [esp+C] 00010000
4: [esp+10] 00202000
5: [esp+14] 00000004
```

```
Address  Hex                                              ASCII
774E1000 CC A1 03 00 1D 1E 07 00 31 2A 03 00 F5 7F 03 00  Ì¡......1*..õ...
774E1010 5A AA 05 00 C7 29 0C 00 A8 2B 0C 00 27 4C 0C 00  Zª..Ç)..¨+..'L..
774E1020 16 18 0C 00 9D 18 0C 00 63 BD 0B 00 BA FA 09 00  ........c½..ºú..
774E1030 E9 B3 05 00 15 AD 03 00 F4 AA 03 00 13 5D 06 00  é³......ôª...]..
774E1040 CF 23 04 00 46 4C 0C 00 CD DB 05 00 10 89 05 00  Ï#..FL..ÍÛ......
774E1050 85 F4 09 00 FF 13 05 00 CE CD 05 00 AC 20 02 00  .ô..ÿ...ÎÍ..¬ ..
774E1060 07 0A 0C 00 D1 7D 03 00 02 88 03 00 85 20 05 00  ....Ñ}....... ..
774E1070 CC 5C 06 00 FD 69 05 00 96 60 07 00 49 98 0B 00  Ì\..ýi...`..I...
774E1080 14 B0 04 00 3F A0 04 00 3F 2A 0B 00 6D 1B 0C 00  .°..? ..?*..m...
774E1090 E5 A6 0B 00 08 21 07 00 58 8B 0B 00 7C F9 04 00  å¦...!..X...|ù..
774E10A0 96 B6 0B 00 3F 00 0A 00 F5 26 07 00 71 7C 06 00  .¶..?...õ&..q|..
774E10B0 B3 C5 0B 00 3A 87 03 00 72 EE 02 00 E2 5F 0C 00  ³Å..:...rî..â_..
```

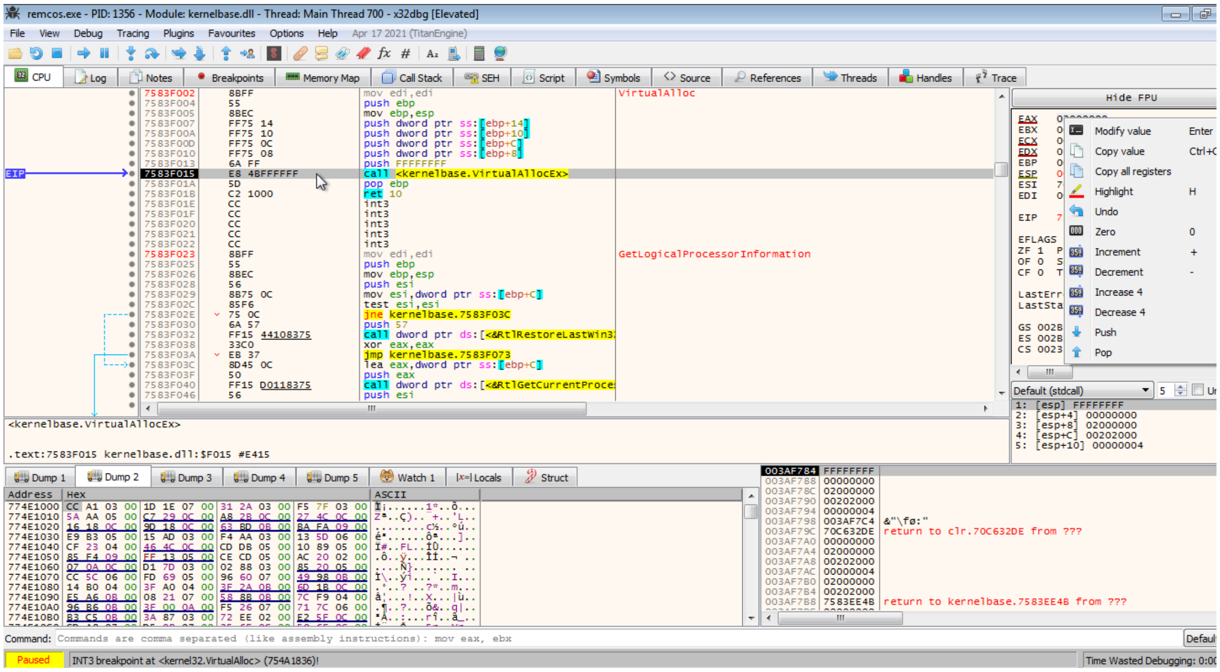
```
003AF7C0  003AF7EC  &"Oø:"
003AF7C4  70C632DE  return to clr.70C632DE from ???
003AF7C8  00000000
003AF7CC  00010000
003AF7D0  00202000
003AF7D4  00000004
003AF7D8  00010000
003AF7DC  01000000
003AF7E0  006F40A0
003AF7E4  00000000
003AF7E8  00010000
003AF7EC  003AF7FC  &"hø:"
003AF7F0  70C63304  return to clr.70C63304 from clr.70C632AA
003AF7F4  00202000
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused INT3 breakpoint at <kernel32.VirtualAlloc> (754A1836)!

Time Wasted Debugging

Here we again hit the brekapoint at VirtualAlloc ,here just step over it and then after the call ,view the returned value in eax.



remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Modify value Enter
Copy value Ctrl+C
Copy all registers
Highlight H
Undo
Zero 0
Increment +
Decrement -
Increase 4
Decrease 4
Push
Pop
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

```
      7583F002   8BFF           mov edi,edi                                  VirtualAlloc
      7583F004   55             push ebp
      7583F005   8BEC           mov ebp,esp
      7583F007   FF75 14        push dword ptr ss:[ebp+14]
      7583F00A   FF75 10        push dword ptr ss:[ebp+10]
      7583F00D   FF75 0C        push dword ptr ss:[ebp+C]
      7583F010   FF75 08        push dword ptr ss:[ebp+8]
      7583F013   6A FF          push FFFFFFFF
EIP → 7583F015   E8 4BFFFFFF    call <kernelbase.VirtualAllocEx>
      7583F01A   5D             pop ebp
      7583F01B   C2 1000        ret 10
      7583F01E   CC             int3
      7583F01F   CC             int3
      7583F020   CC             int3
      7583F021   CC             int3
      7583F022   CC             int3
      7583F023   8BFF           mov edi,edi                                  GetLogicalProcessorInformation
      7583F025   55             push ebp
      7583F026   8BEC           mov ebp,esp
      7583F028   56             push esi
      7583F029   8B75 0C        mov esi,dword ptr ss:[ebp+C]
      7583F02C   85F6           test esi,esi
      7583F02E   75 0C          jne kernelbase.7583F03C
      7583F030   6A 57          push 57
      7583F032   FF15 44108375  call dword ptr ds:[<&RtlRestoreLastWin3
      7583F038   33C0           xor eax,eax
      7583F03A   EB 37          jmp kernelbase.7583F073
      7583F03C   8D45 0C        lea eax,dword ptr ss:[ebp+C]
      7583F03F   50             push eax
      7583F040   FF15 D0118375  call dword ptr ds:[<&RtlGetCurrentProce
      7583F046   56             push esi

<kernelbase.VirtualAllocEx>

.text:7583F015 kernelbase.dll:$F015 #E415
```

```
EAX  0
EBX  0
ECX  0
EDX  0
EBP  0
ESP  0
ESI  7
EDI  0

EIP  7

EFLAGS
ZF 1  P
OF 0  S
CF 0  T

LastErr
LastSta

GS 002B
ES 002B
CS 0023
```

```
Default (stdcall)   5
1: [esp] FFFFFFFF
2: [esp+4] 00000000
3: [esp+8] 02000000
4: [esp+C] 00202000
5: [esp+10] 00000004
```

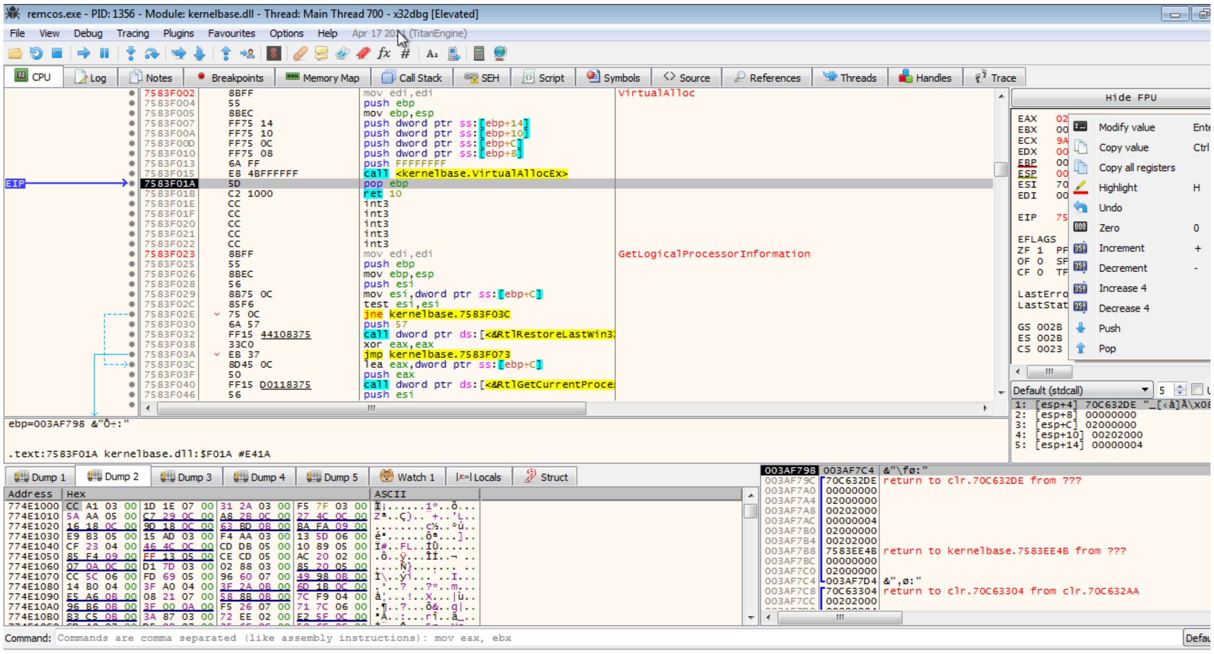
```
Address   Hex                                              ASCII
774E1000  CC A1 03 00 1D 1E 07 00 31 2A 03 00 F5 7F 03 00  Ì¡......1*..õ...
774E1010  5A AA 05 00 C7 29 0C 00 A8 2B 0C 00 27 4C 0C 00  Zª..Ç)..¨+..'L..
774E1020  16 18 0C 00 9D 18 0C 00 63 BD 0B 00 BA FA 09 00  ........c½..ºú..
774E1030  E9 B3 05 00 15 AD 03 00 F4 AA 03 00 13 5D 06 00  é³......ôª...]..
774E1040  CF 23 04 00 46 4C 0C 00 CD DB 05 00 10 89 05 00  Ï#..FL..ÍÛ......
774E1050  85 F4 09 00 FF 13 05 00 CE CD 05 00 AC 20 02 00  .ô..ÿ...ÎÍ..¬ ..
774E1060  07 0A 0C 00 D1 7D 03 00 02 88 03 00 85 20 05 00  ....Ñ}....... ..
774E1070  CC 5C 06 00 FD 69 05 00 96 60 07 00 49 98 0B 00  Ì\..ýi...`..I...
774E1080  14 B0 04 00 3F A0 04 00 3F 2A 0B 00 6D 1B 0C 00  .°..? ..?*..m...
774E1090  E5 A6 0B 00 08 21 07 00 58 8B 0B 00 7C F9 04 00  å¦...!..X...|ù..
774E10A0  96 B6 0B 00 3F 00 0A 00 F5 26 07 00 71 7C 06 00  .¶..?...õ&..q|..
774E10B0  B3 C5 0B 00 3A 87 03 00 72 EE 02 00 E2 5F 0C 00  ³Å..:...rî..â_..
```

```
003AF784  FFFFFFFF
003AF788  00000000
003AF78C  02000000
003AF790  00202000
003AF794  00000004
003AF798  003AF7C4  &"\fø:"
003AF79C  70C632DE  return to clr.70C632DE from ???
003AF7A0  00000000
003AF7A4  02000000
003AF7A8  00202000
003AF7AC  00000004
003AF7B0  02000000
003AF7B4  00202000
003AF7B8  7583EE4B  return to kernelbase.7583EE4B from ???
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused   INT3 breakpoint at <kernel32.VirtualAlloc> (754A1836)!   Time Wasted Debugging: 0:0

Here the address is returned in eax , but here also we are not able to dump it so press f9.



remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Modify value Ente
Copy value Ctrl
Copy all registers
Highlight H
Undo
Zero 0
Increment +
Decrement -
Increase 4
Decrease 4
Push
Pop
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

```
      7583F002   8BFF           mov edi,edi                                  VirtualAlloc
      7583F004   55             push ebp
      7583F005   8BEC           mov ebp,esp
      7583F007   FF75 14        push dword ptr ss:[ebp+14]
      7583F00A   FF75 10        push dword ptr ss:[ebp+10]
      7583F00D   FF75 0C        push dword ptr ss:[ebp+C]
      7583F010   FF75 08        push dword ptr ss:[ebp+8]
      7583F013   6A FF          push FFFFFFFF
      7583F015   E8 4BFFFFFF    call <kernelbase.VirtualAllocEx>
EIP → 7583F01A   5D             pop ebp
      7583F01B   C2 1000        ret 10
      7583F01E   CC             int3
      7583F01F   CC             int3
      7583F020   CC             int3
      7583F021   CC             int3
      7583F022   CC             int3
      7583F023   8BFF           mov edi,edi                                  GetLogicalProcessorInformation
      7583F025   55             push ebp
      7583F026   8BEC           mov ebp,esp
      7583F028   56             push esi
      7583F029   8B75 0C        mov esi,dword ptr ss:[ebp+C]
      7583F02C   85F6           test esi,esi
      7583F02E   75 0C          jne kernelbase.7583F03C
      7583F030   6A 57          push 57
      7583F032   FF15 44108375  call dword ptr ds:[<&RtlRestoreLastWin3
      7583F038   33C0           xor eax,eax
      7583F03A   EB 37          jmp kernelbase.7583F073
      7583F03C   8D45 0C        lea eax,dword ptr ss:[ebp+C]
      7583F03F   50             push eax
      7583F040   FF15 D0118375  call dword ptr ds:[<&RtlGetCurrentProce
      7583F046   56             push esi

ebp=003AF798 &"Õ÷:"

.text:7583F01A kernelbase.dll:$F01A #E41A
```

```
EAX  02
EBX  00
ECX  9A
EDX  00
EBP  00
ESP  00
ESI  70
EDI  00

EIP  75

EFLAGS
ZF 1  PF
OF 0  SF
CF 0  TF

LastErro
LastStat

GS 002B
ES 002B
CS 0023
```

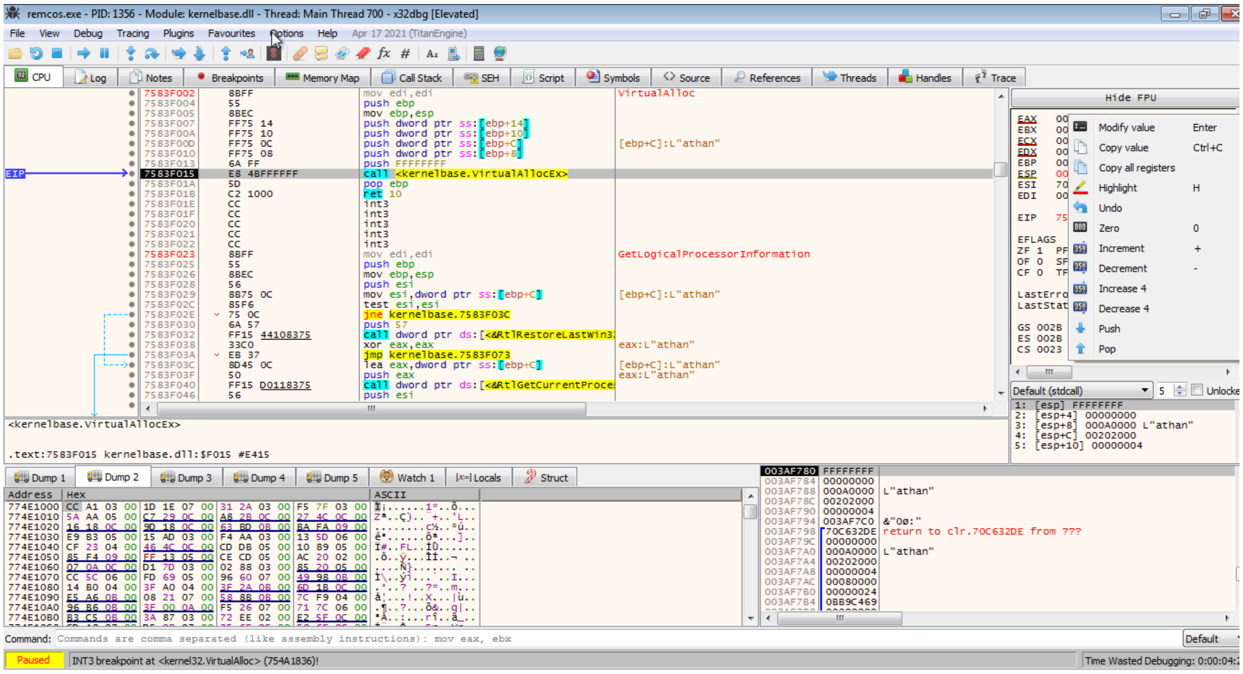
```
Default (stdcall)   5
1: [esp+4] 70C632DE "_[‹å]Â\x08
2: [esp+8] 00000000
3: [esp+C] 02000000
4: [esp+10] 00202000
5: [esp+14] 00000004
```

```
Address   Hex                                              ASCII
774E1000  CC A1 03 00 1D 1E 07 00 31 2A 03 00 F5 7F 03 00  Ì¡......1*..õ...
774E1010  5A AA 05 00 C7 29 0C 00 A8 2B 0C 00 27 4C 0C 00  Zª..Ç)..¨+..'L..
774E1020  16 18 0C 00 9D 18 0C 00 63 BD 0B 00 BA FA 09 00  ........c½..ºú..
774E1030  E9 B3 05 00 15 AD 03 00 F4 AA 03 00 13 5D 06 00  é³......ôª...]..
774E1040  CF 23 04 00 46 4C 0C 00 CD DB 05 00 10 89 05 00  Ï#..FL..ÍÛ......
774E1050  85 F4 09 00 FF 13 05 00 CE CD 05 00 AC 20 02 00  .ô..ÿ...ÎÍ..¬ ..
774E1060  07 0A 0C 00 D1 7D 03 00 02 88 03 00 85 20 05 00  ....Ñ}....... ..
774E1070  CC 5C 06 00 FD 69 05 00 96 60 07 00 49 98 0B 00  Ì\..ýi...`..I...
774E1080  14 B0 04 00 3F A0 04 00 3F 2A 0B 00 6D 1B 0C 00  .°..? ..?*..m...
774E1090  E5 A6 0B 00 08 21 07 00 58 8B 0B 00 7C F9 04 00  å¦...!..X...|ù..
774E10A0  96 B6 0B 00 3F 00 0A 00 F5 26 07 00 71 7C 06 00  .¶..?...õ&..q|..
774E10B0  B3 C5 0B 00 3A 87 03 00 72 EE 02 00 E2 5F 0C 00  ³Å..:...rî..â_..
```

```
003AF798  003AF7C4  &"\fø:"
003AF79C  70C632DE  return to clr.70C632DE from ???
003AF7A0  00000000
003AF7A4  02000000
003AF7A8  00202000
003AF7AC  00000004
003AF7B0  02000000
003AF7B4  00202000
003AF7B8  7583EE4B  return to kernelbase.7583EE4B from ???
003AF7BC  00000000
003AF7C0  02000000
003AF7C4  003AF7D4  &",ø:"
003AF7C8  70C63304  return to clr.70C63304 from clr.70C632AA
003AF7CC  00202000
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Here we got another breakpoint at VirtualAlloc but here also we are not able to dump it .



remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]

```
     7583F002  8BFF            mov edi,edi                           VirtualAlloc
     7583F004  55              push ebp
     7583F005  8BEC            mov ebp,esp
     7583F007  FF75 14         push dword ptr ss:[ebp+14]
     7583F00A  FF75 10         push dword ptr ss:[ebp+10]
     7583F00D  FF75 0C         push dword ptr ss:[ebp+C]             [ebp+C]:L"athan"
     7583F010  FF75 08         push dword ptr ss:[ebp+8]
     7583F013  6A FF           push FFFFFFFF
EIP  7583F015  E8 4BFFFFFF     call <kernelbase.VirtualAllocEx>
     7583F01A  5D              pop ebp
     7583F01B  C2 1000         ret 10
     7583F01E  CC              int3
     7583F01F  CC              int3
     7583F020  CC              int3
     7583F021  CC              int3
     7583F022  CC              int3
     7583F023  8BFF            mov edi,edi                           GetLogicalProcessorInformation
     7583F025  55              push ebp
     7583F026  8BEC            mov ebp,esp
     7583F028  56              push esi
     7583F029  8B75 0C         mov esi,dword ptr ss:[ebp+C]          [ebp+C]:L"athan"
     7583F02C  85F6            test esi,esi
     7583F02E  75 0C           jne kernelbase.7583F03C
     7583F030  6A 57           push 57
     7583F032  FF15 44108375   call dword ptr ds:[<&RtlRestoreLastWin3
     7583F038  33C0            xor eax,eax                           eax:L"athan"
     7583F03A  EB 37           jmp kernelbase.7583F073
     7583F03C  8D45 0C         lea eax,dword ptr ss:[ebp+C]          [ebp+C]:L"athan"
     7583F03F  50              push eax                              eax:L"athan"
     7583F040  FF15 D0118375   call dword ptr ds:[<&RtlGetCurrentProce
     7583F046  56              push esi

<kernelbase.VirtualAllocEx>

.text:7583F015 kernelbase.dll:$F015 #E415
```

```
EAX   00
EBX   00
ECX   00
EDX   00
EBP   00
ESP   00
ESI   70
EDI   00

EIP   75

EFLAGS
ZF 1  PF
OF 0  SF
CF 0  TF

LastErro
LastStat

GS 002B
ES 002B
CS 0023
```

Default (stdcall) 5 □ Unlocke

```
1:  [esp] FFFFFFFF
2:  [esp+4] 00000000
3:  [esp+8] 000A0000 L"athan"
4:  [esp+C] 00202000
5:  [esp+10] 00000004
```

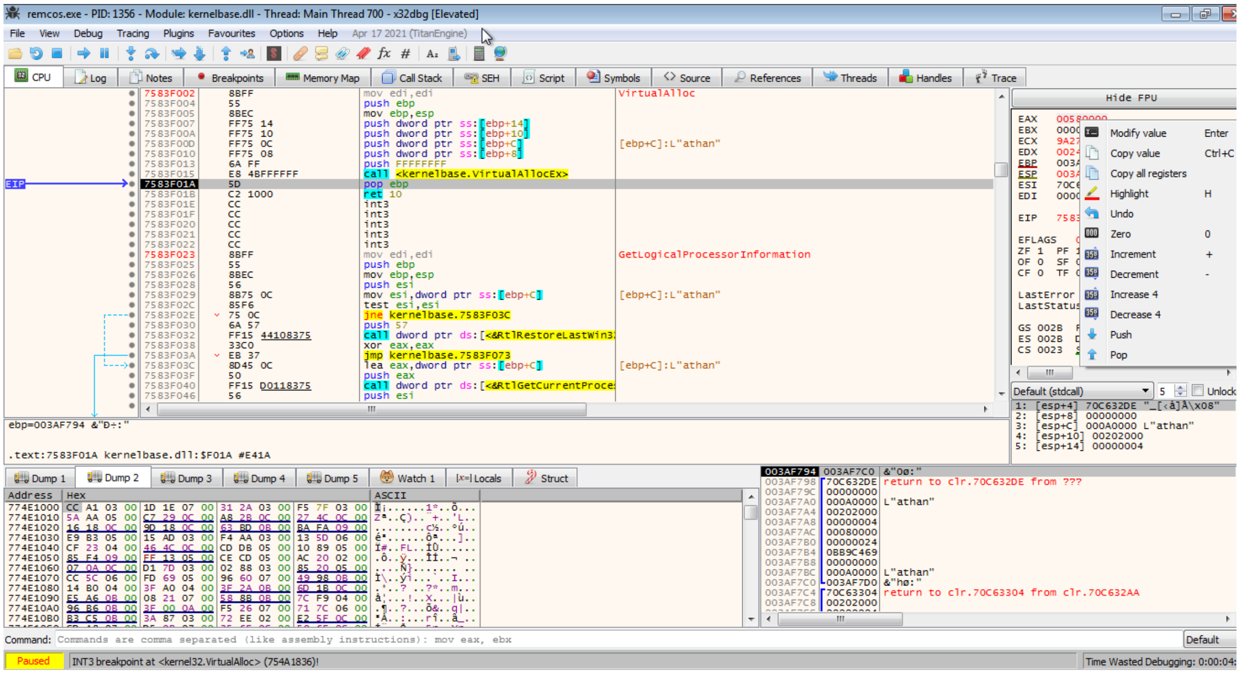
```
Address   Hex                                              ASCII
774E1000  CC A1 03 00 1D 1E 07 00 31 2A 03 00 F5 7F 03 00  Ì¡......1*..õ...
774E1010  5A AA 05 00 C7 29 0C 00 A8 2B 0C 00 27 4C 0C 00  Zª..Ç)..¨+..'L..
774E1020  16 18 0C 00 9D 18 0C 00 63 BD 0B 00 BA FA 09 00  ........c½..ºú..
774E1030  E9 B3 05 00 15 AD 03 00 F4 AA 03 00 13 5D 06 00  é³......ôª...]..
774E1040  CF 23 04 00 46 4C 0C 00 CD DB 05 00 10 89 05 00  Ï#..FL..ÍÛ......
774E1050  85 F4 09 00 FF 13 05 00 CE CD 05 00 AC 20 02 00  .ô..ÿ...ÎÍ..¬ ..
774E1060  07 0A 0C 00 D1 7D 03 00 02 88 03 00 85 20 05 00  ....Ñ}....... ..
774E1070  CC 5C 06 00 FD 69 05 00 96 60 07 00 49 98 0B 00  Ì\..ýi...`..I...
774E1080  14 B0 04 00 3F A0 04 00 3F 2A 0B 00 6D 1B 0C 00  .°..? ..?*..m...
774E1090  E5 A6 0B 00 08 21 07 00 58 8B 0B 00 7C F9 04 00  å¦...!..X...|ù..
774E10A0  96 B6 0B 00 3F 00 0A 00 F5 26 07 00 71 7C 06 00  .¶..?...õ&..q|..
774E10B0  B3 C5 0B 00 3A 87 03 00 72 EE 02 00 E2 5F 0C 00  ³Å..:...rî..â_..
```

```
003AF780  FFFFFFFF
003AF784  00000000
003AF788  000A0000  L"athan"
003AF78C  00202000
003AF790  00000004
003AF794  003AF7C0  &"Oø:"
003AF798  70C632DE  return to clr.70C632DE from ???
003AF79C  00000000
003AF7A0  000A0000  L"athan"
003AF7A4  00202000
003AF7A8  00000004
003AF7AC  00080000
003AF7B0  00000024
003AF7B4  0BB9C469
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused INT3 breakpoint at <kernel32.VirtualAlloc> (754A1836)! Time Wasted Debugging: 0:00:04:2

Here we can see the return address by it is 580000.



remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]

```
     7583F002  8BFF            mov edi,edi                           VirtualAlloc
     7583F004  55              push ebp
     7583F005  8BEC            mov ebp,esp
     7583F007  FF75 14         push dword ptr ss:[ebp+14]
     7583F00A  FF75 10         push dword ptr ss:[ebp+10]
     7583F00D  FF75 0C         push dword ptr ss:[ebp+C]             [ebp+C]:L"athan"
     7583F010  FF75 08         push dword ptr ss:[ebp+8]
     7583F013  6A FF           push FFFFFFFF
     7583F015  E8 4BFFFFFF     call <kernelbase.VirtualAllocEx>
EIP  7583F01A  5D              pop ebp
     7583F01B  C2 1000         ret 10
     7583F01E  CC              int3
     7583F01F  CC              int3
     7583F020  CC              int3
     7583F021  CC              int3
     7583F022  CC              int3
     7583F023  8BFF            mov edi,edi                           GetLogicalProcessorInformation
     7583F025  55              push ebp
     7583F026  8BEC            mov ebp,esp
     7583F028  56              push esi
     7583F029  8B75 0C         mov esi,dword ptr ss:[ebp+C]          [ebp+C]:L"athan"
     7583F02C  85F6            test esi,esi
     7583F02E  75 0C           jne kernelbase.7583F03C
     7583F030  6A 57           push 57
     7583F032  FF15 44108375   call dword ptr ds:[<&RtlRestoreLastWin3
     7583F038  33C0            xor eax,eax
     7583F03A  EB 37           jmp kernelbase.7583F073
     7583F03C  8D45 0C         lea eax,dword ptr ss:[ebp+C]          [ebp+C]:L"athan"
     7583F03F  50              push eax
     7583F040  FF15 D0118375   call dword ptr ds:[<&RtlGetCurrentProce
     7583F046  56              push esi

ebp=003AF794 &"Ð÷:"

.text:7583F01A kernelbase.dll:$F01A #E41A
```

```
EAX   00580000
EBX   0000
ECX   9A27
EDX   0024
EBP   003A
ESP   003A
ESI   70C6
EDI   0000

EIP   7583

EFLAGS
ZF 1  PF 1
OF 0  SF 0
CF 0  TF 0

LastError
LastStatus

GS 002B
ES 002B
CS 0023
```

Default (stdcall) 5 □ Unlock

```
1:  [esp+4] 70C632DE "_[‹å]Å\x08"
2:  [esp+8] 00000000
3:  [esp+C] 000A0000 L"athan"
4:  [esp+10] 00202000
5:  [esp+14] 00000004
```

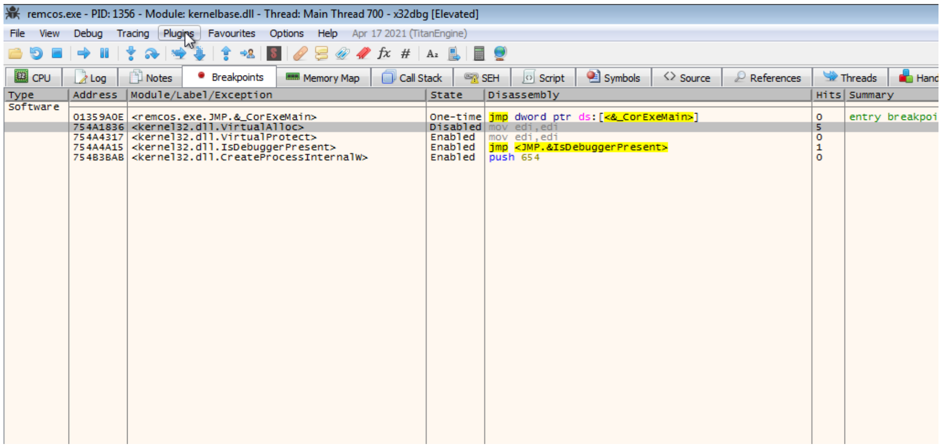
```
Address   Hex                                              ASCII
774E1000  CC A1 03 00 1D 1E 07 00 31 2A 03 00 F5 7F 03 00  Ì¡......1*..õ...
774E1010  5A AA 05 00 C7 29 0C 00 A8 2B 0C 00 27 4C 0C 00  Zª..Ç)..¨+..'L..
774E1020  16 18 0C 00 9D 18 0C 00 63 BD 0B 00 BA FA 09 00  ........c½..ºú..
774E1030  E9 B3 05 00 15 AD 03 00 F4 AA 03 00 13 5D 06 00  é³......ôª...]..
774E1040  CF 23 04 00 46 4C 0C 00 CD DB 05 00 10 89 05 00  Ï#..FL..ÍÛ......
774E1050  85 F4 09 00 FF 13 05 00 CE CD 05 00 AC 20 02 00  .ô..ÿ...ÎÍ..¬ ..
774E1060  07 0A 0C 00 D1 7D 03 00 02 88 03 00 85 20 05 00  ....Ñ}....... ..
774E1070  CC 5C 06 00 FD 69 05 00 96 60 07 00 49 98 0B 00  Ì\..ýi...`..I...
774E1080  14 B0 04 00 3F A0 04 00 3F 2A 0B 00 6D 1B 0C 00  .°..? ..?*..m...
774E1090  E5 A6 0B 00 08 21 07 00 58 8B 0B 00 7C F9 04 00  å¦...!..X...|ù..
774E10A0  96 B6 0B 00 3F 00 0A 00 F5 26 07 00 71 7C 06 00  .¶..?...õ&..q|..
774E10B0  B3 C5 0B 00 3A 87 03 00 72 EE 02 00 E2 5F 0C 00  ³Å..:...rî..â_..
```

```
003AF794  003AF7C0  &"Oø:"
003AF798  70C632DE  return to clr.70C632DE from ???
003AF79C  00000000
003AF7A0  000A0000  L"athan"
003AF7A4  00202000
003AF7A8  00000004
003AF7AC  00080000
003AF7B0  00000024
003AF7B4  0BB9C469
003AF7B8  00000000
003AF7BC  000A0000  L"athan"
003AF7C0  003AF7D0  &"hø:"
003AF7C4  70C63304  return to clr.70C63304 from clr.70C632AA
003AF7C8  00202000
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused INT3 breakpoint at <kernel32.VirtualAlloc> (754A1836)! Time Wasted Debugging: 0:00:04:

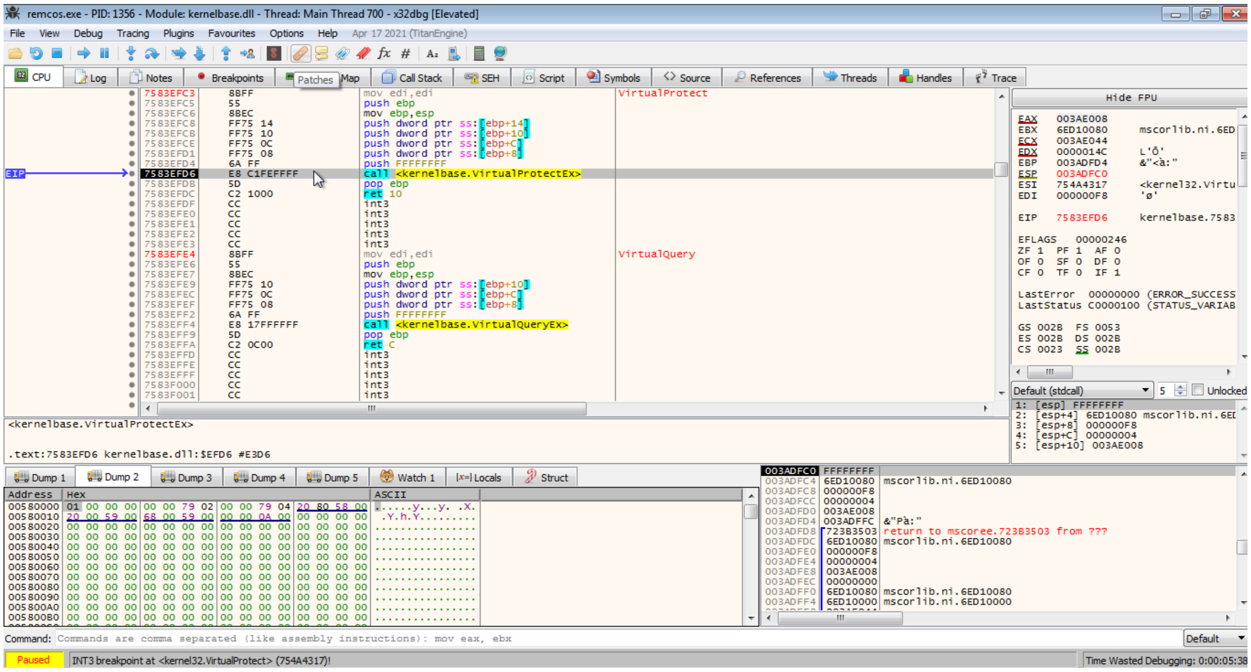
This is the total count of the breakpoints hit till now and now here we disable the VirtualAlloc.



remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Hand

```
Type      Address   Module/Label/Exception                 State     Disassembly                        Hits Summary
Software
          01359A0E  <remcos.exe.JMP.&_CorExeMain>          One-time  jmp dword ptr ds:[<&_CorExeMain>]  0    entry breakpoi
          754A1836  <kernel32.dll.VirtualAlloc>            Disabled  mov edi,edi                        5
          754A4317  <kernel32.dll.VirtualProtect>          Enabled   mov edi,edi                        0
          754A4A15  <kernel32.dll.IsDebuggerPresent>       Enabled   jmp <JMP.&IsDebuggerPresent>       1
          754B3BAB  <kernel32.dll.CreateProcessInternalW>  Enabled   push 654                           0
```

Now here we hit the breakpoint at VirtualProtect just step over it ,here we look at the second parameter here it is refering to the mscorlib library which is library for dotnet framework so we don't need to follow it in memory pressf9.



remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Patches Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Default (stdcall) 5 Unlocked
Default

```
      7583EFC3   8BFF          mov edi,edi                         VirtualProtect
      7583EFC5   55            push ebp
      7583EFC6   8BEC          mov ebp,esp
      7583EFC8   FF75 14       push dword ptr ss:[ebp+14]
      7583EFCB   FF75 10       push dword ptr ss:[ebp+10]
      7583EFCE   FF75 0C       push dword ptr ss:[ebp+C]
      7583EFD1   FF75 08       push dword ptr ss:[ebp+8]
      7583EFD4   6A FF         push FFFFFFFF
EIP → 7583EFD6   E8 C1FEFFFF   call <kernelbase.VirtualProtectEx>
      7583EFDB   5D            pop ebp
      7583EFDC   C2 1000       ret 10
      7583EFDF   CC            int3
      7583EFE0   CC            int3
      7583EFE1   CC            int3
      7583EFE2   CC            int3
      7583EFE3   CC            int3
      7583EFE4   8BFF          mov edi,edi                         VirtualQuery
      7583EFE6   55            push ebp
      7583EFE7   8BEC          mov ebp,esp
      7583EFE9   FF75 10       push dword ptr ss:[ebp+10]
      7583EFEC   FF75 0C       push dword ptr ss:[ebp+C]
      7583EFEF   FF75 08       push dword ptr ss:[ebp+8]
      7583EFF2   6A FF         push FFFFFFFF
      7583EFF4   E8 17FFFFFF   call <kernelbase.VirtualQueryEx>
      7583EFF9   5D            pop ebp
      7583EFFA   C2 0C00       ret C
      7583EFFD   CC            int3
      7583EFFE   CC            int3
      7583EFFF   CC            int3
      7583F000   CC            int3
      7583F001   CC            int3

<kernelbase.VirtualProtectEx>

.text:7583EFD6 kernelbase.dll:$EFD6 #E3D6
```

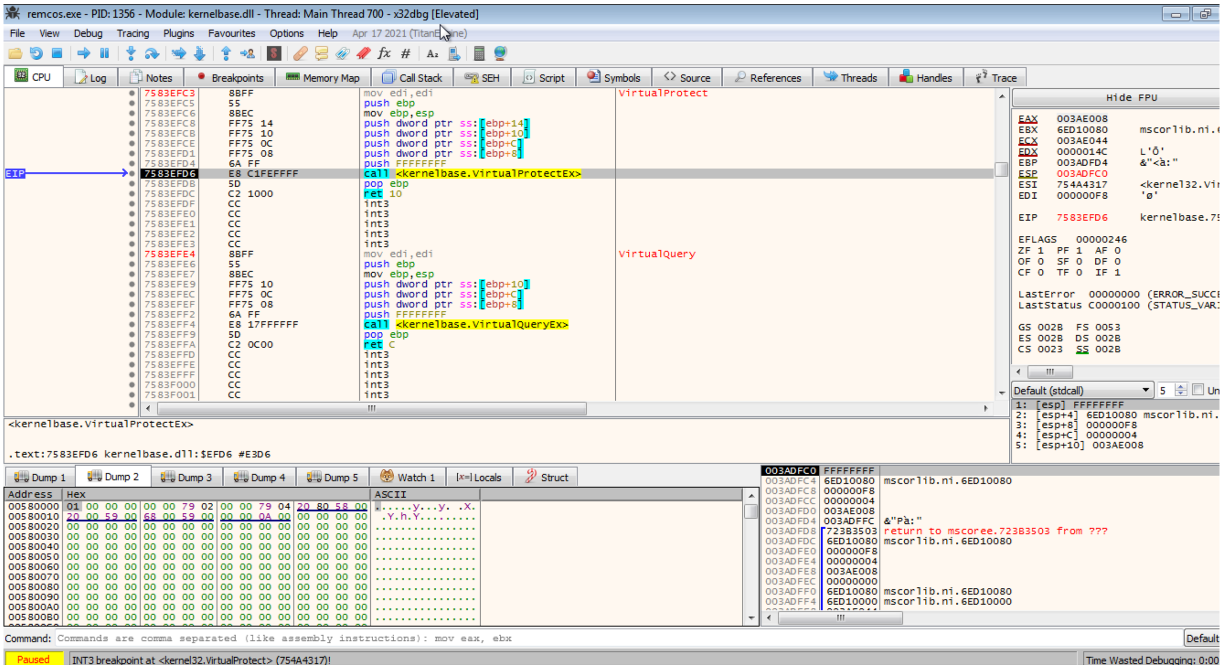
```
EAX   003AE008
EBX   6ED10080   mscorlib.ni.6ED
ECX   003AE044
EDX   0000014C   L'Ō'
EBP   003ADFD4   &"<à:"
ESP   003ADFC0
ESI   754A4317   <kernel32.Virtu
EDI   000000F8   'ø'

EIP   7583EFD6   kernelbase.7583

EFLAGS   00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError   00000000 (ERROR_SUCCESS
LastStatus  C0000100 (STATUS_VARIAB

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

1:  [esp] FFFFFFFF
2:  [esp+4] 6ED10080 mscorlib.ni.6ED
3:  [esp+8] 000000F8
4:  [esp+C] 00000004
5:  [esp+10] 003AE008
```

```
Address   Hex                                              ASCII
00580000  01 00 00 00 00 00 79 02 00 00 79 04 20 80 58 00  ......y...y. .X.
00580010  20 00 59 00 68 00 59 00 00 00 0A 00 00 00 00 00   .Y.h.Y.........
00580020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
003ADFC0  FFFFFFFF
003ADFC4  6ED10080  mscorlib.ni.6ED10080
003ADFC8  000000F8
003ADFCC  00000004
003ADFD0  003AE008
003ADFD4  003ADFFC  &"Pà:"
003ADFD8  723B3503  return to mscoree.723B3503 from ???
003ADFDC  6ED10080  mscorlib.ni.6ED10080
003ADFE0  000000F8
003ADFE4  00000004
003ADFE8  003AE008
003ADFEC  00000000
003ADFF0  6ED10080  mscorlib.ni.6ED10080
003ADFF4  6ED10000  mscorlib.ni.6ED10000
```

```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused   INT3 breakpoint at <kernel32.VirtualProtect> (754A4317)!     Time Wasted Debugging: 0:00:05:38
```

Here again we hit VirtualProtect just step over it ,here we look at the second parameter here it is refering to the mscorlib library which is library for dotnet framework so we don't need to follow it in memory pressf9.



remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]

```
7583EFC3   8BFF             mov edi,edi                                  VirtualProtect
7583EFC5   55               push ebp
7583EFC6   8BEC             mov ebp,esp
7583EFC8   FF75 14          push dword ptr ss:[ebp+14]
7583EFCB   FF75 10          push dword ptr ss:[ebp+10]
7583EFCE   FF75 0C          push dword ptr ss:[ebp+C]
7583EFD1   FF75 08          push dword ptr ss:[ebp+8]
7583EFD4   6A FF            push FFFFFFFF
EIP --> 7583EFD6   E8 C1FEFFFF      call <kernelbase.VirtualProtectEx>
7583EFDB   5D               pop ebp
7583EFDC   C2 1000          ret 10
7583EFDF   CC               int3
7583EFE0   CC               int3
7583EFE1   CC               int3
7583EFE2   CC               int3
7583EFE3   CC               int3
7583EFE4   8BFF             mov edi,edi                                  VirtualQuery
7583EFE6   55               push ebp
7583EFE7   8BEC             mov ebp,esp
7583EFE9   FF75 10          push dword ptr ss:[ebp+10]
7583EFEC   FF75 0C          push dword ptr ss:[ebp+C]
7583EFEF   FF75 08          push dword ptr ss:[ebp+8]
7583EFF2   6A FF            push FFFFFFFF
7583EFF4   E8 17FFFFFF      call <kernelbase.VirtualQueryEx>
7583EFF9   5D               pop ebp
7583EFFA   C2 0C00          ret C
7583EFFD   CC               int3
7583EFFE   CC               int3
7583EFFF   CC               int3
7583F000   CC               int3
7583F001   CC               int3

<kernelbase.VirtualProtectEx>

.text:7583EFD6 kernelbase.dll:$EFD6 #E3D6
```

```
EAX   003AE008
EBX   6ED10080     mscorlib.ni.
ECX   003AE044
EDX   0000014C     L'Ō'
EBP   003ADFD4     &"<à:"
ESP   003ADFC0
ESI   754A4317     <kernel32.Vi
EDI   000000F8     'ø'

EIP   7583EFD6     kernelbase.75

EFLAGS   00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCE
LastStatus C0000100 (STATUS_VARI

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B
```

Default (stdcall) 5

```
1: [esp] FFFFFFFF
2: [esp+4] 6ED10080 mscorlib.ni.
3: [esp+8] 000000F8
4: [esp+C] 00000004
5: [esp+10] 003AE008
```

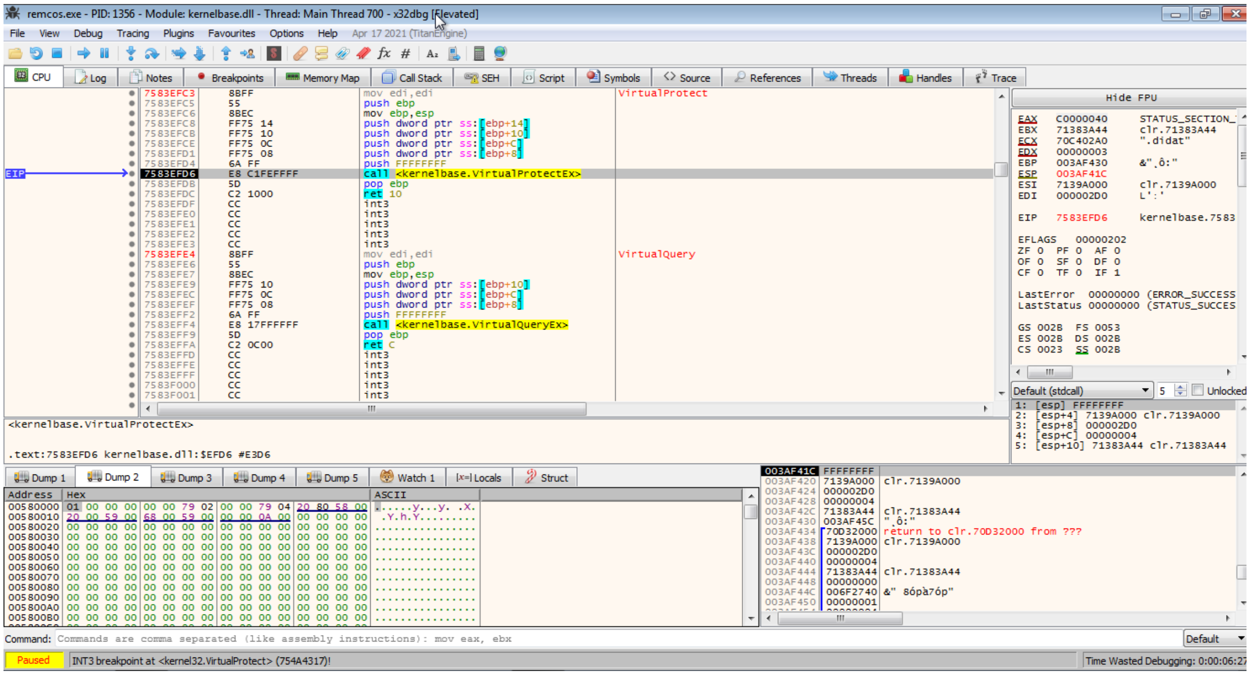
```
Address  Hex                                              ASCII
00580000 01 00 00 00 00 00 79 02 00 00 79 04 20 80 58 00 ......y...y. .X.
00580010 20 00 59 00 68 00 59 00 00 00 0A 00 00 00 00 00  .Y.h.Y.........
00580020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
005800A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
005800B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

```
003ADFC0 FFFFFFFF
003ADFC4 6ED10080 mscorlib.ni.6ED10080
003ADFC8 000000F8
003ADFCC 00000004
003ADFD0 003AE008
003ADFD4 003ADFFC &"Pà:"
003ADFD8 723B3503 return to mscoree.723B3503 from ???
003ADFDC 6ED10080 mscorlib.ni.6ED10080
003ADFE0 000000F8
003ADFE4 00000004
003ADFE8 003AE008
003ADFEC 00000000
003ADFF0 6ED10080 mscorlib.ni.6ED10080
003ADFF4 6ED10000 mscorlib.ni.6ED10000
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused   INT3 breakpoint at <kernel32.VirtualProtect> (754A4317)!   Time Wasted Debugging: 0:00

Here again we hit VirtualProtect just step over it ,here we look at the second parameter here it is refering to the which is part of common language runtime pressf9.



remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]

```
7583EFC3   8BFF             mov edi,edi                                  VirtualProtect
7583EFC5   55               push ebp
7583EFC6   8BEC             mov ebp,esp
7583EFC8   FF75 14          push dword ptr ss:[ebp+14]
7583EFCB   FF75 10          push dword ptr ss:[ebp+10]
7583EFCE   FF75 0C          push dword ptr ss:[ebp+C]
7583EFD1   FF75 08          push dword ptr ss:[ebp+8]
7583EFD4   6A FF            push FFFFFFFF
EIP --> 7583EFD6   E8 C1FEFFFF      call <kernelbase.VirtualProtectEx>
7583EFDB   5D               pop ebp
7583EFDC   C2 1000          ret 10
7583EFDF   CC               int3
7583EFE0   CC               int3
7583EFE1   CC               int3
7583EFE2   CC               int3
7583EFE3   CC               int3
7583EFE4   8BFF             mov edi,edi                                  VirtualQuery
7583EFE6   55               push ebp
7583EFE7   8BEC             mov ebp,esp
7583EFE9   FF75 10          push dword ptr ss:[ebp+10]
7583EFEC   FF75 0C          push dword ptr ss:[ebp+C]
7583EFEF   FF75 08          push dword ptr ss:[ebp+8]
7583EFF2   6A FF            push FFFFFFFF
7583EFF4   E8 17FFFFFF      call <kernelbase.VirtualQueryEx>
7583EFF9   5D               pop ebp
7583EFFA   C2 0C00          ret C
7583EFFD   CC               int3
7583EFFE   CC               int3
7583EFFF   CC               int3
7583F000   CC               int3
7583F001   CC               int3

<kernelbase.VirtualProtectEx>

.text:7583EFD6 kernelbase.dll:$EFD6 #E3D6
```

```
EAX   C0000040     STATUS_SECTION_
EBX   71383A44     clr.71383A44
ECX   70C402A0     ".didat"
EDX   00000003
EBP   003AF430     &"¸ô:"
ESP   003AF41C
ESI   7139A000     clr.7139A000
EDI   000002D0     L':'

EIP   7583EFD6     kernelbase.7583

EFLAGS   00000202
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS
LastStatus 00000000 (STATUS_SUCCES

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B
```

Default (stdcall) 5 ☐ Unlocked

```
1: [esp] FFFFFFFF
2: [esp+4] 7139A000 clr.7139A000
3: [esp+8] 000002D0
4: [esp+C] 00000004
5: [esp+10] 71383A44 clr.71383A44
```

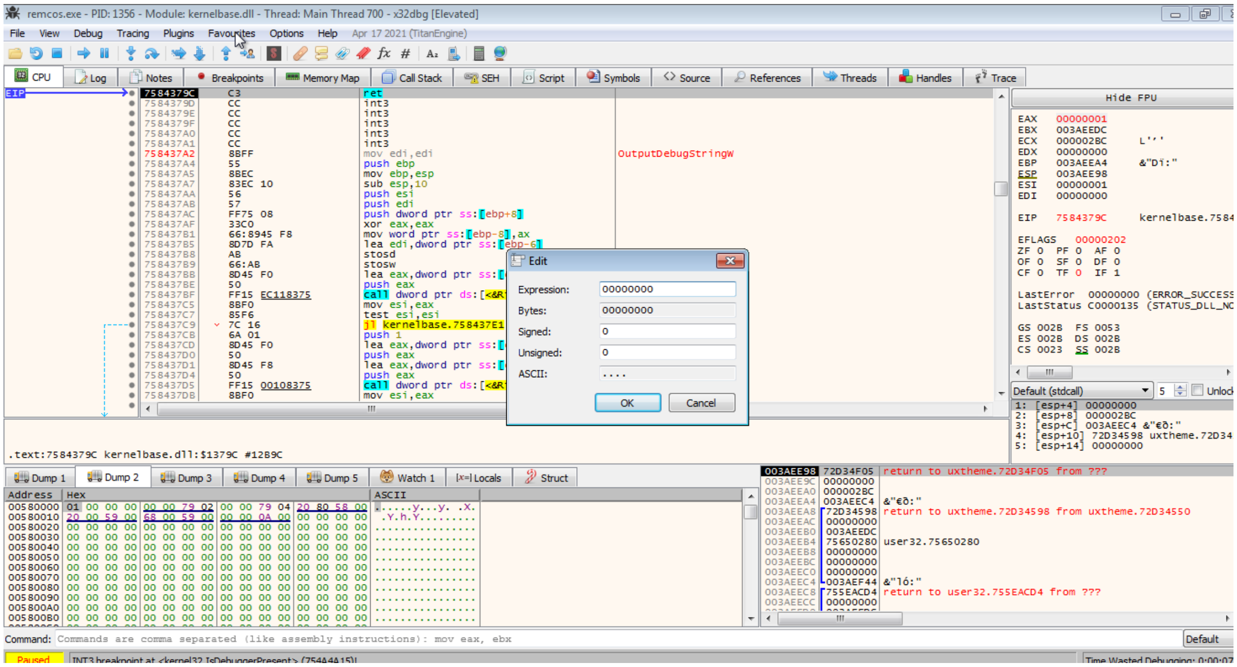
```
Address  Hex                                              ASCII
00580000 01 00 00 00 00 00 79 02 00 00 79 04 20 80 58 00 ......y...y. .X.
00580010 20 00 59 00 68 00 59 00 00 00 0A 00 00 00 00 00  .Y.h.Y.........
00580020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00580090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
005800A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
005800B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

```
003AF41C FFFFFFFF
003AF420 7139A000 clr.7139A000
003AF424 000002D0
003AF428 00000004
003AF42C 71383A44 clr.71383A44
003AF430 003AF45C "¸ô:"
003AF434 70D32000 return to clr.70D32000 from ???
003AF438 7139A000 clr.7139A000
003AF43C 000002D0
003AF440 00000004
003AF444 71383A44 clr.71383A44
003AF448 00000000
003AF44C 006F2740 &" 8óp à7óp"
003AF450 00000001
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused   INT3 breakpoint at <kernel32.VirtualProtect> (754A4317)!   Time Wasted Debugging: 0:00:06:27

Here we hit the breakpoint at IsDebuggerPresent here now we will make it execute till return and then modify the value return n eax form 1 to 0.



remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]

```
EIP →  7584379C   C3              ret
       7584379D   CC              int3
       7584379E   CC              int3
       7584379F   CC              int3
       758437A0   CC              int3
       758437A1   CC              int3
       758437A2   8BFF            mov edi,edi                          OutputDebugStringW
       758437A4   55              push ebp
       758437A5   8BEC            mov ebp,esp
       758437A7   83EC 10         sub esp,10
       758437AA   56              push esi
       758437AB   57              push edi
       758437AC   FF75 08         push dword ptr ss:[ebp+8]
       758437AF   33C0            xor eax,eax
       758437B1   66:8945 F8      mov word ptr ss:[ebp-8],ax
       758437B5   8D7D FA         lea edi,dword ptr ss:[ebp-6]
       758437B8   AB              stosd
       758437B9   66:AB           stosw
       758437BB   8D45 F0         lea eax,dword ptr ss:[
       758437BE   50              push eax
       758437BF   FF15 EC118375   call dword ptr ds:[<&R
       758437C5   8BF0            mov esi,eax
       758437C7   85F6            test esi,esi
       758437C9   7C 16           jl kernelbase.758437E1
       758437CB   6A 01           push 1
       758437CD   8D45 F0         lea eax,dword ptr ss:[
       758437D0   50              push eax
       758437D1   8D45 F8         lea eax,dword ptr ss:[
       758437D4   50              push eax
       758437D5   FF15 00108375   call dword ptr ds:[<&R
       758437DB   8BF0            mov esi,eax

.text:7584379C kernelbase.dll:$1379C #12B9C
```

```
Edit
Expression:  00000000
Bytes:       00000000
Signed:      0
Unsigned:    0
ASCII:       ....
```

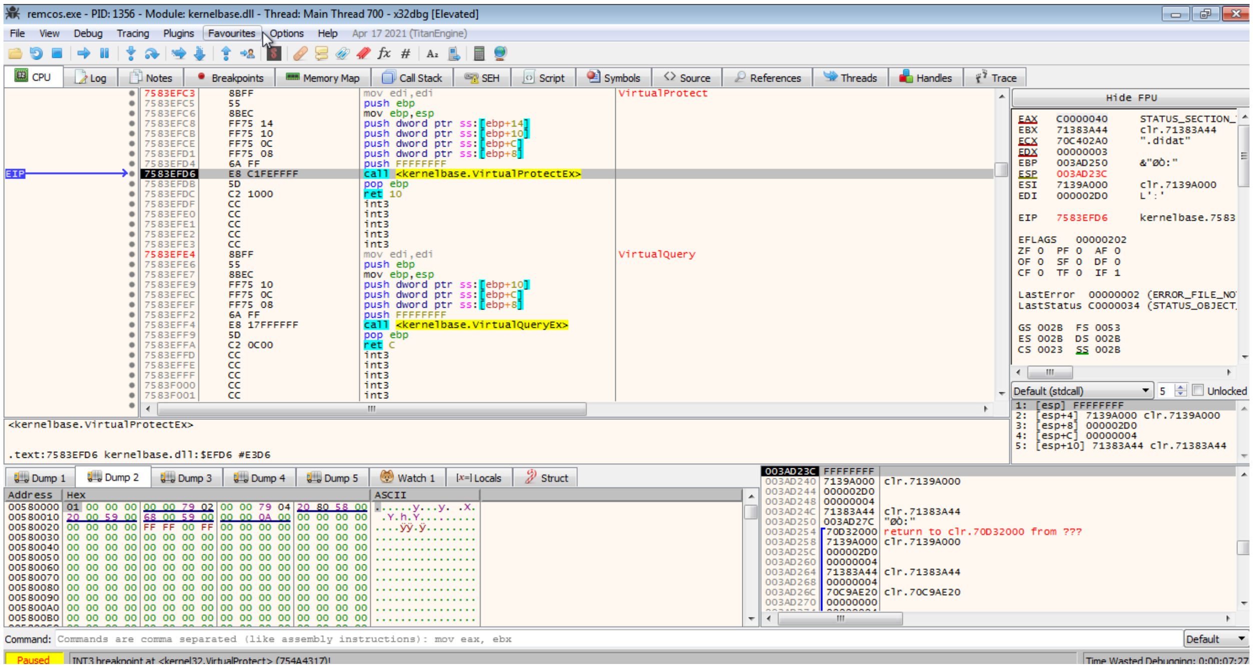
```
EAX   00000001
EBX   003AEEDC
ECX   000002BC     L''
EDX   00000000
EBP   003AEEA4     &"Dï:"
ESP   003AEE98
ESI   00000001
EDI   00000000

EIP   7584379C     kernelbase.7584

EFLAGS   00000202
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS
LastStatus C0000135 (STATUS_DLL_NC

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

Default (stdcall)  5  Unlock
1: [esp+4] 00000000
2: [esp+8] 000002BC
3: [esp+C] 003AEEC4 &"€ð:"
4: [esp+10] 72D34598 uxtheme.72D34
5: [esp+14] 00000000
```

```
Address   Hex                                               ASCII
00580000  01 00 00 00 00 00 79 02 00 00 79 04 20 80 58 00  ......y...y. .X.
00580010  20 00 59 00 68 00 59 00 00 00 0A 00 00 00 00 00   .Y.h.Y.........
00580020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
003AEE98  72D34F05  return to uxtheme.72D34F05 from ???
003AEE9C  00000000
003AEEA0  000002BC
003AEEA4  003AEEC4  &"€ð:"
003AEEA8  72D34598  return to uxtheme.72D34598 from uxtheme.72D34550
003AEEAC  00000000
003AEEB0  003AEEDC
003AEEB4  75650280  user32.75650280
003AEEB8  00000000
003AEEBC  00000000
003AEEC0  00000000
003AEEC4  003AEF44  &"1ó:"
003AEEC8  755EACD4  return to user32.755EACD4 from ???
003AEECC  00000000
```

```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused   INT3 breakpoint at <kernel32.IsDebuggerPresent> (754A4A15)!
Time Wasted Debugging: 0:00:07
```

So here now here again get breakpoint at VirtualProtect and here again the second parameter is clr.Now we will disable the breakpoint at VirtualProtect.



remcos.exe - PID: 1356 - Module: kernelbase.dll - Thread: Main Thread 700 - x32dbg [Elevated]

```
       7583EFC3   8BFF            mov edi,edi                          VirtualProtect
       7583EFC5   55              push ebp
       7583EFC6   8BEC            mov ebp,esp
       7583EFC8   FF75 14         push dword ptr ss:[ebp+14]
       7583EFCB   FF75 10         push dword ptr ss:[ebp+10]
       7583EFCE   FF75 0C         push dword ptr ss:[ebp+C]
       7583EFD1   FF75 08         push dword ptr ss:[ebp+8]
       7583EFD4   6A FF           push FFFFFFFF
EIP →  7583EFD6   E8 C1FEFFFF     call <kernelbase.VirtualProtectEx>
       7583EFDB   5D              pop ebp
       7583EFDC   C2 1000         ret 10
       7583EFDF   CC              int3
       7583EFE0   CC              int3
       7583EFE1   CC              int3
       7583EFE2   CC              int3
       7583EFE3   CC              int3
       7583EFE4   8BFF            mov edi,edi                          VirtualQuery
       7583EFE6   55              push ebp
       7583EFE7   8BEC            mov ebp,esp
       7583EFE9   FF75 10         push dword ptr ss:[ebp+10]
       7583EFEC   FF75 0C         push dword ptr ss:[ebp+C]
       7583EFEF   FF75 08         push dword ptr ss:[ebp+8]
       7583EFF2   6A FF           push FFFFFFFF
       7583EFF4   E8 17FFFFFF     call <kernelbase.VirtualQueryEx>
       7583EFF9   5D              pop ebp
       7583EFFA   C2 0C00         ret C
       7583EFFD   CC              int3
       7583EFFE   CC              int3
       7583EFFF   CC              int3
       7583F000   CC              int3
       7583F001   CC              int3

<kernelbase.VirtualProtectEx>

.text:7583EFD6 kernelbase.dll:$EFD6 #E3D6
```

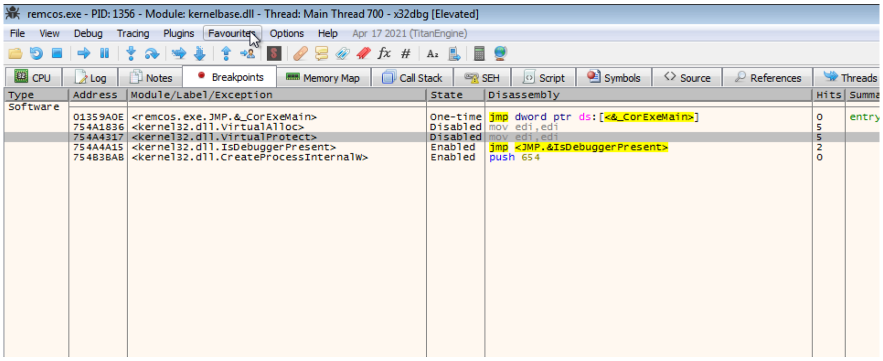
```
EAX   C0000040     STATUS_SECTION_
EBX   71383A44     clr.71383A44
ECX   70C402A0     ".didat"
EDX   00000003
EBP   003AD250     &"ØÒ:"
ESP   003AD23C
ESI   7139A000     clr.7139A000
EDI   000002D0     L':'

EIP   7583EFD6     kernelbase.7583

EFLAGS   00000202
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000002 (ERROR_FILE_NO
LastStatus C0000034 (STATUS_OBJECT

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

Default (stdcall)  5  Unlocked
1: [esp] FFFFFFFF
2: [esp+4] 7139A000 clr.7139A000
3: [esp+8] 000002D0
4: [esp+C] 00000004
5: [esp+10] 71383A44 clr.71383A44
```

```
Address   Hex                                               ASCII
00580000  01 00 00 00 00 00 79 02 00 00 79 04 20 80 58 00  ......y...y. .X.
00580010  20 00 59 00 68 00 59 00 00 00 0A 00 00 00 00 00   .Y.h.Y.........
00580020  00 00 00 00 FF FF 00 FF 00 00 00 00 00 00 00 00  ....ÿÿ.ÿ........
00580030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
003AD23C  FFFFFFFF
003AD240  7139A000  clr.7139A000
003AD244  000002D0
003AD248  00000004
003AD24C  71383A44  clr.71383A44
003AD250  003AD27C  "ØÒ:"
003AD254  70D32000  return to clr.70D32000 from ???
003AD258  7139A000  clr.7139A000
003AD25C  000002D0
003AD260  00000004
003AD264  71383A44  clr.71383A44
003AD268  00000004
003AD26C  70C9AE20  clr.70C9AE20
003AD270  00000000
```

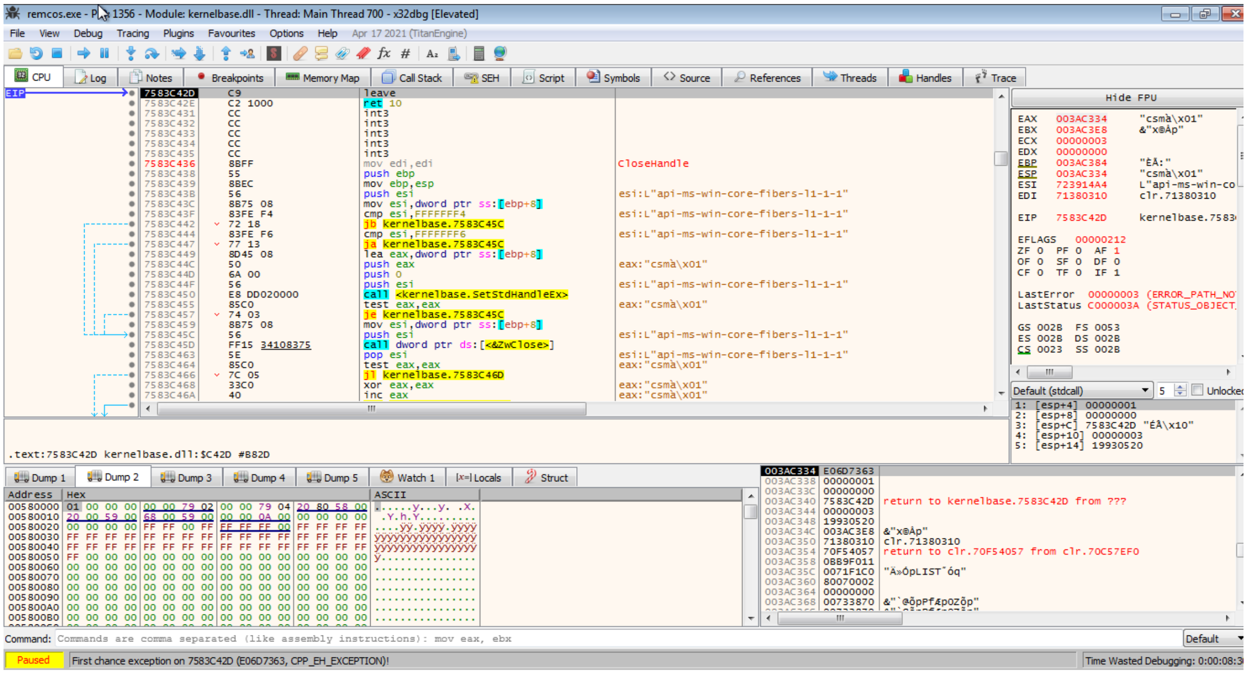
```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused   INT3 breakpoint at <kernel32.VirtualProtect> (754A4317)!
Time Wasted Debugging: 0:00:07:27
```

Here we disable the breakpoint at VirtualProtect.



```
Type      Address   Module/Label/Exception                 State     Disassembly                         Hits Summa
Software
          01359A0E  <remcos.exe.JMP.&_CorExeMain>          One-time  jmp dword ptr ds:[<&_CorExeMain>]   0    entry
          754A1836  <kernel32.dll.VirtualAlloc>            Disabled  mov edi,edi                         5
          754A4317  <kernel32.dll.VirtualProtect>          Disabled  mov edi,edi                         5
          754A4A15  <kernel32.dll.IsDebuggerPresent>       Enabled   jmp <JMP.&IsDebuggerPresent>        2
          754B3BAB  <kernel32.dll.CreateProcessInternalW>  Enabled   push 654                            0
```

Here we got first chance exception just press f9.



```
EIP  7583C42D  C9            leave
     7583C42E  C2 1000       ret 10
     7583C431  CC            int3
     7583C432  CC            int3
     7583C433  CC            int3
     7583C434  CC            int3
     7583C435  CC            int3
     7583C436  8BFF          mov edi,edi                          CloseHandle
     7583C438  55            push ebp
     7583C439  8BEC          mov ebp,esp
     7583C43B  56            push esi                             esi:L"api-ms-win-core-fibers-l1-1-1"
     7583C43C  8B75 08       mov esi,dword ptr ss:[ebp+8]
     7583C43F  83FE F4       cmp esi,FFFFFFF4                     esi:L"api-ms-win-core-fibers-l1-1-1"
     7583C442  72 18         jb kernelbase.7583C45C
     7583C444  83FE F6       cmp esi,FFFFFFF6                     esi:L"api-ms-win-core-fibers-l1-1-1"
     7583C447  77 13         ja kernelbase.7583C45C
     7583C449  8D45 08       lea eax,dword ptr ss:[ebp+8]
     7583C44C  50            push eax                             eax:"csmà\x01"
     7583C44D  6A 00         push 0
     7583C44F  56            push esi                             esi:L"api-ms-win-core-fibers-l1-1-1"
     7583C450  E8 DD020000   call <kernelbase.SetStdHandleEx>
     7583C455  85C0          test eax,eax                         eax:"csmà\x01"
     7583C457  74 03         je kernelbase.7583C45C
     7583C459  8B75 08       mov esi,dword ptr ss:[ebp+8]
     7583C45C  56            push esi                             esi:L"api-ms-win-core-fibers-l1-1-1"
     7583C45D  FF15 34108375 call dword ptr ds:[<&ZwClose>]
     7583C463  5E            pop esi                              esi:L"api-ms-win-core-fibers-l1-1-1"
     7583C464  85C0          test eax,eax                         eax:"csmà\x01"
     7583C466  7C 05         jl kernelbase.7583C46D
     7583C468  33C0          xor eax,eax                          eax:"csmà\x01"
     7583C46A  40            inc eax                              eax:"csmà\x01"

.text:7583C42D kernelbase.dll:$C42D #B82D
```

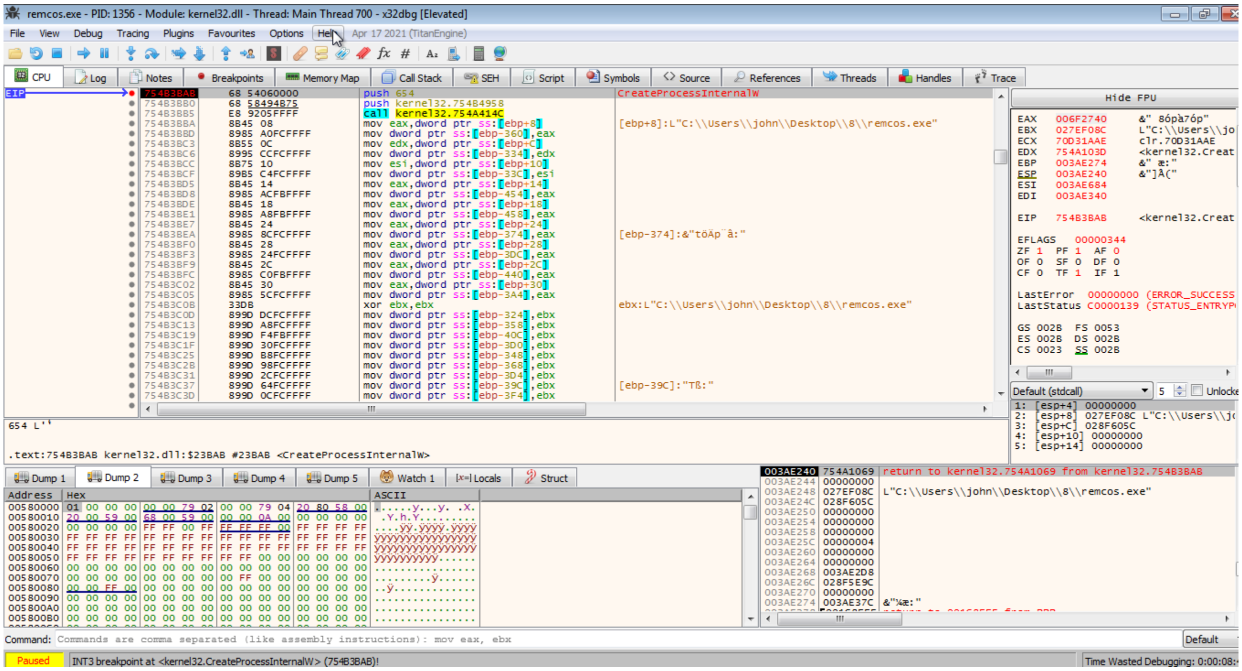
```
EAX   003AC334     "csmà\x01"
EBX   003AC3E8     &"x®Åp"
ECX   00000003
EDX   00000000
EBP   003AC384     "ÈÅ:"
ESP   003AC334     "csmà\x01"
ESI   723914A4     L"api-ms-win-co
EDI   71380310     clr.71380310

EIP   7583C42D     kernelbase.7583

EFLAGS    00000212
ZF 0  PF 0  AF 1
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000003 (ERROR_PATH_NO
LastStatus C000003A (STATUS_OBJECT_

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

1: [esp+4] 00000001
2: [esp+8] 00000000
3: [esp+C] 7583C42D "ÉÅ\x10"
4: [esp+10] 00000003
5: [esp+14] 19930520
```

```
Address   Hex                                              ASCII
00580000  01 00 00 00 00 00 79 02 00 00 79 04 20 80 58 00  ......y...y. .X.
00580010  20 00 59 00 68 00 59 00 00 00 0A 00 00 00 00 00   .Y.h.Y.........
00580020  00 00 00 00 FF FF 00 FF FF FF FF 00 FF FF FF FF  ....ÿÿ.ÿÿÿÿ.ÿÿÿÿ
00580030  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00580040  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00580050  FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ÿ...............
00580060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
003AC334  E06D7363
003AC338  00000001
003AC33C  00000000
003AC340  7583C42D  return to kernelbase.7583C42D from ???
003AC344  00000003
003AC348  19930520
003AC34C  003AC3E8  &"x®Åp"
003AC350  71380310  clr.71380310
003AC354  70F54057  return to clr.70F54057 from clr.70C57EF0
003AC358  0BB9F011
003AC35C  0071F1C0  "Ä»ÓpLIST˜óq"
003AC360  80070002
003AC364  00000000
003AC368  00733870  &"`@õpPfÆpOZõp"
```

```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused  First chance exception on 7583C42D (E06D7363, CPP_EH_EXCEPTION)!        Time Wasted Debugging: 0:00:08:3
```

Now here we got breakpoint at CreateProcessInternalW (here in its parameter it have remcos.exe that means it is going to spawn a child process from his ownself).



remcos.exe - PID: 1356 - Module: kernel32.dll - Thread: Main Thread 700 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace

```
EIP 754B3BAB  68 54060000     push 654                                CreateProcessInternalW
    754B3BB0  68 58494B75     push kernel32.754B4958
    754B3BB5  E8 9205FFFF     call kernel32.754A414C
    754B3BBA  8B45 08         mov eax,dword ptr ss:[ebp+8]            [ebp+8]:L"C:\\Users\\john\\Desktop\\8\\remcos.exe"
    754B3BBD  8985 A0FCFFFF   mov dword ptr ss:[ebp-360],eax
    754B3BC3  8B55 0C         mov edx,dword ptr ss:[ebp+C]
    754B3BC6  8995 CCFCFFFF   mov dword ptr ss:[ebp-334],edx
    754B3BCC  8B75 10         mov esi,dword ptr ss:[ebp+10]
    754B3BCF  89B5 C4FCFFFF   mov dword ptr ss:[ebp-33C],esi
    754B3BD5  8B45 14         mov eax,dword ptr ss:[ebp+14]
    754B3BD8  8985 ACFBFFFF   mov dword ptr ss:[ebp-454],eax
    754B3BDE  8B45 18         mov eax,dword ptr ss:[ebp+18]
    754B3BE1  8985 A8FBFFFF   mov dword ptr ss:[ebp-458],eax
    754B3BE7  8B45 24         mov eax,dword ptr ss:[ebp+24]
    754B3BEA  8985 8CFCFFFF   mov dword ptr ss:[ebp-374],eax          [ebp-374]:&"töÄp¨â:"
    754B3BF0  8B45 28         mov eax,dword ptr ss:[ebp+28]
    754B3BF3  8985 24FCFFFF   mov dword ptr ss:[ebp-3DC],eax
    754B3BF9  8B45 2C         mov eax,dword ptr ss:[ebp+2C]
    754B3BFC  8985 C0FBFFFF   mov dword ptr ss:[ebp-440],eax
    754B3C02  8B45 30         mov eax,dword ptr ss:[ebp+30]
    754B3C05  8985 5CFCFFFF   mov dword ptr ss:[ebp-3A4],eax
    754B3C0B  33DB            xor ebx,ebx                             ebx:L"C:\\Users\\john\\Desktop\\8\\remcos.exe"
    754B3C0D  899D DCFCFFFF   mov dword ptr ss:[ebp-324],ebx
    754B3C13  899D A8FCFFFF   mov dword ptr ss:[ebp-358],ebx
    754B3C19  899D F4FBFFFF   mov dword ptr ss:[ebp-40C],ebx
    754B3C1F  899D 30FCFFFF   mov dword ptr ss:[ebp-3D0],ebx
    754B3C25  899D B8FCFFFF   mov dword ptr ss:[ebp-348],ebx
    754B3C2B  899D 98FCFFFF   mov dword ptr ss:[ebp-368],ebx
    754B3C31  899D 2CFCFFFF   mov dword ptr ss:[ebp-3D4],ebx
    754B3C37  899D 64FCFFFF   mov dword ptr ss:[ebp-39C],ebx          [ebp-39C]:"Tß:"
    754B3C3D  899D 0CFCFFFF   mov dword ptr ss:[ebp-3F4],ebx

654 L''

.text:754B3BAB kernel32.dll:$23BAB #23BAB <CreateProcessInternalW>
```

```
Hide FPU
EAX     006F2740      &" 8ópà7óp"
EBX     027EF08C      L"C:\\Users\\jo
ECX     70D31AAE      clr.70D31AAE
EDX     754A103D      <kernel32.Creat
EBP     003AE274      &" æ:"
ESP     003AE240      &"]Â("
ESI     003AE684
EDI     003AE340

EIP     754B3BAB      <kernel32.Creat

EFLAGS    00000344
ZF 1   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 1   IF 1

LastError   00000000 (ERROR_SUCCESS
LastStatus  C0000139 (STATUS_ENTRYP

GS 002B   FS 0053
ES 002B   DS 002B
CS 0023   SS 002B

Default (stdcall)   5   Unlocke
1:  [esp+4]  00000000
2:  [esp+8]  027EF08C L"C:\\Users\\jo
3:  [esp+C]  028F605C
4:  [esp+10] 00000000
5:  [esp+14] 00000000
```

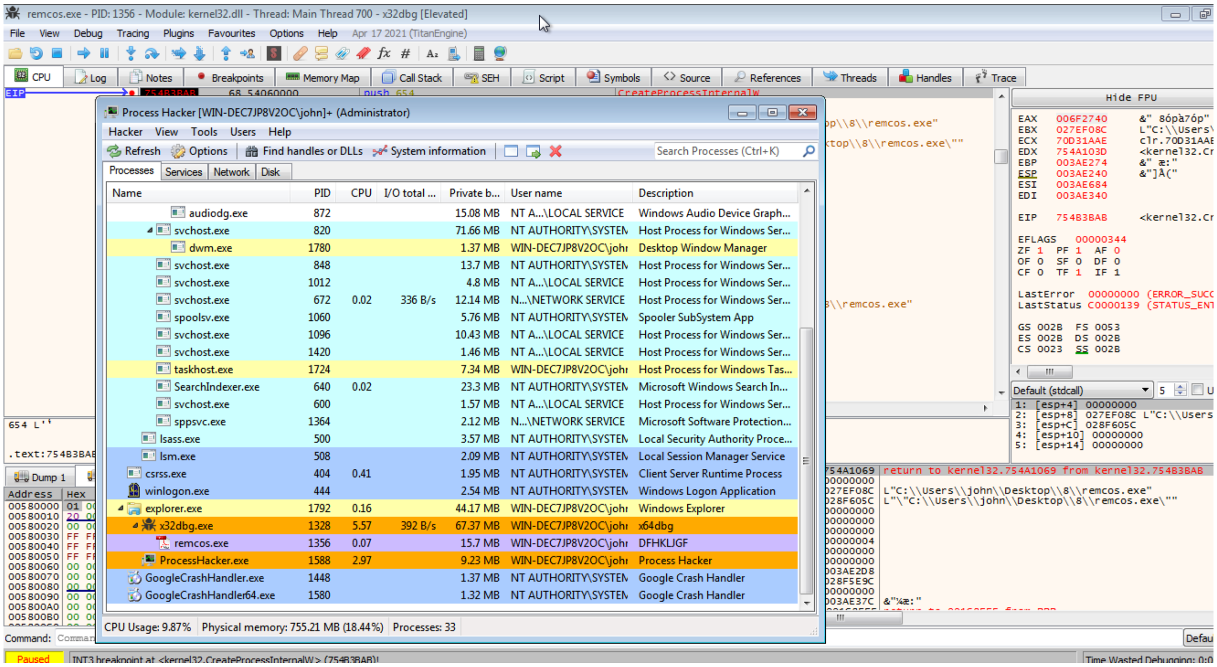
```
Address   Hex                                               ASCII
00580000  01 00 00 00 00 00 79 02 00 00 79 04 20 80 58 00  ......y...y. .X.
00580010  20 00 59 00 68 00 59 00 00 00 0A 00 00 00 00 00   .Y.h.Y.........
00580020  00 00 00 00 FF FF 00 FF FF FF FF 00 FF FF FF FF  ....ÿÿ.ÿÿÿÿ.ÿÿÿÿ
00580030  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00580040  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00580050  FF FF FF FF FF FF FF FF FF FF 00 00 00 00 00 00  ÿÿÿÿÿÿÿÿÿÿ......
00580060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580070  00 00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00  .........ÿ......
00580080  00 00 FF 00 00 00 00 00 00 00 00 00 00 00 00 00  ..ÿ.............
00580090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
003AE240  754A1069  return to kernel32.754A1069 from kernel32.754B3BAB
003AE244  00000000
003AE248  027EF08C  L"C:\\Users\\john\\Desktop\\8\\remcos.exe"
003AE24C  028F605C
003AE250  00000000
003AE254  00000000
003AE258  00000000
003AE25C  00000004
003AE260  00000000
003AE264  00000000
003AE268  003AE2D8
003AE26C  028F5E9C
003AE270  00000000
003AE274  003AE37C  &"¼æ:"
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused   INT3 breakpoint at <kernel32.CreateProcessInternalW> (754B3BAB)!   Time Wasted Debugging: 0:00:08:

Here we can view that process in Process Hacker.



Process Hacker [WIN-DEC7JP8V2OC\john]+ (Administrator)

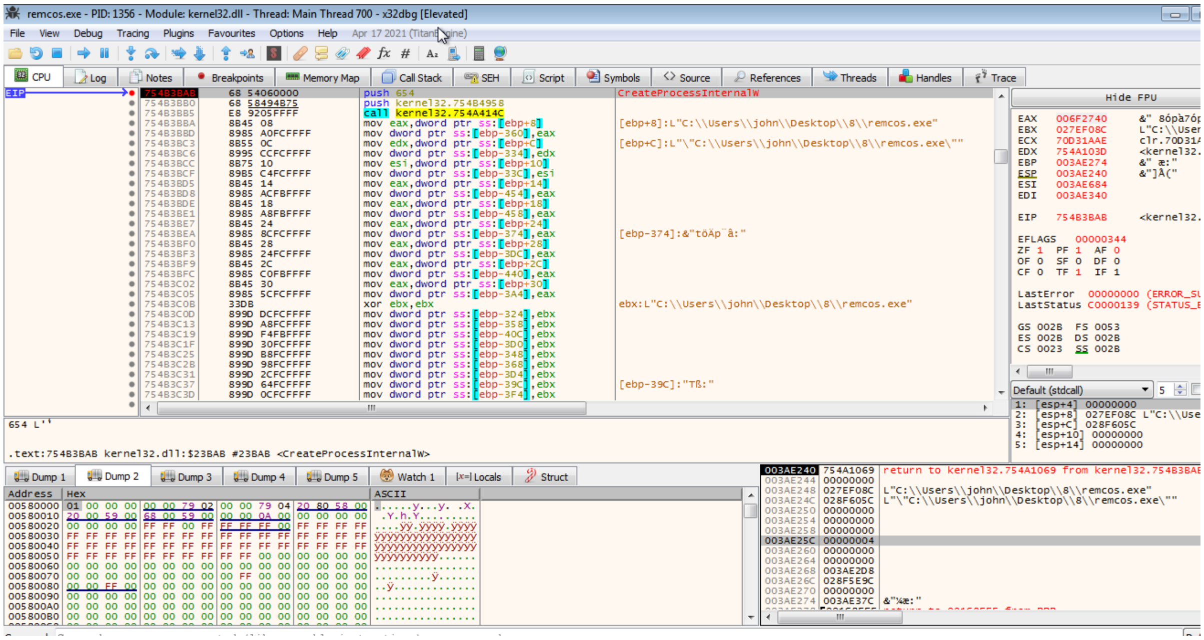
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
Processes Services Network Disk

Name	PID	CPU	I/O total ...	Private b...	User name	Description
audiodg.exe	872			15.08 MB	NT A...\LOCAL SERVICE	Windows Audio Device Graph...
svchost.exe	820			71.66 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
dwm.exe	1780			1.37 MB	WIN-DEC7JP8V2OC\john	Desktop Window Manager
svchost.exe	848			13.7 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	1012			4.8 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
svchost.exe	672	0.02	336 B/s	12.14 MB	N...\NETWORK SERVICE	Host Process for Windows Ser...
spoolsv.exe	1060			5.76 MB	NT AUTHORITY\SYSTEM	Spooler SubSystem App
svchost.exe	1096			10.43 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
svchost.exe	1420			1.46 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
taskhost.exe	1724			7.34 MB	WIN-DEC7JP8V2OC\john	Host Process for Windows Tas...
SearchIndexer.exe	640	0.02		23.3 MB	NT AUTHORITY\SYSTEM	Microsoft Windows Search In...
svchost.exe	600			1.57 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
sppsvc.exe	1364			2.12 MB	N...\NETWORK SERVICE	Microsoft Software Protection...
lsass.exe	500			3.57 MB	NT AUTHORITY\SYSTEM	Local Security Authority Proce...
lsm.exe	508			2.09 MB	NT AUTHORITY\SYSTEM	Local Session Manager Service
csrss.exe	404	0.41		1.95 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
winlogon.exe	444			2.54 MB	NT AUTHORITY\SYSTEM	Windows Logon Application
explorer.exe	1792	0.16		44.17 MB	WIN-DEC7JP8V2OC\john	Windows Explorer
x32dbg.exe	1328	5.57	392 B/s	67.37 MB	WIN-DEC7JP8V2OC\john	x64dbg
remcos.exe	1356	0.07		15.7 MB	WIN-DEC7JP8V2OC\john	DFHKLJGF
ProcessHacker.exe	1588	2.97		9.23 MB	WIN-DEC7JP8V2OC\john	Process Hacker
GoogleCrashHandler.exe	1448			1.37 MB	NT AUTHORITY\SYSTEM	Google Crash Handler
GoogleCrashHandler64.exe	1580			1.32 MB	NT AUTHORITY\SYSTEM	Google Crash Handler

CPU Usage: 9.87%   Physical memory: 755.21 MB (18.44%)   Processes: 33

```
754A1069  return to kernel32.754A1069 from kernel32.754B3BAB
00000000
027EF08C  L"C:\\Users\\john\\Desktop\\8\\remcos.exe"
028F605C  L"\"C:\\Users\\john\\Desktop\\8\\remcos.exe\""
00000000
00000000
00000000
00000004
00000000
00000000
003AE2D8
028F5E9C
00000000
003AE37C  &"¼æ:"
```

Here we look at the seventh parameter i.e 4 which indicates that it will create the new process at suspended state.Now here we can add breakpoint at NtResumeThread which would bring this out of suspended state.


remcos.exe - PID: 1356 - Module: kernel32.dll - Thread: Main Thread 700 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Default (stdcall) 5

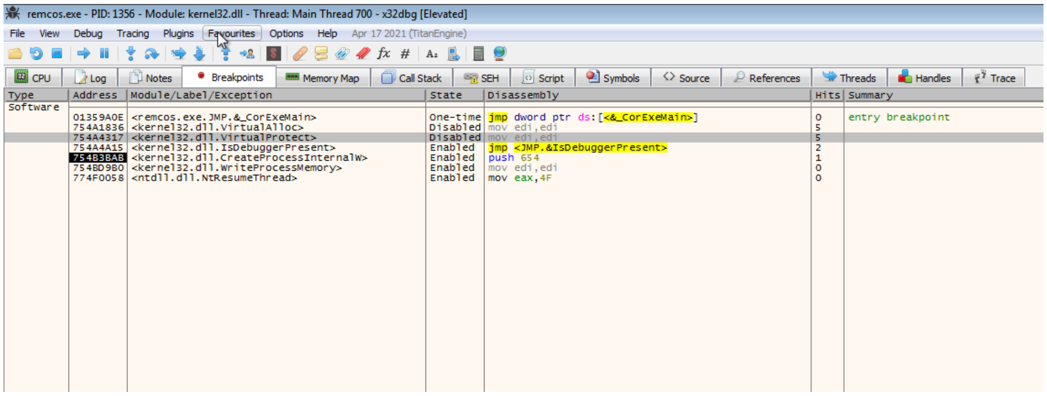
```
EIP  754B3BAB   68 54060000   push 654                             CreateProcessInternalW
     754B3BB0   68 58494B75   push kernel32.754B4958
     754B3BB5   E8 9205FFFF   call kernel32.754A414C
     754B3BBA   8B45 08       mov eax,dword ptr ss:[ebp+8]         [ebp+8]:L"C:\\Users\\john\\Desktop\\8\\remcos.exe"
     754B3BBD   8985 A0FCFFFF mov dword ptr ss:[ebp-360],eax
     754B3BC3   8B55 0C       mov edx,dword ptr ss:[ebp+C]         [ebp+C]:L"\"C:\\Users\\john\\Desktop\\8\\remcos.exe\""
     754B3BC6   8995 CCFCFFFF mov dword ptr ss:[ebp-334],edx
     754B3BCC   8B75 10       mov esi,dword ptr ss:[ebp+10]
     754B3BCF   89B5 C4FCFFFF mov dword ptr ss:[ebp-33C],esi
     754B3BD5   8B45 14       mov eax,dword ptr ss:[ebp+14]
     754B3BD8   8985 ACFBFFFF mov dword ptr ss:[ebp-454],eax
     754B3BDE   8B45 18       mov eax,dword ptr ss:[ebp+18]
     754B3BE1   8985 A8FBFFFF mov dword ptr ss:[ebp-458],eax
     754B3BE7   8B45 24       mov eax,dword ptr ss:[ebp+24]
     754B3BEA   8985 8CFCFFFF mov dword ptr ss:[ebp-374],eax         [ebp-374]:&"töÄp¨â:"
     754B3BF0   8B45 28       mov eax,dword ptr ss:[ebp+28]
     754B3BF3   8985 24FCFFFF mov dword ptr ss:[ebp-3DC],eax
     754B3BF9   8B45 2C       mov eax,dword ptr ss:[ebp+2C]
     754B3BFC   8985 C0FBFFFF mov dword ptr ss:[ebp-440],eax
     754B3C02   8B45 30       mov eax,dword ptr ss:[ebp+30]
     754B3C05   8985 5CFCFFFF mov dword ptr ss:[ebp-3A4],eax
     754B3C0B   33DB          xor ebx,ebx                          ebx:L"C:\\Users\\john\\Desktop\\8\\remcos.exe"
     754B3C0D   899D DCFCFFFF mov dword ptr ss:[ebp-324],ebx
     754B3C13   899D A8FCFFFF mov dword ptr ss:[ebp-358],ebx
     754B3C19   899D F4FBFFFF mov dword ptr ss:[ebp-40C],ebx
     754B3C1F   899D 30FCFFFF mov dword ptr ss:[ebp-3D0],ebx
     754B3C25   899D B8FCFFFF mov dword ptr ss:[ebp-348],ebx
     754B3C2B   899D 98FCFFFF mov dword ptr ss:[ebp-368],ebx
     754B3C31   899D 2CFCFFFF mov dword ptr ss:[ebp-3D4],ebx
     754B3C37   899D 64FCFFFF mov dword ptr ss:[ebp-39C],ebx         [ebp-39C]:"Tß:"
     754B3C3D   899D 0CFCFFFF mov dword ptr ss:[ebp-3F4],ebx

654 L''

.text:754B3BAB kernel32.dll:$23BAB #23BAB <CreateProcessInternalW>
```

```
EAX  006F2740   &" 8ópà7óp
EBX  027EF08C   L"C:\\User
ECX  70D31AAE   clr.70D31A
EDX  754A103D   <kernel32.
EBP  003AE274   &" æ:"
ESP  003AE240   &"]Å("
ESI  003AE684
EDI  003AE340

EIP  754B3BAB   <kernel32.

EFLAGS  00000344
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1

LastError  00000000 (ERROR_SU
LastStatus C0000139 (STATUS_E

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

1: [esp+4] 00000000
2: [esp+8] 027EF08C L"C:\\Use
3: [esp+C] 028F605C
4: [esp+10] 00000000
5: [esp+14] 00000000
```

```
Address   Hex                                              ASCII
00580000  01 00 00 00 00 00 79 02 00 00 79 04 20 80 58 00  ......y...y. .X.
00580010  20 00 59 00 68 00 59 00 00 00 0A 00 00 00 00 00   .Y.h.Y.........
00580020  00 00 00 00 FF FF 00 FF FF FF FF 00 FF FF FF FF  ....ÿÿ.ÿÿÿÿ.ÿÿÿÿ
00580030  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00580040  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00580050  FF FF FF FF FF FF FF FF FF FF 00 00 00 00 00 00  ÿÿÿÿÿÿÿÿÿÿ......
00580060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580070  00 00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00  .........ÿ......
00580080  00 00 FF 00 00 00 00 00 00 00 00 00 00 00 00 00  ..ÿ.............
00580090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

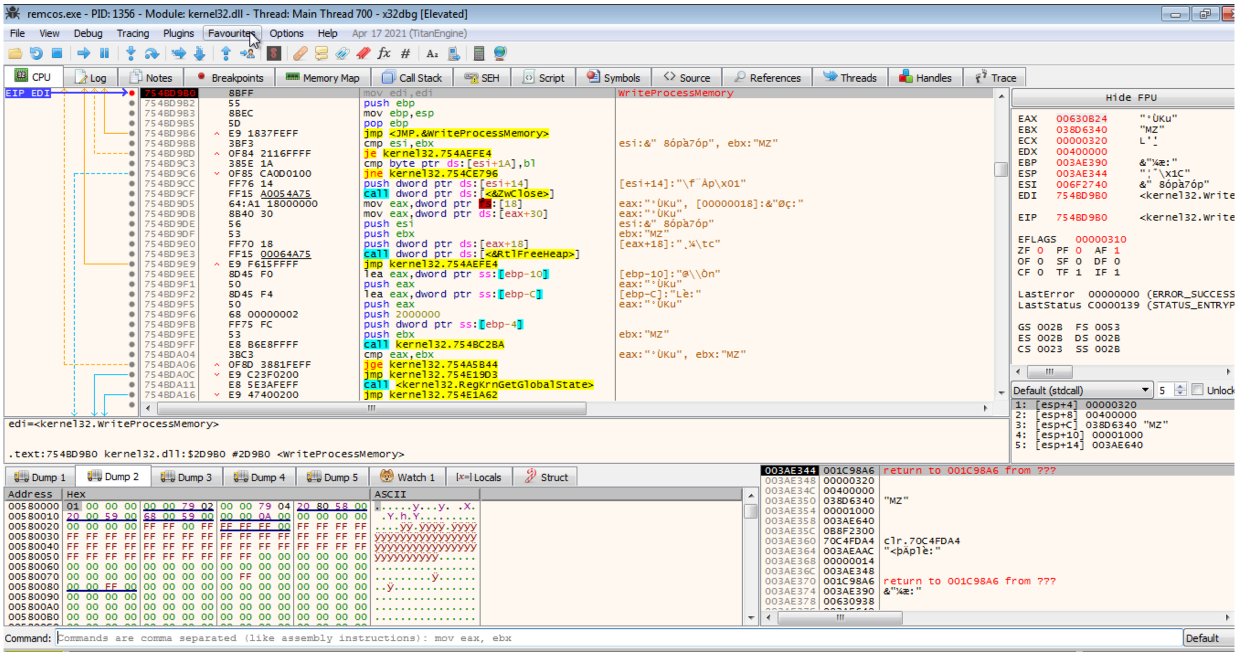
```
003AE240  754A1069  return to kernel32.754A1069 from kernel32.754B3BAB
003AE244  00000000
003AE248  027EF08C  L"C:\\Users\\john\\Desktop\\8\\remcos.exe"
003AE24C  028F605C  L"\"C:\\Users\\john\\Desktop\\8\\remcos.exe\""
003AE250  00000000
003AE254  00000000
003AE258  00000000
003AE25C  00000004
003AE260  00000000
003AE264  00000000
003AE268  003AE2D8
003AE26C  028F5E9C
003AE270  00000000
003AE274  003AE37C  &"¼æ:"
```

Here we add breakpoint at NtResumeThread(to resume a process from a suspended state) and also at WriteProcessMemory(to overwrite the section of child process with some another code).


remcos.exe - PID: 1356 - Module: kernel32.dll - Thread: Main Thread 700 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace

Type	Address	Module/Label/Exception	State	Disassembly	Hits	Summary
Software						
	01359A0E	<remcos.exe.JMP.&_CorExeMain>	One-time	jmp dword ptr ds:[<&_CorExeMain>]	0	entry breakpoint
	754A1836	<kernel32.dll.VirtualAlloc>	Disabled	mov edi,edi	5	
	754A4317	<kernel32.dll.VirtualProtect>	Disabled	mov edi,edi	5	
	754A4A15	<kernel32.dll.IsDebuggerPresent>	Enabled	jmp <JMP.&IsDebuggerPresent>	2	
	754B3BAB	<kernel32.dll.CreateProcessInternalW>	Enabled	push 654	1	
	754BD9B0	<kernel32.dll.WriteProcessMemory>	Enabled	mov edi,edi	0	
	774F0058	<ntdll.dll.NtResumeThread>	Enabled	mov eax,4F	0	

Here we hit breakpoint at WriteProcessMemory , here it will write to the child process we can view it in Process Hacker.



remcos.exe - PID: 1356 - Module: kernel32.dll - Thread: Main Thread 700 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

```
EIP EDI  754BD9B0  8BFF            mov edi,edi                               WriteProcessMemory
         754BD9B2  55              push ebp
         754BD9B3  8BEC            mov ebp,esp
         754BD9B5  5D              pop ebp
         754BD9B6  E9 1837FEFF     jmp <JMP.&WriteProcessMemory>
         754BD9BB  3BF3            cmp esi,ebx                               esi:&" 8ópà7óp", ebx:"MZ"
         754BD9BD  0F84 2116FFFF   je kernel32.754AEFE4
         754BD9C3  385E 1A         cmp byte ptr ds:[esi+1A],bl
         754BD9C6  0F85 CA0D0100   jne kernel32.754CE796
         754BD9CC  FF76 14         push dword ptr ds:[esi+14]                [esi+14]:"\f¨Áp\x01"
         754BD9CF  FF15 A0054A75   call dword ptr ds:[<&ZwClose>]
         754BD9D5  64:A1 18000000  mov eax,dword ptr fs:[18]                 eax:"◦ÙKu", [00000018]:&"øç:"
         754BD9DB  8B40 30         mov eax,dword ptr ds:[eax+30]             eax:"◦ÙKu"
         754BD9DE  56              push esi                                  esi:&" 8ópà7óp"
         754BD9DF  53              push ebx                                  ebx:"MZ"
         754BD9E0  FF70 18         push dword ptr ds:[eax+18]                [eax+18]:"¸¼\tc"
         754BD9E3  FF15 00064A75   call dword ptr ds:[<&RtlFreeHeap>]
         754BD9E9  E9 F615FFFF     jmp kernel32.754AEFE4
         754BD9EE  8D45 F0         lea eax,dword ptr ss:[ebp-10]             [ebp-10]:"@\\Òn"
         754BD9F1  50              push eax                                  eax:"◦ÙKu"
         754BD9F2  8D45 F4         lea eax,dword ptr ss:[ebp-C]              [ebp-C]:"Lè:"
         754BD9F5  50              push eax                                  eax:"◦ÙKu"
         754BD9F6  68 00000002     push 2000000
         754BD9FB  FF75 FC         push dword ptr ss:[ebp-4]
         754BD9FE  53              push ebx                                  ebx:"MZ"
         754BD9FF  E8 B6E8FFFF     call kernel32.754BC2BA
         754BDA04  3BC3            cmp eax,ebx                               eax:"◦ÙKu", ebx:"MZ"
         754BDA06  0F8D 3881FEFF   jge kernel32.754A5B44
         754BDA0C  E9 C23F0200     jmp kernel32.754E19D3
         754BDA11  E8 5E3AFEFF     call <kernel32.RegKrnGetGlobalState>
         754BDA16  E9 47400200     jmp kernel32.754E1A62

edi=<kernel32.WriteProcessMemory>

.text:754BD9B0 kernel32.dll:$2D9B0 #2D9B0 <WriteProcessMemory>
```

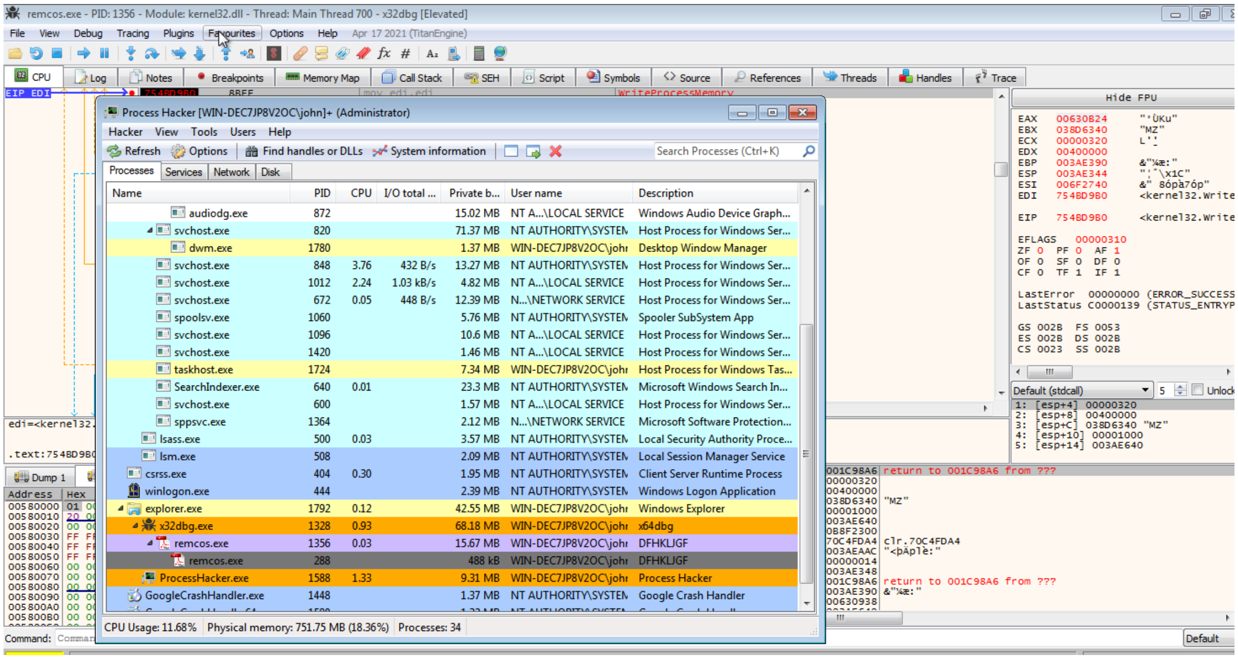
```
EAX     00630B24     "◦ÙKu"
EBX     038D6340     "MZ"
ECX     00000320     L'̲'
EDX     00400000
EBP     003AE390     &"¼æ:"
ESP     003AE344     "¦ˆ\x1C"
ESI     006F2740     &" 8ópà7óp"
EDI     754BD9B0     <kernel32.Write

EIP     754BD9B0     <kernel32.Write

EFLAGS   00000310
ZF 0  PF 0  AF 1
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1

LastError  00000000 (ERROR_SUCCESS
LastStatus C0000139 (STATUS_ENTRYP

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

Default (stdcall)  5  Unlock
1: [esp+4] 00000320
2: [esp+8] 00400000
3: [esp+C] 038D6340 "MZ"
4: [esp+10] 00001000
5: [esp+14] 003AE640
```

```
Address   Hex                                              ASCII
00580000  01 00 00 00 00 00 79 02 00 00 79 04 20 80 58 00  ......y...y. .X.
00580010  20 00 59 00 68 00 59 00 00 00 0A 00 00 00 00 00   .Y.h.Y.........
00580020  00 00 00 00 FF FF 00 FF FF FF FF 00 FF FF FF FF  ....ÿÿ.ÿÿÿÿ.ÿÿÿÿ
00580030  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00580040  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00580050  FF FF FF FF FF FF FF FF FF FF 00 00 00 00 00 00  ÿÿÿÿÿÿÿÿÿÿ......
00580060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580070  00 00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00  .........ÿ......
00580080  00 00 FF 00 00 00 00 00 00 00 00 00 00 00 00 00  ..ÿ.............
00580090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
003AE344  001C98A6  return to 001C98A6 from ???
003AE348  00000320
003AE34C  00400000
003AE350  038D6340  "MZ"
003AE354  00001000
003AE358  003AE640
003AE35C  0B8F2300
003AE360  70C4FDA4  clr.70C4FDA4
003AE364  003AEAAC  "<þÄplè:"
003AE368  00000014
003AE36C  003AE348
003AE370  001C98A6  return to 001C98A6 from ???
003AE374  003AE390  &"¼æ:"
003AE378  00630938
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx Default

Here we can see that parent has spawn a child.



Process Hacker [WIN-DEC7JP8V2OC\john]+ (Administrator)

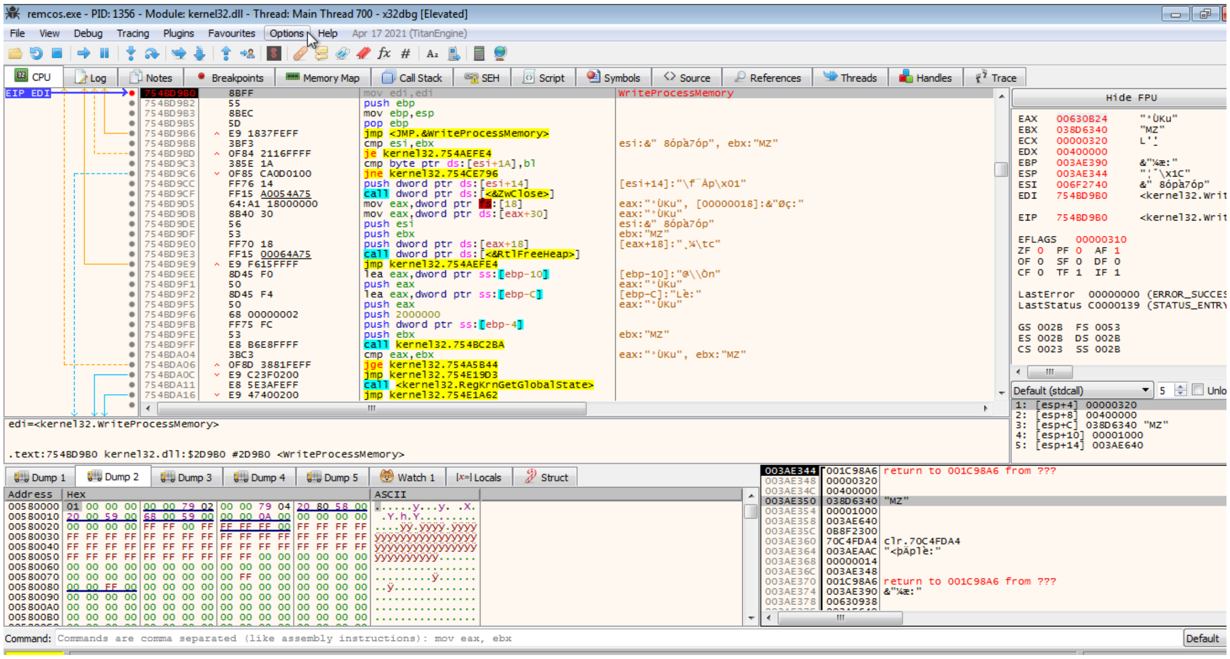
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
Processes Services Network Disk

Name	PID	CPU	I/O total ...	Private b...	User name	Description
audiodg.exe	872			15.02 MB	NT A...\LOCAL SERVICE	Windows Audio Device Graph...
svchost.exe	820			71.37 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
dwm.exe	1780			1.37 MB	WIN-DEC7JP8V2OC\john	Desktop Window Manager
svchost.exe	848	3.76	432 B/s	13.27 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	1012	2.24	1.03 kB/s	4.82 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
svchost.exe	672	0.05	448 B/s	12.39 MB	N...\NETWORK SERVICE	Host Process for Windows Ser...
spoolsv.exe	1060			5.76 MB	NT AUTHORITY\SYSTEM	Spooler SubSystem App
svchost.exe	1096			10.6 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
svchost.exe	1420			1.46 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
taskhost.exe	1724			7.34 MB	WIN-DEC7JP8V2OC\john	Host Process for Windows Tas...
SearchIndexer.exe	640	0.01		23.3 MB	NT AUTHORITY\SYSTEM	Microsoft Windows Search In...
svchost.exe	600			1.57 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
sppsvc.exe	1364			2.12 MB	N...\NETWORK SERVICE	Microsoft Software Protection...
lsass.exe	500	0.03		3.57 MB	NT AUTHORITY\SYSTEM	Local Security Authority Proce...
lsm.exe	508			2.09 MB	NT AUTHORITY\SYSTEM	Local Session Manager Service
csrss.exe	404	0.30		1.95 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
winlogon.exe	444			2.39 MB	NT AUTHORITY\SYSTEM	Windows Logon Application
explorer.exe	1792	0.12		42.55 MB	WIN-DEC7JP8V2OC\john	Windows Explorer
x32dbg.exe	1328	0.93		68.18 MB	WIN-DEC7JP8V2OC\john	x64dbg
remcos.exe	1356	0.03		15.67 MB	WIN-DEC7JP8V2OC\john	DFHKLJGF
remcos.exe	288			488 kB	WIN-DEC7JP8V2OC\john	DFHKLJGF
ProcessHacker.exe	1588	1.33		9.31 MB	WIN-DEC7JP8V2OC\john	Process Hacker
GoogleCrashHandler.exe	1448			1.37 MB	NT AUTHORITY\SYSTEM	Google Crash Handler

CPU Usage: 11.68% | Physical memory: 751.75 MB (18.36%) | Processes: 34

Here we can view the third parameter of the API which is the buffer from where the data will be copied.

```
BOOL WriteProcessMemory(
  [in]  HANDLE  hProcess,
  [in]  LPVOID  lpBaseAddress,
  [in]  LPCVOID lpBuffer,
  [in]  SIZE_T  nSize,
  [out] SIZE_T  *lpNumberOfBytesWritten
);
```



remcos.exe - PID: 1356 - Module: kernel32.dll - Thread: Main Thread 700 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace

```
EIP EDI  754BD9B0    8BFF             mov edi,edi                                WriteProcessMemory
         754BD9B2    55               push ebp
         754BD9B3    8BEC             mov ebp,esp
         754BD9B5    5D               pop ebp
         754BD9B6  ^ E9 1837FEFF      jmp <JMP.&WriteProcessMemory>
         754BD9BB    3BF3             cmp esi,ebx                                esi:&" 8ópà7óp", ebx:"MZ"
         754BD9BD  ^ 0F84 2116FFFF    je kernel32.754AEFE4
         754BD9C3    385E 1A          cmp byte ptr ds:[esi+1A],bl
         754BD9C6  v 0F85 CA0D0100    jne kernel32.754CE796
         754BD9CC    FF76 14          push dword ptr ds:[esi+14]                 [esi+14]:"\f¨Áp\x01"
         754BD9CF    FF15 A0054A75    call dword ptr ds:[<&ZwClose>]
         754BD9D5    64:A1 18000000   mov eax,dword ptr fs:[18]                  eax:"∘ÙKu", [00000018]:&"øç:"
         754BD9DB    8B40 30          mov eax,dword ptr ds:[eax+30]              eax:"∘ÙKu"
         754BD9DE    56               push esi                                   esi:&" 8ópà7óp"
         754BD9DF    53               push ebx                                   ebx:"MZ"
         754BD9E0    FF70 18          push dword ptr ds:[eax+18]                 [eax+18]:"¸¼\tc"
         754BD9E3    FF15 00064A75    call dword ptr ds:[<&RtlFreeHeap>]
         754BD9E9  ^ E9 F615FFFF      jmp kernel32.754AEFE4
         754BD9EE    8D45 F0          lea eax,dword ptr ss:[ebp-10]              [ebp-10]:"@\\Òn"
         754BD9F1    50               push eax                                   eax:"∘ÙKu"
         754BD9F2    8D45 F4          lea eax,dword ptr ss:[ebp-C]               [ebp-C]:"Lè:"
         754BD9F5    50               push eax                                   eax:"∘ÙKu"
         754BD9F6    68 00000002      push 2000000
         754BD9FB    FF75 FC          push dword ptr ss:[ebp-4]
         754BD9FE    53               push ebx                                   ebx:"MZ"
         754BD9FF    E8 B6E8FFFF      call kernel32.754BC2BA
         754BDA04    3BC3             cmp eax,ebx                                eax:"∘ÙKu", ebx:"MZ"
         754BDA06  ^ 0F8D 3881FEFF    jge kernel32.754A5B44
         754BDA0C  v E9 C23F0200      jmp kernel32.754E19D3
         754BDA11    E8 5E3AFEFF      call <kernel32.RegKrnGetGlobalState>
         754BDA16  v E9 47400200      jmp kernel32.754E1A62
```

```
Hide FPU

EAX   00630B24   "∘ÙKu"
EBX   038D6340   "MZ"
ECX   00000320   L'̠'
EDX   00400000
EBP   003AE390   &"¼æ:"
ESP   003AE344   "¦¨\x1C"
ESI   006F2740   &" 8ópà7óp"
EDI   754BD9B0   <kernel32.Writ

EIP   754BD9B0   <kernel32.Writ

EFLAGS   00000310
ZF 0  PF 0  AF 1
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1

LastError  00000000 (ERROR_SUCCES
LastStatus C0000139 (STATUS_ENTRY

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B
```

```
Default (stdcall)   5   □ Unlo
1: [esp+4] 00000320
2: [esp+8] 00400000
3: [esp+C] 038D6340 "MZ"
4: [esp+10] 00001000
5: [esp+14] 003AE640
```

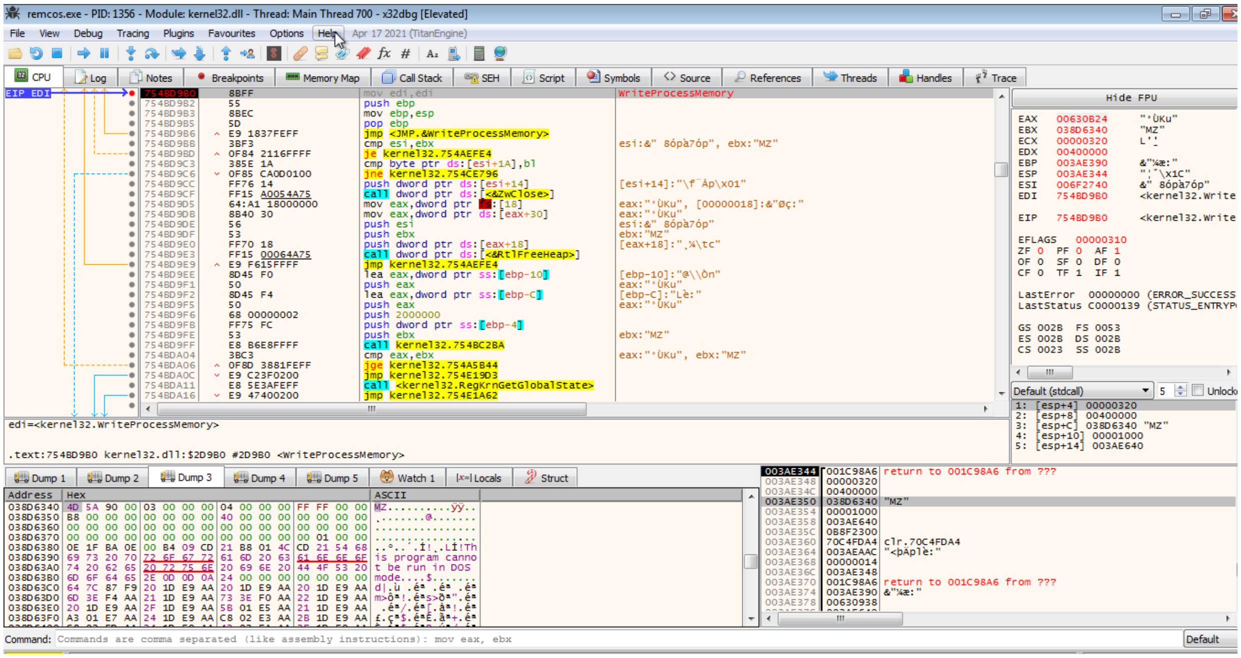
```
edi=<kernel32.WriteProcessMemory>

.text:754BD9B0 kernel32.dll:$2D9B0 #2D9B0 <WriteProcessMemory>
```

```
Address   Hex                                              ASCII
00580000  01 00 00 00 00 00 79 02 00 00 79 04 20 80 58 00  ......y...y. .X.
00580010  20 00 59 00 68 00 59 00 00 00 0A 00 00 00 00 00   .Y.h.Y.........
00580020  00 00 00 00 FF FF 00 FF FF FF FF 00 FF FF FF FF  ....ÿÿ.ÿÿÿÿ.ÿÿÿÿ
00580030  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00580040  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00580050  FF FF FF FF FF FF FF FF FF FF 00 00 00 00 00 00  ÿÿÿÿÿÿÿÿÿÿ......
00580060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00580070  00 00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00  .........ÿ......
00580080  00 00 FF 00 00 00 00 00 00 00 00 00 00 00 00 00  ..ÿ.............
00580090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005800B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
003AE344  001C98A6  return to 001C98A6 from ???
003AE348  00000320
003AE34C  00400000
003AE350  038D6340  "MZ"
003AE354  00001000
003AE358  003AE640
003AE35C  0B8F2300
003AE360  70C4FDA4  clr.70C4FDA4
003AE364  003AEAAC  "<þÄplè:"
003AE368  00000014
003AE36C  003AE348
003AE370  001C98A6  return to 001C98A6 from ???
003AE374  003AE390  &"¼æ:"
003AE378  00630938
```

```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
```

So here now we dump the location 38D6340 in dump3 this is an exe from here we can dump this to a file.



remcos.exe - PID: 1356 - Module: kernel32.dll - Thread: Main Thread 700 - x32dbg [Elevated]

```
EIP EDI  754BD9B0    8BFF             mov edi,edi                                WriteProcessMemory
         754BD9B2    55               push ebp
         754BD9B3    8BEC             mov ebp,esp
         754BD9B5    5D               pop ebp
         754BD9B6  ^ E9 1837FEFF      jmp <JMP.&WriteProcessMemory>
         754BD9BB    3BF3             cmp esi,ebx                                esi:&" 8ópà7óp", ebx:"MZ"
         754BD9BD  ^ 0F84 2116FFFF    je kernel32.754AEFE4
         754BD9C3    385E 1A          cmp byte ptr ds:[esi+1A],bl
         754BD9C6  v 0F85 CA0D0100    jne kernel32.754CE796
         754BD9CC    FF76 14          push dword ptr ds:[esi+14]                 [esi+14]:"\f¨Áp\x01"
         754BD9CF    FF15 A0054A75    call dword ptr ds:[<&ZwClose>]
         754BD9D5    64:A1 18000000   mov eax,dword ptr fs:[18]                  eax:"∘ÙKu", [00000018]:&"øç:"
         754BD9DB    8B40 30          mov eax,dword ptr ds:[eax+30]              eax:"∘ÙKu"
         754BD9DE    56               push esi                                   esi:&" 8ópà7óp"
         754BD9DF    53               push ebx                                   ebx:"MZ"
         754BD9E0    FF70 18          push dword ptr ds:[eax+18]                 [eax+18]:"¸¼\tc"
         754BD9E3    FF15 00064A75    call dword ptr ds:[<&RtlFreeHeap>]
         754BD9E9  ^ E9 F615FFFF      jmp kernel32.754AEFE4
         754BD9EE    8D45 F0          lea eax,dword ptr ss:[ebp-10]              [ebp-10]:"@\\Òn"
         754BD9F1    50               push eax                                   eax:"∘ÙKu"
         754BD9F2    8D45 F4          lea eax,dword ptr ss:[ebp-C]               [ebp-C]:"Lè:"
         754BD9F5    50               push eax                                   eax:"∘ÙKu"
         754BD9F6    68 00000002      push 2000000
         754BD9FB    FF75 FC          push dword ptr ss:[ebp-4]
         754BD9FE    53               push ebx                                   ebx:"MZ"
         754BD9FF    E8 B6E8FFFF      call kernel32.754BC2BA
         754BDA04    3BC3             cmp eax,ebx                                eax:"∘ÙKu", ebx:"MZ"
         754BDA06  ^ 0F8D 3881FEFF    jge kernel32.754A5B44
         754BDA0C  v E9 C23F0200      jmp kernel32.754E19D3
         754BDA11    E8 5E3AFEFF      call <kernel32.RegKrnGetGlobalState>
         754BDA16  v E9 47400200      jmp kernel32.754E1A62
```

```
EAX   00630B24   "∘ÙKu"
EBX   038D6340   "MZ"
ECX   00000320   L'̠'
EDX   00400000
EBP   003AE390   &"¼æ:"
ESP   003AE344   "¦¨\x1C"
ESI   006F2740   &" 8ópà7óp"
EDI   754BD9B0   <kernel32.Write

EIP   754BD9B0   <kernel32.Write

EFLAGS   00000310
ZF 0  PF 0  AF 1
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1

LastError  00000000 (ERROR_SUCCESS
LastStatus C0000139 (STATUS_ENTRYP

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B
```

```
1: [esp+4] 00000320
2: [esp+8] 00400000
3: [esp+C] 038D6340 "MZ"
4: [esp+10] 00001000
5: [esp+14] 003AE640
```

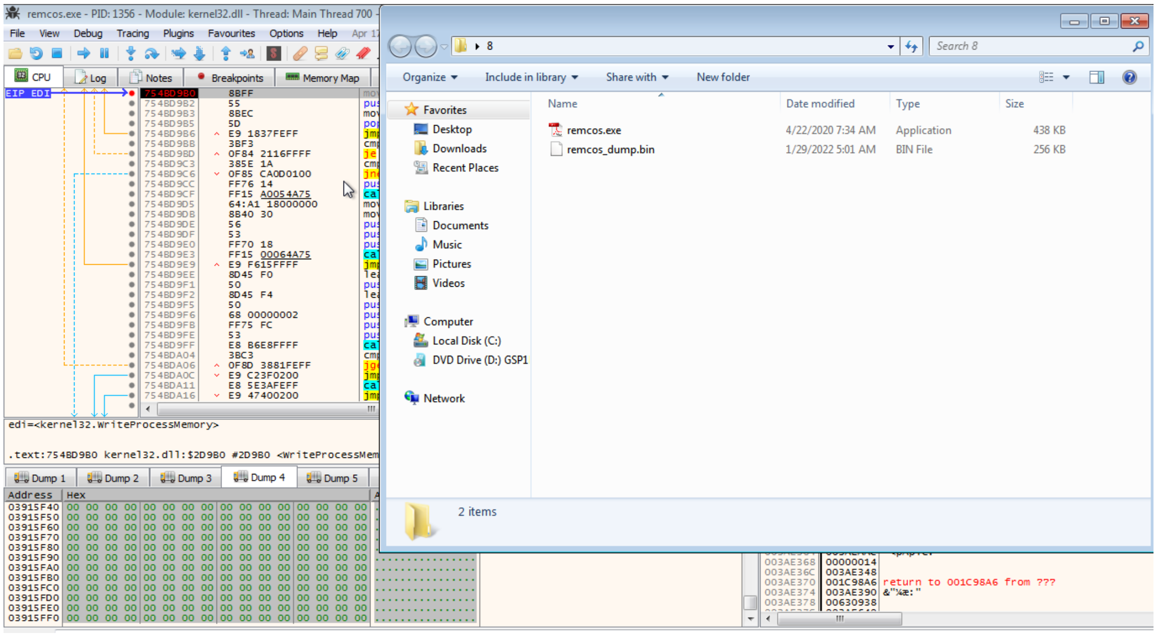
```
edi=<kernel32.WriteProcessMemory>

.text:754BD9B0 kernel32.dll:$2D9B0 #2D9B0 <WriteProcessMemory>
```

```
003AE344  001C98A6  return to 001C98A6 from ???
003AE348  00000320
003AE34C  00400000
003AE350  038D6340  "MZ"
003AE354  00001000
003AE358  003AE640
003AE35C  0B8F2300
003AE360  70C4FDA4  clr.70C4FDA4
003AE364  003AEAAC  "<þÄplè:"
003AE368  00000014
003AE36C  003AE348
003AE370  001C98A6  return to 001C98A6 from ???
003AE374  003AE390  &"¼æ:"
003AE378  00630938
```

```
Address   Hex                                              ASCII
038D6340  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
038D6350  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
038D6360  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
038D6370  00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00  ................
038D6380  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
038D6390  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
038D63A0  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
038D63B0  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
038D63C0  64 7C 87 F9 20 1D E9 AA 20 1D E9 AA 20 1D E9 AA  d|.ù .éª .éª .éª
038D63D0  6D 3E F4 AA 21 1D E9 AA 73 3E F0 AA 22 1D E9 AA  m>ôª!.éªs>ðª".éª
038D63E0  20 1D E9 AA 2F 1D E9 AA 5B 01 E5 AA 21 1D E9 AA   .éª/.éª[.åª!.éª
038D63F0  A3 01 E7 AA 24 1D E9 AA C8 02 E3 AA 2B 1D E9 AA  £.çª$.éªÈ.ãª+.éª
```

```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
```

Here we save it.



remcos.exe - PID: 1356 - Module: kernel32.dll - Thread: Main Thread 700 -

```
754BD9B0    8BFF              mo
754BD9B2    55                pus
754BD9B3    8BEC              mov
754BD9B5    5D                pop
754BD9B6  ^ E9 1837FEFF       jmp
754BD9BB    3BF3              cmp
754BD9BD  ^ 0F84 2116FFFF     je
754BD9C3    385E 1A           cmp
754BD9C6  v 0F85 CA0D0100     jne
754BD9CC    FF76 14           pus
754BD9CF    FF15 A0054A75     ca
754BD9D5    64:A1 18000000    mov
754BD9DB    8B40 30           mov
754BD9DE    56                pus
754BD9DF    53                pus
754BD9E0    FF70 18           pus
754BD9E3    FF15 00064A75     ca
754BD9E9  ^ E9 F615FFFF       jmp
754BD9EE    8D45 F0           lea
754BD9F1    50                pus
754BD9F2    8D45 F4           lea
754BD9F5    50                pus
754BD9F6    68 00000002       pus
754BD9FB    FF75 FC           pus
754BD9FE    53                pus
754BD9FF    E8 B6E8FFFF       ca
754BDA04    3BC3              cmp
754BDA06  ^ 0F8D 3881FEFF     jg
754BDA0C  v E9 C23F0200       jmp
754BDA11    E8 5E3AFEFF       ca
754BDA16  v E9 47400200       jmp

edi=<kernel32.WriteProcessMemory>

.text:754BD9B0 kernel32.dll:$2D9B0 #2D9B0 <WriteProcessMem
```

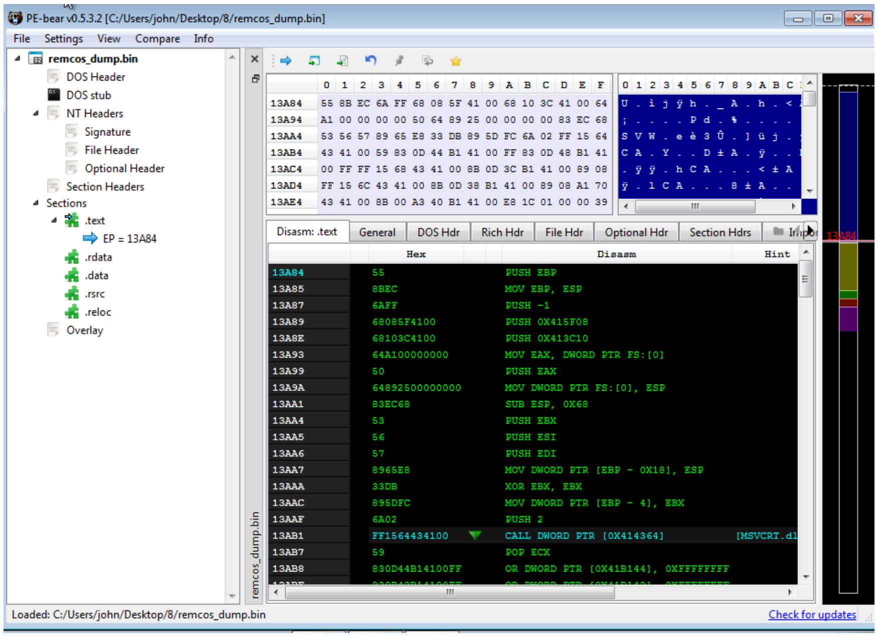
```
Address   Hex
03915F40  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03915F50  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03915F60  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03915F70  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03915F80  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03915F90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03915FA0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03915FB0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03915FC0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03915FD0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03915FE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03915FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
003AE368  00000014
003AE36C  003AE348
003AE370  001C98A6  return to 001C98A6 from ???
003AE374  003AE390  &"%æ:"
003AE378  00630938
```

Name	Date modified	Type	Size
remcos.exe	4/22/2020 7:34 AM	Application	438 KB
remcos_dump.bin	1/29/2022 5:01 AM	BIN File	256 KB

2 items

Now here we load the dump file in PE-bear to unmap it.



PE-bear v0.5.3.2 [C:/Users/john/Desktop/8/remcos_dump.bin]

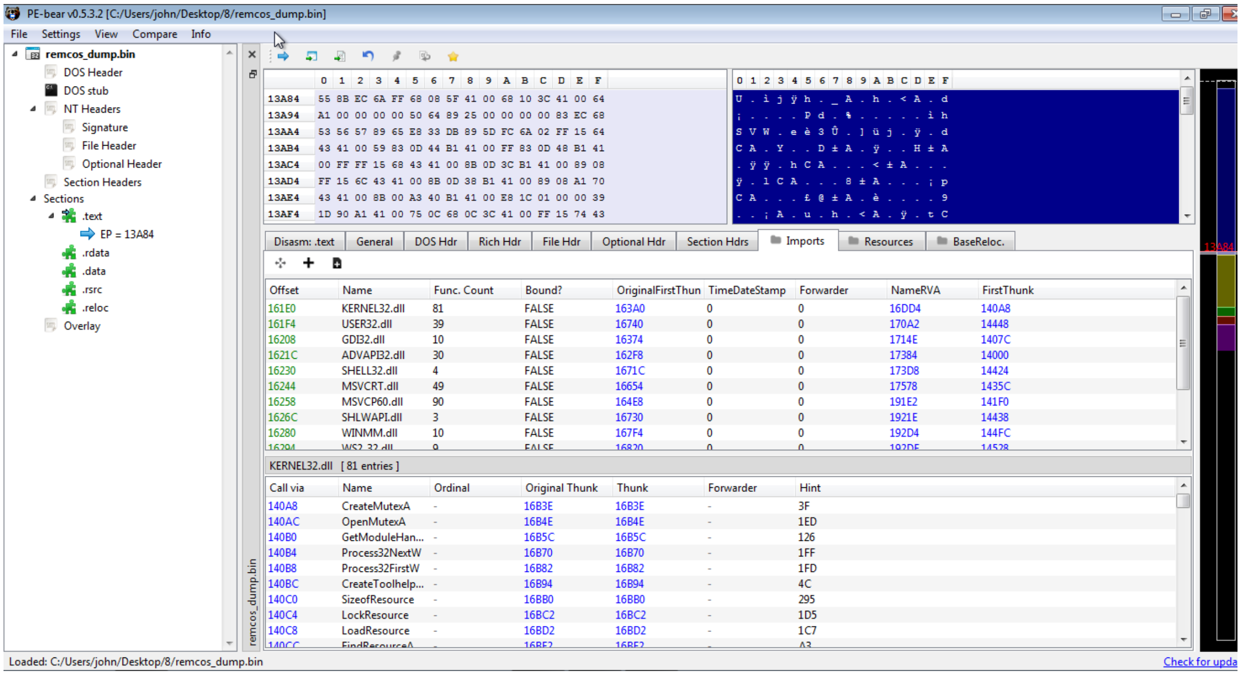
```
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0 1 2 3 4 5 6 7 8 9 A B C
13A84  55 8B EC 6A FF 68 08 5F 41 00 68 10 3C 41 00 64  U . ì j ÿ h . _ A . h . <
13A94  A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 68  ¡ . . . . P d . % . . . .
13AA4  53 56 57 89 65 E8 33 DB 89 5D FC 6A 02 FF 15 64  S V W . e è 3 Û . ] ü j .
13AB4  43 41 00 59 83 0D 44 B1 41 00 FF 83 0D 48 B1 41  C A . Y . . D ± A . ÿ . .
13AC4  00 FF FF 15 68 43 41 00 8B 0D 3C B1 41 00 89 08  . ÿ ÿ . h C A . . . < ± A
13AD4  FF 15 6C 43 41 00 8B 0D 38 B1 41 00 89 08 A1 70  ÿ . l C A . . . 8 ± A . .
13AE4  43 41 00 8B 00 A3 40 B1 41 00 E8 1C 01 00 00 39
```

```
         Hex                Disasm                                   Hint
13A84    55                 PUSH EBP
13A85    8BEC               MOV EBP, ESP
13A87    6AFF               PUSH -1
13A89    68085F4100         PUSH 0X415F08
13A8E    68103C4100         PUSH 0X413C10
13A93    64A100000000       MOV EAX, DWORD PTR FS:[0]
13A99    50                 PUSH EAX
13A9A    64892500000000     MOV DWORD PTR FS:[0], ESP
13AA1    83EC68             SUB ESP, 0X68
13AA4    53                 PUSH EBX
13AA5    56                 PUSH ESI
13AA6    57                 PUSH EDI
13AA7    8965E8             MOV DWORD PTR [EBP - 0X18], ESP
13AAA    33DB               XOR EBX, EBX
13AAC    895DFC             MOV DWORD PTR [EBP - 4], EBX
13AAF    6A02               PUSH 2
13AB1    FF1564434100       CALL DWORD PTR [0X414364]                [MSVCRT.dl
13AB7    59                 POP ECX
13AB8    830D44B14100FF     OR DWORD PTR [0X41B144], 0XFFFFFFFF
```

Loaded: C:/Users/john/Desktop/8/remcos_dump.bin

Check for updates

Here we can see that everything is in order so unmapping is not required ,Now we can analyse it with pestudio .



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F     0 1 2 3 4 5 6 7 8 9 A B C D E F
13A84   55 8B EC 6A FF 68 08 5F 41 00 68 10 3C 41 00 64    U . ì j ÿ h . _ A . h . < A . d
13A94   A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 68    ¡ . . . . P d . % . . . . . ì h
13AA4   53 56 57 89 65 E8 33 DB 89 5D FC 6A 02 FF 15 64    S V W . e è 3 Û . ] ü j . ÿ . d
13AB4   43 41 00 59 83 0D 44 B1 41 00 FF 83 0D 48 B1 41    C A . Y . . D ± A . ÿ . . H ± A
13AC4   00 FF FF 15 68 43 41 00 8B 0D 3C B1 41 00 89 08    . ÿ ÿ . h C A . . . < ± A . . .
13AD4   FF 15 6C 43 41 00 8B 0D 38 B1 41 00 89 08 A1 70    ÿ . l C A . . . 8 ± A . . . ¡ p
13AE4   43 41 00 8B 00 A3 40 B1 41 00 E8 1C 01 00 00 39    C A . . . £ @ ± A . è . . . . 9
13AF4   1D 90 A1 41 00 75 0C 68 0C 3C 41 00 FF 15 74 43    . . ¡ A . u . h . < A . ÿ . t C
```

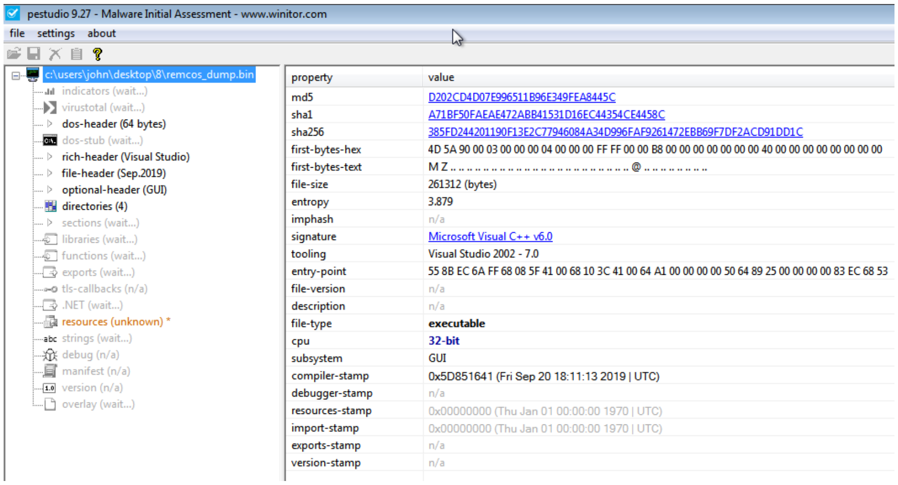
Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder	NameRVA	FirstThunk
161E0	KERNEL32.dll	81	FALSE	163A0	0	0	16DD4	140A8
161F4	USER32.dll	39	FALSE	16740	0	0	170A2	14448
16208	GDI32.dll	10	FALSE	16374	0	0	1714E	1407C
1621C	ADVAPI32.dll	30	FALSE	162F8	0	0	17384	14000
16230	SHELL32.dll	4	FALSE	1671C	0	0	173D8	14424
16244	MSVCRT.dll	49	FALSE	16654	0	0	17578	1435C
16258	MSVCP60.dll	90	FALSE	164E8	0	0	191E2	141F0
1626C	SHLWAPI.dll	3	FALSE	16730	0	0	1921E	14438
16280	WINMM.dll	10	FALSE	167F4	0	0	192D4	144FC
16294	WS2_32.dll	9	FALSE	16820	0	0	192DE	14528

KERNEL32.dll [81 entries]

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
140A8	CreateMutexA	-	16B3E	16B3E	-	3F
140AC	OpenMutexA	-	16B4E	16B4E	-	1ED
140B0	GetModuleHan...	-	16B5C	16B5C	-	126
140B4	Process32NextW	-	16B70	16B70	-	1FF
140B8	Process32FirstW	-	16B82	16B82	-	1FD
140BC	CreateToolhelp...	-	16B94	16B94	-	4C
140C0	SizeofResource	-	16BB0	16BB0	-	295
140C4	LockResource	-	16BC2	16BC2	-	1D5
140C8	LoadResource	-	16BD2	16BD2	-	1C7
140CC	FindResourceA	-	16BE2	16BE2	-	A3

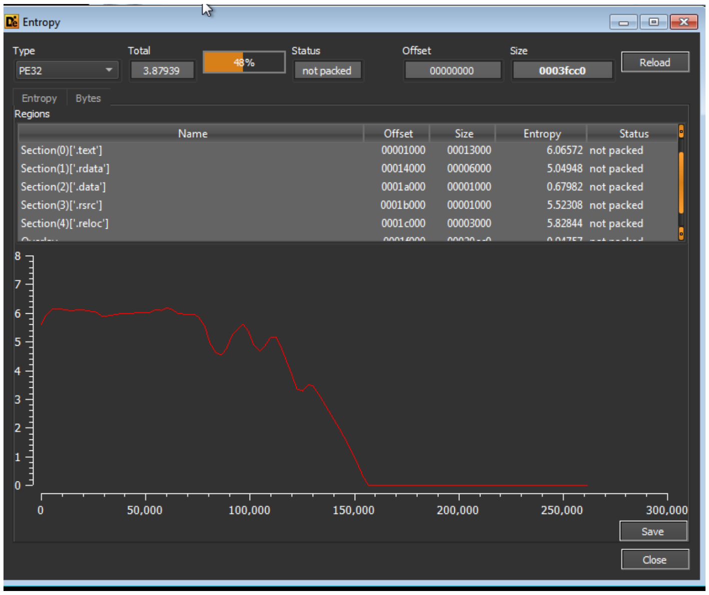
Loaded: C:/Users/john/Desktop/8/remcos_dump.bin

Here we loaded the sample in pestudio , here the entropy is 3.8 which means we have successfully unpacked it.



property	value
md5	D202CD4D07E996511B96E349FEA8445C
sha1	A71BF50FAEAE472ABB41531D16EC44354CE4458C
sha256	385FD244201190F13E2C77946084A34D996FAF9261472EBB69F7DF2ACD91DD1C
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	261312 (bytes)
entropy	3.879
imphash	n/a
signature	Microsoft Visual C++ v6.0
tooling	Visual Studio 2002 - 7.0
entry-point	55 8B EC 6A FF 68 08 5F 41 00 68 10 3C 41 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 68 53
file-version	n/a
description	n/a
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x5D851641 (Fri Sep 20 18:11:13 2019 | UTC)
debugger-stamp	n/a
resources-stamp	0x00000000 (Thu Jan 01 00:00:00 1970 | UTC)
import-stamp	0x00000000 (Thu Jan 01 00:00:00 1970 | UTC)
exports-stamp	n/a
version-stamp	n/a

Here also in Detect It Easy we can see that now we have successfully unpacked the sample.



Type: PE32
Total: 3.87939
48%
Status: not packed
Offset: 00000000
Size: 0003fcc0

Regions

Name	Offset	Size	Entropy	Status
Section(0)['.text']	00001000	00013000	6.06572	not packed
Section(1)['.rdata']	00014000	00006000	5.04948	not packed
Section(2)['.data']	0001a000	00001000	0.67982	not packed
Section(3)['.rsrc']	0001b000	00001000	5.52308	not packed
Section(4)['.reloc']	0001c000	00003000	5.82844	not packed
Overlay	0001f000	00020cc0	0.04757	not packed