

E8 10 3e = 1110 1000 0001 0000 0011 1110

55 push ebp

8B EC mov ebp,esp

83 EC 18 sub esp,18h

53 push ebx

C7 45 F4 03 00 00 00 mov dword ptr [ebp-0Ch],3

C7 45 FC 00 00 00 00 mov dword ptr [ebp-4],0

EB 09 jmp Stage2+20h (0445590h)

---------------------TROZO SALTADO------------------------------------------

8B 45 FC mov eax,dword ptr [ebp-4]

0044558A 83 C0 01 add eax,1

0044558D 89 45 FC mov dword ptr [ebp-4],eax

----------------------------------------------------------------------------

83 7D FC 03 cmp dword ptr [ebp-4],3

7D 14 jge Stage2+3Ah (04455AAh)

8B 4D FC mov ecx,dword ptr [ebp-4]

8D 54 8D E8 lea edx,[ebp+ecx\*4-18h]

52 push edx

B9 B0 6B 53 00 mov ecx,offset std::cin (0536BB0h)

E8 C8 0F 00 00 call std::basic\_istream<char,std::char\_traits<char> >::operator>> (0446570h)

55 push ebp

8B EC mov ebp,esp

6A FF push 0FFFFFFFFh

68 C0 FB 4F 00 push 4FFBC0h

64 A1 00 00 00 00 mov eax,dword ptr fs:[00000000h]

50 push eax

64 89 25 00 00 00 00 mov dword ptr fs:[0],esp

51 push ecx

83 EC 4C sub esp,4Ch

53 push ebx

56 push esi

57 push edi

89 65 F0 mov dword ptr [ebp-10h],esp

89 4D EC mov dword ptr [ebp-14h],ecx

C7 45 E8 00 00 00 00 mov dword ptr [ebp-18h],0

6A 00 push 0

8B 45 EC mov eax,dword ptr [ebp-14h]

50 push eax

8D 4D C4 lea ecx,[ebp-3Ch]

E8 56 FE FF FF call std::basic\_istream<char,std::char\_traits<char> >::sentry::sentry (0446400h)

55 push ebp

8B EC mov ebp,esp

6A FF push 0FFFFFFFFh

68 78 FB 4F 00 push 4FFB78h

64 A1 00 00 00 00 mov eax,dword ptr fs:[00000000h]

50 push eax

64 89 25 00 00 00 00 mov dword ptr fs:[0],esp

51 push ecx

89 4D F0 mov dword ptr [ebp-10h],ecx

8B 45 08 mov eax,dword ptr [ebp+8]

50 push eax

8B 4D F0 mov ecx,dword ptr [ebp-10h]

E8 58 FF FF FF call std::basic\_istream<char,std::char\_traits<char> >::\_Sentry\_base::\_Sentry\_base (0446380h)

55 push ebp

8B EC mov ebp,esp

83 EC 10 sub esp,10h

89 4D FC mov dword ptr [ebp-4],ecx

8B 45 FC mov eax,dword ptr [ebp-4]

8B 4D 08 mov ecx,dword ptr [ebp+8]

89 08 mov dword ptr [eax],ecx

8B 55 FC mov edx,dword ptr [ebp-4]

8B 02 mov eax,dword ptr [edx]

89 45 F8 mov dword ptr [ebp-8],eax

8B 4D F8 mov ecx,dword ptr [ebp-8]

8B 11 mov edx,dword ptr [ecx]

8B 4D F8 mov ecx,dword ptr [ebp-8]

03 4A 04 add ecx,dword ptr [edx+4]

E8 E7 ED FF FF call std::basic\_ios<char,std::char\_traits<char> >::rdbuf (0445190h)

55 push ebp

8B EC mov ebp,esp

51 push ecx

89 4D FC mov dword ptr [this],ecx

8B 45 FC mov eax,dword ptr [this]

8B 40 38 mov eax,dword ptr [eax+38h]

8B E5 mov esp,ebp

5D pop ebp

C3 ret

85 C0 test eax,eax

74 28 je std::basic\_istream<char,std::char\_traits<char> >::\_Sentry\_base::\_Sentry\_base+55h (04463D5h)

8B 45 FC mov eax,dword ptr [ebp-4]

8B 08 mov ecx,dword ptr [eax]

89 4D F4 mov dword ptr [ebp-0Ch],ecx

8B 55 F4 mov edx,dword ptr [ebp-0Ch]

8B 02 mov eax,dword ptr [edx]

8B 4D F4 mov ecx,dword ptr [ebp-0Ch]

03 48 04 add ecx,dword ptr [eax+4]

E8 CB ED FF FF call std::basic\_ios<char,std::char\_traits<char> >::rdbuf (0445190h)

55 push ebp

8B EC mov ebp,esp

51 push ecx

89 4D FC mov dword ptr [this],ecx

8B 45 FC mov eax,dword ptr [this]

8B 40 38 mov eax,dword ptr [eax+38h]

8B E5 mov esp,ebp

5D pop ebp

C3 ret

89 45 F0 mov dword ptr [ebp-10h],eax

8B 4D F0 mov ecx,dword ptr [ebp-10h]

8B 11 mov edx,dword ptr [ecx]

8B 4D F0 mov ecx,dword ptr [ebp-10h]

8B 42 04 mov eax,dword ptr [edx+4]

FF D0 call eax

0044F220 55 push ebp

0044F221 8B EC mov ebp,esp

0044F223 51 push ecx

0044F224 89 4D FC mov dword ptr [this],ecx

0044F227 8B 45 FC mov eax,dword ptr [this]

0044F22A 83 78 4C 00 cmp dword ptr [eax+4Ch],0

0044F22E 74 0F je std::basic\_filebuf<char,std::char\_traits<char> >::\_Lock+1Fh (044F23Fh)

0044F230 8B 4D FC mov ecx,dword ptr [this]

0044F233 8B 51 4C mov edx,dword ptr [ecx+4Ch]

0044F236 52 push edx

0044F237 E8 64 61 07 00 call \_lock\_file (04C53A0h)

0044F23C 83 C4 04 add esp,4

0044F23F 8B E5 mov esp,ebp

0044F241 5D pop ebp

0044F242 C3 ret

004C53A0 8B FF mov edi,edi

004C53A2 55 push ebp

004C53A3 8B EC mov ebp,esp

004C53A5 51 push ecx

004C53A6 8B 45 08 mov eax,dword ptr [stream]

004C53A9 50 push eax

004C53AA 8D 4D FC lea ecx,[ebp-4]

004C53AD E8 DE 2D FE FF call \_\_crt\_stdio\_stream::\_\_crt\_stdio\_stream (04A8190h)

004A8190 8B FF mov edi,edi

004A8192 55 push ebp

004A8193 8B EC mov ebp,esp

004A8195 51 push ecx

004A8196 89 4D FC mov dword ptr [this],ecx

004A8199 8B 45 FC mov eax,dword ptr [this]

004A819C 8B 4D 08 mov ecx,dword ptr [stream]

004A819F 89 08 mov dword ptr [eax],ecx

004A81A1 8B 45 FC mov eax,dword ptr [this]

004A81A4 8B E5 mov esp,ebp

004A81A6 5D pop ebp

004A81A7 C2 04 00 ret 4

004C53B2 8B C8 mov ecx,eax

004C53B4 E8 97 32 FE FF call \_\_crt\_stdio\_stream::operator->

(04A8650h)

004C53B9 83 C0 20 add eax,20h

004C53BC 50 push eax

004A8650 8B FF mov edi,edi

004A8652 55 push ebp

004A8653 8B EC mov ebp,esp

004A8655 51 push ecx

004A8656 89 4D FC mov dword ptr [this],ecx

004A8659 8B 45 FC mov eax,dword ptr [this]

004A865C 8B 00 mov eax,dword ptr [eax]

004A865E 8B E5 mov esp,ebp

004A8660 5D pop ebp

004A8661 C3 ret

004C53B9 83 C0 20 add eax,20h

004C53BC 50 push eax

004C53BD FF 15 34 50 50 00 call dword ptr [\_\_imp\_\_EnterCriticalSection@4 (0505034h)]

004C53C3 8B E5 mov esp,ebp

004C53C5 5D pop ebp

004C53C6 C3 ret

7722E570 8B FF mov edi,edi

7722E572 55 push ebp

7722E573 8B EC mov ebp,esp

7722E575 83 E4 F8 and esp,0FFFFFFF8h

7722E578 8B 4D 08 mov ecx,dword ptr [ebp+8]

7722E57B 64 8B 15 18 00 00 00 mov edx,dword ptr fs:[18h]

7722E582 8D 41 04 lea eax,[ecx+4]

7722E585 F0 0F BA 30 00 lock btr dword ptr [eax],0

7722E58A 73 15 jae 7722E5A1

7722E58C 8B 42 24 mov eax,dword ptr [edx+24h]

7722E58F 89 41 0C mov dword ptr [ecx+0Ch],eax

7722E592 33 C0 xor eax,eax

7722E594 C7 41 08 01 00 00 00 mov dword ptr [ecx+8],1

7722E59B 8B E5 mov esp,ebp

7722E59D 5D pop ebp

7722E59E C2 04 00 ret 4

004C53C3 8B E5 mov esp,ebp

004C53C5 5D pop ebp

004C53C6 C3 ret

0044F23C 83 C4 04 add esp,4

0044F23F 8B E5 mov esp,ebp

0044F241 5D pop ebp

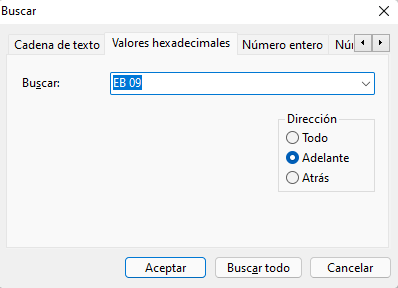
0044F242 C3 ret

004463D5 8B 45 FC mov eax,dword ptr [ebp-4]

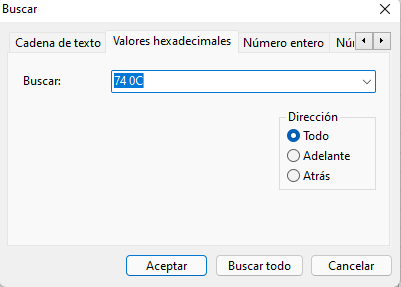
004463D8 8B E5 mov esp,ebp

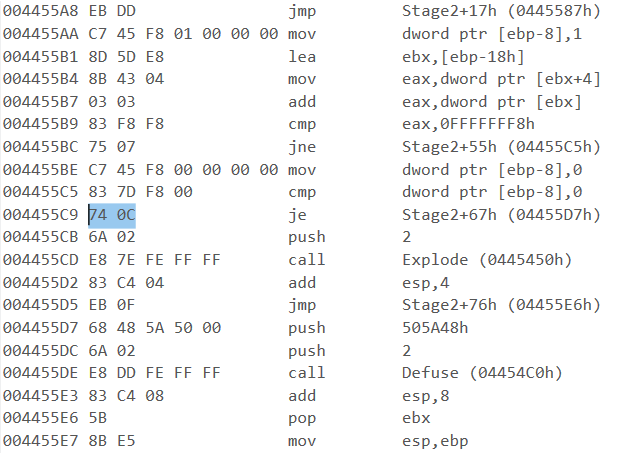
004463DA 5D pop ebp

004463DB C2 04 00 ret 4



8B 45 FC 83 C0 = 1000 1011 / 0100 0101 / 1111 1100 / 1000 0011 / 1100 0000





---------------------------------Cadena que desactivaba la bomba-------------------------------------

00445570 55 push ebp **// r6**

00445571 8B EC mov ebp,esp **// r6 y r7 apuntan a lo mismo**

00445573 83 EC 18 sub esp,18h **// r7 se mueve 24 posiciones arriba**

00445576 53 push ebx

00445577 C7 45 F4 03 00 00 00 mov dword ptr [ebp-0Ch],3 **// el contenido de lo que apunta r6 subido 12 posiciones arriba guarda el valor 3 en hexadecimal**

0044557E C7 45 FC 00 00 00 00 mov dword ptr [ebp-4],0 **// el contenido de lo que apunta r6 subido 16 posiciones arriba (con respecto a la posición inicial) guarda el valor 3 en hexadecimal**

00445585 EB 09 jmp Stage2+20h (0445590h) **// SALTO 1**

00445587 8B 45 FC mov eax,dword ptr [ebp-4]

0044558A 83 C0 01 add eax,1

0044558D 89 45 FC mov dword ptr [ebp-4],eax

00445590 83 7D FC 03 cmp dword ptr [ebp-4],3 **// CAÍDA 1**

00445594 7D 14 jge Stage2+3Ah (04455AAh) **// >= en magnitudes con signo (si el contenido de lo que apunta r6 subido 20 posiciones arriba (con respecto a la posición inicial) es mayor que 3 en hexadecimal). SALTO 2**

00445596 8B 4D FC mov ecx,dword ptr [ebp-4]

00445599 8D 54 8D E8 lea edx,[ebp+ecx\*4-18h]

0044559D 52 push edx

0044559E B9 B0 6B 53 00 mov ecx,offset std::cin (0536BB0h)

004455A3 E8 C8 0F 00 00 call

std::basic\_istream<char,std::char\_traits<char> >::operator>> (0446570h)

004455A8 EB DD jmp Stage2+17h (0445587h)

004455AA C7 45 F8 01 00 00 00 mov dword ptr [ebp-8],1 **// CAÍDA 2**

004455B1 8D 5D E8 lea ebx,[ebp-18h]

004455B4 8B 43 04 mov eax,dword ptr [ebx+4]

004455B7 03 03 add eax,dword ptr [ebx]

004455B9 83 F8 F8 cmp eax,0FFFFFFF8h

004455BC 75 07 jne Stage2+55h (04455C5h)

004455BE C7 45 F8 00 00 00 00 mov dword ptr [ebp-8],0

004455C5 83 7D F8 00 cmp dword ptr [ebp-8],0

004455C9 EB 0C jmp Stage2+67h (04455D7h)