Blizzhackers

Home of the Dupe since 2001

Login Register FAQ Search

Join us on IRC: #bh@irc.synirc.net (or Mibbit Web IRC)

It is currently Sat Jun 23, 2018 12:55 pm

View unanswered posts | View active topics

Board index » **Diablo II** » **Diablo II Hacking Development** All times are UTC [DST]

Diablo II 1.14b Pointers - Patches - Functions - Structures

Moderator: Diablo Mods

newtopic postreply **Page 1 of 3** [37 posts] **Go to page 1, 2, 3 Next**

Print view **Previous topic | Next topic**

Author	Message
77920	**Post subject:** Diablo II 1.14b Pointers - Patches - Functions - Structures **Posted:** Thu Apr 07, 2016 9:51 pm

User Gold

User

Joined: Mon Dec 14, 2009 1:40 pm

Code: Select all

```
{PatchBytes, GetOffset(0x661C5), (DWORD)ShiftClickFarcast, 1 }, //Updated 1.14b //004661C5-BASE
{PatchBytes, GetOffset(0xA6B96), (DWORD)LeftClickAllSkills, 1 }, //Updated 1.14b //004A6B96-BASE
{PatchCall, GetOffset(0x4A9C2), (DWORD)GameLoop_STUB,6 }, //Updated 1.14b //0044A9C2-BASE
{PatchJmp,  GetOffset(0x67AE0), (DWORD)GameDraw_STUB, 5 }, //Updated 1.14b //00467AE0-BASE
{PatchJmp,  GetOffset(0x564F3), (DWORD)GameDrawAutomapInfo_STUB, 5 }, //Updated 1.14b //004564F3-BASE
{PatchCall, GetOffset(0x55F00), (DWORD)GameDrawUnitBlob_STUB,5 }, //Updated 1.14b //00455F00-BASE
{PatchJmp,  GetOffset(0x74228), (DWORD)SendPacketIntercept_STUB, 6}, //Updated 1.14b //00474228-BASE
{PatchCall, GetOffset(0x5AF94), (DWORD)ReceivePacketIntercept_STUB,5 }, //Updated 1.14b 0045AF94-BASE
{PatchCall, GetOffset(0x7864F), (DWORD)GameInput_Interception, 5}, //Updated 1.14b //0047864F-BASE
{PatchCall, GetOffset(0xC33A6), (DWORD)CreateMissile_STUB,5}, //Updated 1.14b //004C33A6-BASE
```

```
{PatchCall, GetOffset(0x414BE), (DWORD)NextGameNamePatch, 5}, //Updated 1.14b // 004414BE-BASE
{PatchCall, GetOffset(0x414F9), (DWORD)NextGamePasswordPatch, 5}, //Updated 1.14b // 004414F9-BASE
{PatchCall, GetOffset(0x4170C), (DWORD)NextGameNamePatch, 5}, //Updated 1.14b //0044170C-BASE
{PatchCall, GetOffset(0x41747), (DWORD)NextGamePasswordPatch, 5}, //Updated 1.14b //00441747-BASE
{PatchCall,GetOffset(0x544E2), (DWORD)AddShrine_STUB, 6}, //Updated 1.14b //004544E2-BASE
{PatchCall,GetOffset(0x71ED4), (DWORD)OverrideShrine_STUB, 7}, //Updated 1.14b //00453177-BASE
{PatchJmp,  GetOffset(0x21DB56), (DWORD)WeatherSTUB,    5, }, //Updated 1.14b //0061DB56-BASE
{PatchCall, GetOffset(0x4A658),  (DWORD)GameFailToJoin_STUB, 6 }, //Updated 1.14b //0044A658-BASE
{PatchCall,GetOffset(0xFFAD0),  (DWORD)MonsterLifeBarNameSTUB   ,6}, //Updated 1.14b //004FFAD0-BASE
{PatchCall,GetOffset(0x450B1),   (DWORD)OnMCPPacketReceivedSTUB, 5}, //Updated 1.14b //004450B1-BASE
{PatchCall,GetOffset(0x414A2), (DWORD)CreateGameBoxSTUB, 5}, //Updated 1.14b //004414A2-BASE
{PatchCall,GetOffset(0x3E6A9),   (DWORD)DestroyGameList,    5}, //Updated 1.14b //0043E6A9-BASE
```

Code: Select all

```
FUNCPTR(BNCLIENT, SendBNMessage, void __fastcall, (LPSTR lpMessage), 0x118B70) //Updated 1.14b //00518B70-BASE
FUNCPTR(D2CLIENT, GetSelectedUnit, UnitAny * __stdcall, (), 0x63250)//Updated 1.14b //00463250-BASE
FUNCPTR(D2CLIENT, GetMonsterTxt, MonsterTxt * FASTCALL, (DWORD MonsterNumber), 0x4D5D2)  //Updated 1.14b //0044D5D2-BASE
FUNCPTR(D2CLIENT, PrintGameString, void __fastcall, (wchar_t *wMessage, int nColor), 0x9AB40) //Updated 1.14b //0049AB40-BASE
FUNCPTR(D2CLIENT, PrintPartyString, void __fastcall, (wchar_t *wMessage, int nColor), 0x9AD60)//Updated 1.14b //0049AD60-BASE
FUNCPTR(D2CLIENT, GetDifficulty, BYTE __stdcall, (), 0x49240)//Updated 1.14b //00449240-BASE
FUNCPTR(D2CLIENT, GetAutomapSize, DWORD __stdcall, (void), 0x55E20) //Updated 1.14b //00455E20-BASE
FUNCPTR(D2CLIENT, GetGameInfo, GameStructInfo *__stdcall, (), 0x46C60) //Updated 1.14b //00446C60-BASE
FUNCPTR(D2CLIENT, NewAutomapCell, AutomapCell * __fastcall, (), 0x532B0) //Updated 1.14b //004532B0-BASE
FUNCPTR(D2CLIENT, AddAutomapCell, void __fastcall, (AutomapCell *aCell, AutomapCell **node), 0x53190) //Updated 1.14b //00453190-BASE
FUNCPTR(D2CLIENT, RevealAutomapRoom, void __stdcall, (Room1 *pRoom1, DWORD dwClipFlag, AutomapLayer *aLayer), 0x545D0) //Updated 1.14b //004545D0-BASE
FUNCPTR(D2CLIENT, InitAutomapLayer_I, AutomapLayer* __fastcall, (DWORD nLayerNo), 0x543E0)//Updated 1.14b //004543E0-BASE
FUNCPTR(D2CLIENT, GetMonsterOwner, DWORD __fastcall, (DWORD nMonsterId), 0x747D0) //Updated 1.14b //004747D0-BASE
FUNCPTR(D2CLIENT, GetUiVar_I, DWORD __fastcall, (DWORD dwVarNo), 0x4EEF0) //Updated 1.14b //0044EEF0-BASE
FUNCPTR(D2CLIENT, CalculateShake, void __stdcall, (DWORD *dwPosX, DWORD *dwPosY), 0x11E4E0)//Updated 1.14b //0051E4E0-BASE
```

Last edited by 77920 on Tue May 17, 2016 1:59 am, edited 14 times in total.

Top profile

thaison **Post subject:** Re: Diablo II 1.14b Pointers - Patches - Functions - Structu **Posted:** Mon Apr 11, 2016 3:41 pm

User

Joined: Sat Mar 26, 2016 1:48 pm

I'll get you one hand , i have to find the code here and not copied anywhere. Thank watched .

Code: Select all

```
D2PTR(Game, CharInfo_I, 0xA41D0)
D2PTR(Game, DrawHook_I, 0x52968)
D2PTR(Game, InputCall_I, 0x744E0)

D2VAR(Game, ScreenSizeX, DWORD, 0x310F48)
D2VAR(Game, ScreenSizeY, DWORD, 0x310F4C)
D2VAR(Game, Ping, DWORD, 0x39852C)
D2VAR(Game, FPS, DWORD, 0x3B3418)
D2VAR(Game, Skip, DWORD, 0x398538)
D2VAR(Game, sgptDataTables, sgptDataTable*, 0x340D78)
D2VAR(Game, MonsterLifeNamePatch1, UnitAny, 0x30CBC0)
D2VAR(Game, MonsterLifeNamePatch2, UnitAny, 0x30CBC7)
D2VAR(Game, PlayerUnitList, LPROSTERUNIT, 0x7B709C)
D2VAR(Game, MouseX, int, 0x39A8E4)// 00842F5C - BASE
D2VAR(Game, MouseY, int, 0x39A8E0)// 00842F58 - BASE
D2VAR(Game, MouseOffsetX, int, 0x39D294)
D2VAR(Game, MouseOffsetY, int, 0x39D290)
D2VAR(Game, MouseOffsetZ, int, 0x39D29C)
D2VAR(Game, FocusedControl, LPCONTROL, 0x7CD654)
D2VAR(Game, PlayersComm, BYTE, 0x47BDB0)

D2FUNC(Game, D2PrintLineOnTextBox, void, __fastcall, (void* screen, char* s, DWORD color), 0xF8D80)//PlugY
D2FUNC(Game, D2CreateTextBox, void*, __stdcall, (DWORD* data), 0xF6A30)//PlugY
```

Top profile

77920 **Post subject:** Re: Diablo II 1.14b Pointers - Patches - Functions - Structu **Posted:** Tue Apr 12, 2016 10:39 pm

User Gold

User

Joined: Mon Dec 14, 2009 1:40 pm

> **thaison » Mon Apr 11, 2016 9:41 am** wrote:
>
> I'll get you one hand , i have to find the code here and not copied anywhere. Thank watched .
>
> **Code:** Select all
>
> ```
> D2PTR(Game, CharInfo_I, 0xA41D0)
> D2PTR(Game, DrawHook_I, 0x52968)
> D2PTR(Game, InputCall_I, 0x744E0)
>
> D2VAR(Game, ScreenSizeX, DWORD, 0x310F48)
> D2VAR(Game, ScreenSizeY, DWORD, 0x310F4C)
> D2VAR(Game, Ping, DWORD, 0x39852C)
> D2VAR(Game, FPS, DWORD, 0x3B3418)
> D2VAR(Game, Skip, DWORD, 0x398538)
> D2VAR(Game, sgptDataTables, sgptDataTable*, 0x340D78)
> D2VAR(Game, MonsterLifeNamePatch1, UnitAny, 0x30CBC0)
> D2VAR(Game, MonsterLifeNamePatch2, UnitAny, 0x30CBC7)
> D2VAR(Game, PlayerUnitList, LPROSTERUNIT, 0x7B709C)
> D2VAR(Game, MouseX, int, 0x39A8E4)// 00842F5C - BASE
> D2VAR(Game, MouseY, int, 0x39A8E0)// 00842F58 - BASE
> D2VAR(Game, MouseOffsetX, int, 0x39D294)
> D2VAR(Game, MouseOffsetY, int, 0x39D290)
> D2VAR(Game, MouseOffsetZ, int, 0x39D29C)
> D2VAR(Game, FocusedControl, LPCONTROL, 0x7CD654)
> D2VAR(Game, PlayersComm, BYTE, 0x47BDB0)
>
> D2FUNC(Game, D2PrintLineOnTextBox, void, __fastcall, (void* screen, char* s, DWORD color), 0xF8D80)//PlugY
> D2FUNC(Game, D2CreateTextBox, void*, __stdcall, (DWORD* data), 0xF6A30)//PlugY
> ```

I'm just curious have you tested all these to confirm they work for 1.14b cause I don't really understand what you mean by "i'll get you one hand, I have to find the code here and not copied anywhere. Thank watched."

Top profile

thaison **Post subject:** Re: Diablo II 1.14b Pointers - Patches - Functions - Structu **Posted:** Wed Apr 13, 2016 1:17 pm

User

User

Joined: Sat Mar 26, 2016 1:48 pm

> 77920 » Tue Apr 12, 2016 9:39 pm wrote:
>
> > thaison » Mon Apr 11, 2016 9:41 am wrote:
> >
> > I'll get you one hand , i have to find the code here and not copied anywhere. Thank watched .
> >
> > **Code:** Select all
> >
> > ```
> > D2PTR(Game, CharInfo_I, 0xA41D0)
> > D2PTR(Game, DrawHook_I, 0x52968)
> > D2PTR(Game, InputCall_I, 0x744E0)
> >
> > D2VAR(Game, ScreenSizeX, DWORD, 0x310F48)
> > D2VAR(Game, ScreenSizeY, DWORD, 0x310F4C)
> > D2VAR(Game, Ping, DWORD, 0x39852C)
> > D2VAR(Game, FPS, DWORD, 0x3B3418)
> > D2VAR(Game, Skip, DWORD, 0x398538)
> > D2VAR(Game, sgptDataTables, sgptDataTable*, 0x340D78)
> > D2VAR(Game, MonsterLifeNamePatch1, UnitAny, 0x30CBC0)
> > D2VAR(Game, MonsterLifeNamePatch2, UnitAny, 0x30CBC7)
> > D2VAR(Game, PlayerUnitList, LPROSTERUNIT, 0x7B709C)
> > D2VAR(Game, MouseX, int, 0x39A8E4)// 00842F5C - BASE
> > D2VAR(Game, MouseY, int, 0x39A8E0)// 00842F58 - BASE
> > D2VAR(Game, MouseOffsetX, int, 0x39D294)
> > D2VAR(Game, MouseOffsetY, int, 0x39D290)
> > D2VAR(Game, MouseOffsetZ, int, 0x39D29C)
> > D2VAR(Game, FocusedControl, LPCONTROL, 0x7CD654)
> > D2VAR(Game, PlayersComm, BYTE, 0x47BDB0)
> >
> > D2FUNC(Game, D2PrintLineOnTextBox, void, __fastcall, (void* screen, char* s, DWORD color),
> > 0xF8D80)//PlugY
> > ```
>
> I'm just curious have you tested all these to confirm they work for 1.14b cause I don't really understand what you mean by "i'll get you one hand, I have to find the code here and not copied anywhere. Thank watched."

I ran it on my mod , it works out results

Top profile

77920

Post subject: Re: Diablo II 1.14b Pointers - Patches - Functions - Structu

Posted: Wed Apr 13, 2016 1:46 pm

User Gold

User

Joined: Mon Dec 14, 2009 1:40 pm

> thaison » Wed Apr 13, 2016 7:17 am wrote:
>
> > 77920 » Tue Apr 12, 2016 9:39 pm wrote:
> >
> > > thaison » Mon Apr 11, 2016 9:41 am wrote:
> > >
> > > I'll get you one hand , i have to find the code here and not copied anywhere. Thank watched .
> > >
> > > **Code:** Select all
> > >
> > > ```
> > > D2PTR(Game, CharInfo_I, 0xA41D0)
> > > D2PTR(Game, DrawHook_I, 0x52968)
> > > D2PTR(Game, InputCall_I, 0x744E0)
> > >
> > > D2VAR(Game, ScreenSizeX, DWORD, 0x310F48)
> > > D2VAR(Game, ScreenSizeY, DWORD, 0x310F4C)
> > > D2VAR(Game, Ping, DWORD, 0x39852C)
> > > D2VAR(Game, FPS, DWORD, 0x3B3418)
> > > D2VAR(Game, Skip, DWORD, 0x398538)
> > > D2VAR(Game, sgptDataTables, sgptDataTable*, 0x340D78)
> > > D2VAR(Game, MonsterLifeNamePatch1, UnitAny, 0x30CBC0)
> > > D2VAR(Game, MonsterLifeNamePatch2, UnitAny, 0x30CBC7)
> > > D2VAR(Game, PlayerUnitList, LPROSTERUNIT, 0x7B709C)
> > > D2VAR(Game, MouseX, int, 0x39A8E4)// 00842F5C - BASE
> > > D2VAR(Game, MouseY, int, 0x39A8E0)// 00842F58 - BASE
> > > D2VAR(Game, MouseOffsetX, int, 0x39D294)
> > > D2VAR(Game, MouseOffsetY, int, 0x39D290)
> > > D2VAR(Game, MouseOffsetZ, int, 0x39D29C)
> > > D2VAR(Game, FocusedControl, LPCONTROL, 0x7CD654)
> > > D2VAR(Game, PlayersComm, BYTE, 0x47BDB0)
> > >
> > > D2FUNC(Game, D2PrintLineOnTextBox, void, __fastcall, (void* screen, char* s, DWORD color),
> > > ```

> > I'm just curious have you tested all these to confirm they work for 1.14b cause I don't really understand what you mean by "i'll get you one hand, I have to find the code here and not copied anywhere. Thank watched."
>
> I ran it on my mod , it works out results

u Sure? #2 patch you posted 0070CBC7 doesn't exist in 1.14b executable...

Image http://upload.teamihpk.net/files/monsterpatch12.png

```
1.13d was
VARPTR(D2CLIENT, MonsterLifeNamePatch1, UnitAny, 0xEE49C)
VARPTR(D2CLIENT, MonsterLifeNamePatch2, UnitAny, 0xEE4A0)

1.14b
VARPTR(D2CLIENT, MonsterLifeNamePatch1, UnitAny, 0x3212E0) //Updated 1.14b //007212E0-BASE
VARPTR(D2CLIENT, MonsterLifeNamePatch2, UnitAny, 0x3212E4) //Updated 1.14b //007212E4-BASE
```

Top profile

thaison | **Post subject:** Re: Diablo II 1.14b Pointers - Patches - Functions - Structu | **Posted:** Wed Apr 13, 2016 2:13 pm

User

User

Joined: Sat Mar 26, 2016 1:48 pm

> 77920 » Wed Apr 13, 2016 12:46 pm wrote:
>
> > thaison » Wed Apr 13, 2016 7:17 am wrote:
> >
> > > 77920 » Tue Apr 12, 2016 9:39 pm wrote:

> > > I'm just curious have you tested all these to confirm they work for 1.14b cause I don't really understand what you mean by "i'll get you one hand, I have to find the code here and not copied anywhere. Thank watched."
> >
> > I ran it on my mod , it works out results
>
> u Sure? #2 patch you posted 0070CBC7 doesn't exist in 1.14b executable...
>
> Image http://upload.teamihpk.net/files/monsterpatch12.png
>
> 1.13d was
> VARPTR(D2CLIENT, MonsterLifeNamePatch1, UnitAny, 0xEE49C)
> VARPTR(D2CLIENT, MonsterLifeNamePatch2, UnitAny, 0xEE4A0)
>
> 1.14b
> VARPTR(D2CLIENT, MonsterLifeNamePatch1, UnitAny, 0x3212E0) //Updated 1.14b //007212E0-BASE
> VARPTR(D2CLIENT, MonsterLifeNamePatch2, UnitAny, 0x3212E4) //Updated 1.14b //007212E4-BASE

thank you for finding bugs in my code, I 'll fix soon

Top profile

77920

Post subject: Re: Diablo II 1.14b Pointers - Patches - Functions - Structu

Posted: Wed Apr 13, 2016 2:16 pm

User Gold

User

Joined: Mon Dec 14, 2009 1:40 pm

> thaison » Wed Apr 13, 2016 8:13 am wrote:
>
> > 77920 » Wed Apr 13, 2016 12:46 pm wrote:
> >
> > > thaison » Wed Apr 13, 2016 7:17 am wrote:

> > > I ran it on my mod , it works out results
> >
> > u Sure? #2 patch you posted 0070CBC7 doesn't exist in 1.14b executable...
> >
> > Image
> >
> > 1.13d was
> > VARPTR(D2CLIENT, MonsterLifeNamePatch1, UnitAny, 0xEE49C)
> > VARPTR(D2CLIENT, MonsterLifeNamePatch2, UnitAny, 0xEE4A0)
> >
> > 1.14b
> > VARPTR(D2CLIENT, MonsterLifeNamePatch1, UnitAny, 0x3212E0) //Updated 1.14b //007212E0-BASE
> > VARPTR(D2CLIENT, MonsterLifeNamePatch2, UnitAny, 0x3212E4) //Updated 1.14b //007212E4-BASE
>
> thank you for finding bugs in my code, I 'll fix soon

Well with what little I know... that's why i was questioning it. Glad I could help.

Top profile

whisty

Post subject: Re: Diablo II 1.14b Pointers - Patches - Functions - Structu **Posted:** Wed Apr 13, 2016 6:30 pm

User

User

Joined: Sun Sep 04, 2011 10:07 pm

One thing to do would be to fix those erroneous definitions that have been used since as far as 1.10f patch. Bad struct defs, misguiding and/or plain wrong function names, incorrect args, etc. For example D2WIN_GetTextWidthFileNo is just plain wrong, the third arg actually outputs the height, no idea where the fileno idea was taken from. I called this function D2WIN_GetTextDimensions in my code. The fun thing is I've seen some code here use this function, and then manually getting the height via some hardcoded cases based on used font & what not

~~The last arg of D2WIN_DrawText defines how the text will be aligned. Again I've seen codes on here manually centering text.~~ (nvm that, confused it with another function). And hell there's so many examples like this one I could come up with. But as long as it works eh?

Top profile

Vampirewolve

Post subject: Re: Diablo II 1.14b Pointers - Patches - Functions - Structu

Posted: Wed Apr 13, 2016 7:27 pm

User

User

Joined: Tue Mar 01, 2005 8:31 pm

Most definitions are just copypasted since d2hackit, mousepads maphack, stings maphack and so on.

IE Monsterlifenamepatch
They found a unitany variable and gave them the tag for the the used patch.
SocketProtectOriginal is another example.

DLRG is also a good example.

You could have a look at the pointer headers and find some pointers 2 or even 3 times. You example is also named GetTextSize.

Another example is "GetUnitfromId_I" aka "Clienthashtable". When check what's calling the RemoveUnit function you find 2 Tableoffsets, when you look what's calling those functions you see one parameter is the UnitID the other is the Type. Those tables are typespecific! You could also find that out when you look at the AddUnitfunction.

A good thing is Blizzard did a good cleanup on under-/unused d2client functions meaning now you need to understand the ASM code. The "GetUnit" / "FindUnit" function is a good example.
~~The tables still exists but you need to write an Inline Asmfunction/rewrite the GetUnit function yourself or hook the Add/RemoveUnit functions and keep a track of units yourself(slow).~~

nvm Blizzard wrote 2 new functions using those tables

Code: Select all

```
FUNCPTR(FindUnitType3, UnitAny* __fastcall, (DWORD dwId, DWORD dwType), 0x5F1F0)
FUNCPTR(FindUnitOther, UnitAny* __fastcall, (DWORD dwId, DWORD dwType), 0x5F190)
```

> **Quote:**
>
> And hell there's so many examples like this one I could come up with. But as long as it works eh?

That's a mentality you see in many games. 100% CPU usage "Fuck it", 100% memory load "Fuck it", bad memory management/leaks "fuck it everybody has 16 GB ram, fuck those 2 GB peasants, Moore's Law FTW"
The funny part is that at some point the gamservers start crashing because of this kind of poor coding and the maintenance devs haven't a single idea why.

Blizzard isn't much better in that regard. The coders could have added some sleep to the OOG and IngameLoops to reduce CPU usage but it's more likely they will just ban players using the sleepy patch.

The D2 bots are another good example of bad memory management. How much MB takes 1 botting instance of D2BS nowdays? 200 MB+?But hey let's update to to FF20 instead of using the FreeMemory functions to clean up.

But as I said once. The leechers here only know how to compare. Once they try to find changed functions or removed functions they will just give up or beg all around.

D2Clientfunctions had a good cleanups of unused ones they also shrank some functions in size and instead call subroutines instead of copy pasting them in every function.

BTW enjoy TylerErdie aka Grimz over at Phrozenkeep^^

____

Last edited by Vampirewolve on Sun Apr 17, 2016 12:01 am, edited 1 time in total.

Top profile

whisty

User

Post subject: Re: Diablo II 1.14b Pointers - Patches - Functions - Structu **Posted:** Thu Apr 14, 2016 4:41 pm

These are a few examples of terrible hardcoding

User

Joined: Sun Sep 04, 2011 10:07 pm

Code: Select all

```
BOOL IsTownLevel(INT nLevel)
{
   if(nLevel == MAP_A1_ROGUE_ENCAMPMENT ||
      nLevel == MAP_A2_LUT_GHOLEIN ||
      nLevel == MAP_A3_KURAST_DOCKS ||
      nLevel == MAP_A4_THE_PANDEMONIUM_FORTRESS ||
      nLevel == MAP_A5_HARROGATH)
      return TRUE;

   return FALSE;
}
```

When there's this function (original was stdcall)

Code: Select all

```
/*
   Function:      DRLG_RoomIsTown
   Address:      D2Common.#10057
   Notes:
*/
BOOL __fastcall DRLG_RoomIsTown(D2RoomStrc* pRoom)
```

Then there's this one, I think I don't even need to explain why this is horrible

Code: Select all

```
BOOL GetSkillInfo(WORD wSpell, D2SpellInfo *lpBuffer)
{
   if (lpBuffer == NULL)
      return FALSE;

   ::memset(lpBuffer, 0, sizeof(D2SpellInfo));
   lpBuffer->wSpellID = wSpell;
   lpBuffer->nClass = CLASS_NA;
   switch (wSpell)
   {
      // Common Skills
   case D2S_ATTACK:

      lpBuffer->dwSpellInfoFlag |= DSI_TARGETABLE;
      lpBuffer->dwSpellInfoFlag |= DSI_PHYSICAL;
      lpBuffer->dwSpellInfoFlag |= DSI_MELEE;

      strncpy(lpBuffer->szSpellName, "Attack", SPELL_MAX_NAME);
      break;

   case D2S_THROW:
```

Why looping through the whole inventory when you could just directly access the belt grid

Code: Select all

```
INT GetTotalBeltItems()
{
   INT TotalItems = 0;

   for (LPUNITANY pItem = Me->pInventory->pFirstItem; pItem; pItem = pItem->pItemData->pNextInvItem)
      if (pItem && GetItemLocation(pItem) == STORAGE_BELT)
         TotalItems++;

   return TotalItems;
}

BOOL IsBeltFull()
{
   CHAR szCode[4] = {0};
   LPUNITANY pBelt = FindEquipItem(EQUIP_BELT);

   if(!pBelt)
      if(GetTotalBeltItems() == 4)
         return TRUE;
   GetItemCode(pBelt, szCode, 3);
   if(GetTotalBeltItems() >= D2IsBelt(szCode) * 4)
```

Example of exported function using the belt grid

Code: Select all

```
/*
   Function:      INVENTORY_GetItemFromBelt
   Address:      D2Common.#10455
   Notes:
*/
D2UnitStrc* __stdcall INVENTORY_GetItemFromBelt(int nSlot)
```

Then we have some more useless hardcoding. Fuck item types right?

Code: Select all

```
INT D2IsBelt(LPSTR lpszItemCode)
{
   if(lpszItemCode == NULL)
      return 0;

   if(!_stricmp(lpszItemCode, "lbl")
      || !_stricmp(lpszItemCode, "vbl"))
      return 2;

   else if(!_stricmp(lpszItemCode, "mbl")
      || !_stricmp(lpszItemCode, "tbl"))
      return 3;

   else if(!_stricmp(lpszItemCode, "hbl")
      || !_stricmp(lpszItemCode, "zlb")
      || !_stricmp(lpszItemCode, "zvb")
      || !_stricmp(lpszItemCode, "zmb")
      || !_stricmp(lpszItemCode, "ztb")
      || !_stricmp(lpszItemCode, "zhb")
      || !_stricmp(lpszItemCode, "ulc")
```

```
        || !_stricmp(lpszItemCode, "uvc")
        || !_stricmp(lpszItemCode, "umc")
```

I don't know which one is worse. The fact they hardcoded every single exp values, or that it allocates the array every times the function is called. Also the array type should be DWORD but whatever...

Code: Select all

```
DWORD GetExp(DWORD Level)
{
   INT Experience[] =
   {
      0, 500, 1500, 3750, 7875, 14175, 22680, 32886, 44396, 57715, 72144, 90180, 112725, 140906, 176132, 220165, 275207, 344008,
      430010, 537513, 671891, 839864, 1049830, 1312287, 1640359, 2050449, 2563061, 3203826, 3902260, 4663553, 5493363,
      6397855, 7383752, 8458379, 9629723, 10906488, 12298162, 13815086, 15468534, 17270791, 19235252, 21376515, 23710491,
      26254525, 29027522, 32050088, 35344686, 38935798, 42850109, 47116709, 51767302, 56836449, 62361819, 68384473, 74949165,
      82104680, 89904191, 98405658, 107672256, 117772849, 128782495, 140783010, 153863570, 168121381, 183662396, 200602101,
      219066380, 239192444, 261129853, 285041630, 311105466, 339515048, 370481492, 404234916, 441026148, 481128591, 524840254,
      572485967, 624419793, 681027665, 742730244, 809986056, 883294891, 963201521, 1050299747, 1145236814, 1248718217,
      1361512946, 1484459201, 1618470619, 1764543065, 1923762030, 2097310703, 2286478756, 2492671933, 2717422497, 2962400612,
      3229426756, 3520485254
   };
```

y u do dis?????

Code: Select all

```
BOOL GetMapName(BYTE iMapID, LPSTR lpszBuffer, DWORD dwMaxChars)
{
   if(lpszBuffer == NULL)
      return FALSE;

   lpszBuffer[0] = '\0';
   ::memset(lpszBuffer, 0, sizeof(TCHAR) * dwMaxChars);
   if(dwMaxChars == 0)
      return FALSE;

   switch (iMapID)
   {
      ///////////////////////////////////////////////////
      // Act 1 Maps
      ///////////////////////////////////////////////////
   case MAP_A1_ROGUE_ENCAMPMENT:
      strncpy(lpszBuffer, "Rogue Encampment", dwMaxChars);
      break;

   case MAP_A1_BLOOD_MOOR:
      strncpy(lpszBuffer, "Blood Moor", dwMaxChars);
      break;
```

There's a function for that, my god.

Code: Select all

```
__declspec (naked) const wchar_t* __fastcall D2CLIENT_GetLevelName(int nLevel)
{
   /*
      mov esi, nLevel
      call D2CLIENT_6FB6E240
   */

   __asm
   {
      push esi
      mov esi, ecx
      call D2CLIENT_6FB6E240
      pop esi
      retn
   }
}
```

I won't even comment that one. Also, WideCharToMultiByte? use mbstowcs/wcstombs.

Code: Select all

```
BOOL ValidHostileMonsters(LPUNITANY Unit)
{
   if (!Unit)
      return FALSE;

   if (Unit->dwMode == NPC_MODE_DEATH || Unit->dwMode == NPC_MODE_DEAD)
      return FALSE;

   if (Unit->dwTxtFileNo >= 110 && Unit->dwTxtFileNo <= 113 || Unit->dwTxtFileNo == 608 && Unit->dwMode ==
NPC_MODE_USESKILL1)
      return FALSE;

   if (Unit->dwTxtFileNo == 68 && Unit->dwMode == NPC_MODE_SEQUENCE)
      return FALSE;

   if ((Unit->dwTxtFileNo == 258 || Unit->dwTxtFileNo == 261) && Unit->dwMode == NPC_MODE_SEQUENCE)
      return FALSE;

   if ((Unit->dwTxtFileNo == 356 || Unit->dwTxtFileNo == 357 || Unit->dwTxtFileNo == 424 || Unit->dwTxtFileNo ==
425 ||
      Unit->dwTxtFileNo == 418 || Unit->dwTxtFileNo == 419 || Unit->dwTxtFileNo == 421))
      return FALSE;
```

Don't even get me started on the struct defs. And well these are all from one project, seen cases like these in most of projects posted on here. I mean, all I'm saying is, update your own code before you start updating pointers/patches. Thing that annoys me here is, people actually take this as a reference to learn from, to get started into code editing. Hell, I did myself a long time ago. And truth is, it's the worst reference there is.

Top profile

firk

User

Joined: Thu Oct 11, 2007 6:41 pm
Location: Moscow

Post subject: Re: Diablo II 1.14b Pointers - Patches - Functions - Structu

Posted: Thu Apr 14, 2016 6:14 pm

> whisty » 14-04-16 19:41 **wrote:**
>
> These are a few examples of terrible hardcoding
>
> **Code:** Select all
>
> ```
> BOOL IsTownLevel(INT nLevel)
> {
>    if(nLevel == MAP_A1_ROGUE_ENCAMPMENT ||
>       nLevel == MAP_A2_LUT_GHOLEIN ||
>       nLevel == MAP_A3_KURAST_DOCKS ||
>       nLevel == MAP_A4_THE_PANDEMONIUM_FORTRESS ||
>       nLevel == MAP_A5_HARROGATH)
>       return TRUE;
>
>    return FALSE;
> }
> ```
>
> When there's this function (original was stdcall)
>
> **Code:** Select all
>
> ```
> /*
>    Function:      DRLG_RoomIsTown
>    Address:      D2Common.#10057
>    Notes:
> */
> BOOL __fastcall DRLG_RoomIsTown(D2RoomStrc* pRoom)
> ```

You pointed to wrong function because first says about "level_id is town" and second is about pRoom structure.
Yes, there is "level is town" function somewhere in D2Common too, but it does EXACTLY the same as your first code. And i see nothing wrong in such hardcoding - it speeds up things and looks very simple.

> **Quote:**
>
> Then we have some more useless hardcoding. Fuck item types right?
>
> **Code:** Select all
>
> ```
> INT D2IsBelt(LPSTR lpszItemCode)
> INT D2IsPotion(LPSTR lpszItemCode)
> BOOL D2IsCirclets(LPSTR lpszItemCode)
> BOOL D2IsGloves(LPSTR lpszItemCode)
> BOOL D2IsBoots(LPSTR lpszItemCode)
> BOOL D2IsThrowItem(LPSTR szItemCode)
> BOOL D2IsBow(LPSTR szItemCode)
> BOOL D2IsCrossBow(LPSTR szItemCode)
> ```

This can be optimized but i'm not sure that it is so important and horrible.

Also hardcoding experience per level isn't bad (bad allocating stack array per each call is bad).

As for other quotes, i agree.

____

Top profile

Vampirewolve

Post subject: Re: Diablo II 1.14b Pointers - Patches - Functions - Structu **Posted:** Thu Apr 14, 2016 6:34 pm

User

Joined: Tue Mar 01, 2005 8:31 pm

That's mostly WTFPK also D2Common functions haven't changed aside from some compiler optimizations on the 1.14 series.

I think the Itemnamehardcoding comes from the 1.09 version of Bots when the structs were a bit different and several functions weren't known, consider it lazyness.
Those bots still use those in scripts. It can't be improved that much because the game doesn't make differences between helmet and circlet.
Even stuff such as Bow/Crossbow can only be identified via Ammotype.

I dunno which crappy hack it was but I saw the same wall of text ending with "return D2CLIENT_GetLevelNameByID(ID)"; you pasted the wrong function btw. If WTFPK copypasted mousepad properly the level names texts on the map ironically do it properly.

ValidMonsters can easily be shortened by checking if the npc is dead and if it is selectable(some few exception for certain usage such as as drawing the Baalspirit on map) and hostile.

You might also take D2BS as example the code isn't much better there.
How D2BS navigates and loops through controls. It's much faster to BP each Window to obtain the VARPTRs and just compare if it's 0 or not.
I had to mock a D2BS coder on redundancy till they fixed a simple packetcheck.

The same way every damn pickit works. Instead of proper use of AND you see them loop through all rooms and units or use the bitfieldscanner from hackit.
Even worse is instead of having a 2 level pickit on drop looking if the drop is identified or not the bots go through lists of several 100 lines.If blizz would add several 1000 possible good items the bot would just hang up on reading so large files.
Having a Pickit to set a priority on unid/base items and an identificationlist which is only used on identified drops(can be turned off) and during identification makes pickits much faster.

Stings way to handle fonts and so on.

Then there is stuff like autoparty, enchantbots using threads or loops instead of just using eventhandlers.

The people here want to go into codeediting without having the slightest ASM knowledge or having reversed D2 themselves. They hope the code stays the same and just compare.
If you have reversed D2 yourself you usually make notes in case you forget ie. what calls the function to find certain pointer really fast. The raw skeleton how stuff works won't change that much even they change the code entirely. The cleanup Blizz did with 1.14 was needed because D2 src looked like WTFPK in some terms. Now they properly call subfunctions instead of copy pasting the same stuff over and over.
Look at those Varptrs they have like 3-7 references now down from 100+

What I am really interested in when/if Blizz is removing certain limits because Blizz defined some stuff as bytes and removing those limits.
Well hacking was always possible but it's so bothersome to fix those limits so you need 70+ patches for a simple thing.

I expect if they really change stuff like stash/inventory size they will easily see they need to remove/increase limits such as filesizelimit and so on.

Top | profile

firk

User

User

Joined: Thu Oct 11, 2007 6:41 pm
Location: Moscow

Post subject: Re: Diablo II 1.14b Pointers - Patches - Functions - Structu

Posted: Thu Apr 14, 2016 7:41 pm

> Vampirewolve » 14-04-16 21:34 wrote:
>
> Now they properly call subfunctions instead of copy pasting the same stuff over and over. Look at those Varptrs they have like 3-7 references now down from 100+

I think it was inline expansion and not copypasted functions. Obviously they changed compiler optimization options.
For example, if you compare 1.10 and 1.11b code, you will see that in some places one function inlined in 1.10 and called in 1.11b, and another function called in 1.10 and inlined in 1.11b. That's because they changed compiler version in ~2004-2005.

____

Top | profile

Vampirewolve

User

User

Joined: Tue Mar 01, 2005 8:31 pm

Post subject: Re: Diablo II 1.14b Pointers - Patches - Functions - Structu

Posted: Thu Apr 14, 2016 8:40 pm

In some cases you are right(mainly untouched functions)

Other changes are intentional because when you look at the functions that are above and below you will get the idea. They are sorted behind their meaning just like other functions already were.

Just look if the 1.13d function had a fogcall to "error on line". Those are gone, also redundancies/pointless code got removed. I guess that was more a result Blizzard not wanting to use #pragma warning (disable : whatever) all over the place.

You should also look at unused functions most got removed during the merging process. The ones that didn't most likely had a fancy name so they didn't bother checking. Others obviously were cryptic/unclear or resulted in duplicate names, so they looked them up and found no reference and removed them.

You can find the used functions they called but there is no more reference to the unused function, no more reference to the variables in any way, simply nothing.

Top

profile

whisty

Post subject: Re: Diablo II 1.14b Pointers - Patches - Functions - Structu

Posted: Thu Apr 21, 2016 5:54 am

User

User

Joined: Sun Sep 04, 2011 10:07 pm

Another example of bad research is the "AutomapLayer2" struct. This is actually a LevelDefs.bin record.

Code: Select all

```
struct D2LevelDefsTXT
{
   DWORD dwQuestFlag;      //0x00
   DWORD dwQuestFlagEx;   //0x04
   DWORD dwLayer;         //0x08
   DWORD dwSizeX[3];      //0x0C
   DWORD dwSizeY[3];      //0x18
   DWORD dwOffsetX;      //0x24
   DWORD dwOffsetY;      //0x28
   DWORD dwDepend;         //0x2C
   DWORD dwDrlgType;      //0x30
   DWORD dwLevelType;      //0x34
   DWORD dwSubType;      //0x38
   DWORD dwSubTheme;      //0x3C
   DWORD dwSubWaypoint;   //0x40
   DWORD dwSubShrine;         //0x44
   DWORD dwVis[8];            //0x48
   DWORD dwWarp[8];         //0x68
   BYTE nIntensity;         //0x88
   BYTE nRGB[3];            //0x89
   DWORD dwPortal;            //0x8C
   DWORD dwPosition;         //0x90
```

And "D2COMMON_GetLayer" is just a standard function to retrieve a leveldefs.bin record from sgptDataTables

Code: Select all

```
/*
   Function:      TXT_GetLevelDefRecord
   Address:      D2Common.#10749
   Notes:
*/
__forceinline D2LevelDefsTXT* __fastcall TXT_GetLevelDefRecord(int nRecord)
{
   D2DataTableStrc* pDataTables = *D2COMMON_sgptDataTables;
   if (nRecord < 0 || nRecord >= pDataTables->nLevelsRecords) return NULL;

   return &pDataTables->pLevelDefTables[nRecord];
}
```

Top profile

Display posts from previous: All posts ▼ Sort by Post time ▼ Ascending ▼ Go

newtopic postreply **Page 1 of 3** [37 posts] **Go to page 1, 2, 3 Next**

Board index » Diablo II » Diablo II Hacking Development All times are UTC [DST]

Who is online

Users browsing this forum: No registered users and 1 guest

You **cannot** post new topics in this forum

You **cannot** reply to topics in this forum
You **cannot** edit your posts in this forum
You **cannot** delete your posts in this forum

Search for: [ ] Go

Jump to: Diablo II Hacking Development ▼ Go

DONATE