



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 10:40 am

[View unanswered posts](#) | [View active topics](#)

[Board index](#) » [Diablo II Botting System](#) » [D2BS Help/Support](#)

All times are UTC [[DST](#)]


CALL FOR ASSISTANCE: Reverse engineers

Moderator: D2BS Staff

[newtopic](#) [postreply](#) Page 1 of 1 [11 posts]

[Print view](#)

[Previous topic](#) | [Next topic](#)

Author	Message
lord2800	Post subject: CALL FOR ASSISTANCE: Reverse engineers Posted: Wed Nov 02, 2011 4:05 am
<div>Section Leader</div> <div> S.Leader</div> <div>Joined: Fri Jul 05, 2002 8:51 pm Location: /sbin/</div>	<p>I'd like to get D2BS fully working and confirmed correct for all of the offsets/function pointers/structs that it uses. However, I am nowhere near talented enough at reverse engineering to dream of doing that, which is where you come in. A lot of the offsets/etc. appear correct, but I have no independent way of confirming that to be fact and testing can only go so far. So I'm asking for the assistance of the community: Please help confirm as much as possible of the offsets/etc. that D2BS uses as possible.</p> <p>Additionally, I'd like to start up a project to document as much of the useful (as in user-callable with a purpose) D2 API as possible, but that's a piece of work for later. I'll explain the ideas/goals of that in a later post.</p> <hr/> <p><u>D2BS</u> <u>Programming motherfuckers...</u> DO YOU SPEAK IT?! I, for one, welcome our new black overlo... I mean, president!</p>

1. Create signature generator.
2. ???
3. Profit!

[Top](#)**meow88421464****Post subject:** Re: CALL FOR ASSISTANCE: Reverse engineers**Posted:** Wed Nov 02, 2011 5:20 pm

User

**Joined:** Thu Mar 04, 2010
8:11 pm

so this post is to write d2bs errors for them to get fixed?

if so, id like to report my problem

when leech bot enters to lobby, and writes for example /f l, sometimes once it sees the game name it suddenly drops (happens 85% of the time).

sometimes it detects the name but when he's pressing join button drops again

sometimes it even writes /f l and drops alone, even when runner is offline.

also, when you are running auto baal, tp safe msg and baal msg are ignored in the first run.

in fact, bot starts, restarts at least 4 times, enters to the game, misses the first run in harrogath, s/e with runner and gets temp banned -
_"

my conclusion: bot fails to recognize friend lists game name and tries with every word it sees, imo it's an oog error as the auto baal script, excluding the first run, seems to work correctly.

[Top](#)**GreatBob****Post subject:** Re: CALL FOR ASSISTANCE: Reverse engineers**Posted:** Thu Nov 03, 2011 1:30 am


User






**Joined:** Tue May 18, 2004
11:34 pm
Location: UK

meow88421464 » Wed Nov 02, 2011 8:20 am wrote:

so this post is to write d2bs errors for them to get fixed

No. This is about making sure that D2BS has all of the correct information, and ultimately to catalogue everything that can be done with the Diablo II client. Having all of that information complete and correct would allow for someone with the proper vision and knowledge to create tools that could do anything possible with the client.

When the going gets tough, badly scripted bots die.	
Top	 profile
BlushNine	Post subject: Re: CALL FOR ASSISTANCE: Reverse engineers Posted: Thu Nov 03, 2011 10:33 am
<div>User</div> <div> User</div> <div> User avatar</div> <div>Joined: Sat Jul 30, 2011 1:52 am</div>	<p>Wow. LOL. just wow. Just to make sure he doesn't get any more of these, lets review:</p> <div>Quote: I am nowhere near talented enough at reverse engineering to dream of doing that, which is where you come in.</div> <p>Are you talented with reverse engineering?</p> <div>Quote: Please help confirm as much as possible of the offsets/etc. that D2BS uses as possible.</div> <p>Can you confirm offsets that D2BS uses?</p> <div>Quote: to document as much of the useful (as in user-callable with a purpose) D2 API</div> <p>Can you document D2 API calls?</p> <p>If you answered YES to any of these then please post here. If you answered NO to ALL of these questions then please do not post here. If all else fails read the title of the message a few times until that light bulb above your head turns on. If it doesnt turn on, replace light bulb and try again. How do people mistake that message?</p>
Top	 profile
cloudsloth	Post subject: Re: CALL FOR ASSISTANCE: Reverse engineers Posted: Thu Mar 17, 2016 5:57 pm

<p>User</p>  <p>Joined: Fri Mar 16, 2012 12:14 am</p>	<p>In the spirit of teamwork and learning, I started a spreadsheet for this work:</p> <p>https://docs.google.com/spreadsheets/d/ ... edit#gid=0</p> <p>I only added about 20 functions so far, but I have included the real 1.13d address after the offset to make looking them up easier. I will also add the 1.14a function pointers that I discover (1 so far).</p> <p>I tried to look up a lot of functions by searching for ASM matches but the new functions are quite altered. The only way I found the CloseNpcInteract pointer was by putting a breakpoint in ollydbg on some 200+ functions while messing around in game. The prospect of finding all the pointers this way is nauseating.</p>
<p>Top</p>	<p> profile</p>
<p>77920</p>	<p>Post subject: Re: CALL FOR ASSISTANCE: Reverse engineers Posted: Thu Mar 17, 2016 7:49 pm</p>
<p>User Gold</p>  <p>Joined: Mon Dec 14, 2009 1:40 pm</p>	<p>cloudsloth » Thu Mar 17, 2016 11:57 am wrote:</p> <p>In the spirit of teamwork and learning, I started a spreadsheet for this work:</p> <p>https://docs.google.com/spreadsheets/d/ ... edit#gid=0</p> <p>I only added about 20 functions so far, but I have included the real 1.13d address after the offset to make looking them up easier. I will also add the 1.14a function pointers that I discover (1 so far).</p> <p>I tried to look up a lot of functions by searching for ASM matches but the new functions are quite altered. The only way I found the CloseNpcInteract pointer was by putting a breakpoint in ollydbg on some 200+ functions while messing around in game. The prospect of finding all the pointers this way is nauseating.</p> <p>Great idea.</p>
<p>Top</p>	<p> profile</p>
<p>laztheripper</p>	<p>Post subject: Re: CALL FOR ASSISTANCE: Reverse engineers Posted: Thu Mar 17, 2016 8:12 pm</p>
<p>User</p> 	<p>What you guys could to is have people who have lesser knowledge do the easier, more repetitive offsets, and people who have a firm grasp on how to proceed could work on the harder bits.</p>

Joined: Mon Aug 11, 2014
7:27 pm

Just my 2cents, I cheer you on from the sideline 😊

Top

 [profile](#)

Newbz

Post subject: Re: CALL FOR ASSISTANCE: Reverse engineers

Posted: Tue Mar 22, 2016 3:28 am

User



Joined: Tue Jun 23, 2015
6:43 am

[laztheripper » Thu Mar 17, 2016 7:12 pm wrote:](#)

What you guys could to is have people who have lesser knowledge do the easier, more repetitive offsets, and people who have a firm grasp on how to proceed could work on the harder bits.

Just my 2cents, I cheer you on from the sideline 😊

I'd really appreciate if someone gave a basic overview of all the terminology used for someone that has ZERO knowledge of anything that's going on because they're not nerds.

Not yet at least.

Ex.

What are the basic fundamentals of the game that blizzard seemingly broke. (What is an offset? What is a pointer thingaroo? What purpose did the .DLLs serve? Why and how are the DLLs able to be replaced? What does the term patching an .exe mean? How does kolbot work with relation to all the above terms? What aspects of the above terms cause kolbot to be broken now?)

I can't be alone here. Other than a handful of you guys jerkin to the technical jibberish, nobody else understands wtf is going on.

Top

 [profile](#)

cloudsloth

Post subject: Re: CALL FOR ASSISTANCE: Reverse engineers

Posted: Tue Mar 22, 2016 7:22 am

User



Joined: Fri Mar 16, 2012
12:14 am

[Newbz » Mon Mar 21, 2016 6:28 pm wrote:](#)

[laztheripper » Thu Mar 17, 2016 7:12 pm wrote:](#)

What you guys could to is have people who have lesser knowledge do the easier, more repetitive offsets, and people who have a firm grasp on how to proceed could work on the harder bits.

Just my 2cents, I cheer you on from the sideline 🤔

I'd really appreciate if someone gave a basic overview of all the terminology used for someone that has ZERO knowledge of anything that's going on because they're not nerds.

Not yet at least.

Ex.

What are the basic fundamentals of the game that blizzard seemingly broke. (What is an offset? What is a pointer thingaroo? What purpose did the .DLLs serve? Why and how are the DLLs able to be replaced? What does the term patching an .exe mean? How does kolbot work with relation to all the above terms? What aspects of the above terms cause kolbot to be broken now?)

I can't be alone here. Other than a handful of you guys jerkin to the technical jibberish, nobody else understands wtf is going on.

I'll give it a shot:

When you run the game, previously your computer would load a few files up:

Game.exe
D2Client.dll
D2Common.dll
- and a few more

D2BS would inject itself into Game.exe and then it would be able to execute code from within the game.

At this point each of these files is in assembly language (ASM). A pointer is a line of that code where a function starts and a struct is a line in that code where some data is stored (like all the Units). Kolbot interacts with Diablo by calling lines of that code and interacting with the data structures.

Each of these files exists within your computers memory and the offsets are simply where in the memory that specific file starts.

In 1.14a they moved everything out of the dlls and included it in Game.exe. Additionally they did something (probably a new compiler and build system?) that made all the functions look drastically different. Assembly looks like black magic until you become an uber nerd or study a few lines for a few hours to understand them. It's not that surprising that they look drastically different, but there are many steps to find

our way again. At present we only know where a handful of function pointers are and a few of the data structures. Kolbot has no way of interacting sufficiently with the 1.14a Game.exe .

A lot of what all the functions do is referencing. Sometimes this is calling another function, sometimes it's comparing data. A function would be interacting with data that is related to what it does, so it could be possible to map all these connections and come to an understanding of what's going on in 1.14a based on how that map used to look in 1.13d. The cancelNPCInteract function will reference the data for who you are currently interacted with and also either the data for your busy state or a function that effects your busy state. We don't know where any of this is in 1.14a but if you map out enough connections you might start to see some of the connections making sense again.

There's no single method that's going to get us the information we need. Sometimes there's something in the old function that will remain true in the new version. If a function is preparing to call a packet maybe it will set a register to the packet number, so maybe in the new exe you can search for that packet number and find the function. I was able to use this to narrow down my searches for a couple pointers.

A tl;dr might look something like this:

We use 200 cards in a deck of 10,000+ cards. Blizzard has changed the suits, colors, switched from english to chinese, and reshuffled the entire deck.

It is not enough that you can read chinese, or that you can count cards, or that you have an excellent memory of colors, or that you can decipher symbols. You have to do a little bit of it all and it's not clear at all how long it might take. At least for me, I'm totally new to reverse engineering.

Hope that helps!

[Top](#)**Newbz****Post subject:** Re: CALL FOR ASSISTANCE: Reverse engineers**Posted:** Wed Mar 23, 2016 1:02 am

User



User

Joined: Tue Jun 23, 2015
6:43 am

Thank you cloudslath

You're the one and only person I've met in the D2 community that shares knowledge selflessly, is humble, and goes above and beyond to help the younglings

BlushNine » Thu Nov 03, 2011 9:33 am wrote:

Wow.

If you answered YES to any of these then please post here.

If you answered NO to ALL of these questions then please do not post here.

If all else fails read the title of the message a few times until that light bulb above your head turns on. If it doesnt turn on, replace light bulb and try again.
How do people mistake that message?

Polar opposite.

It seems clear to me that the people who have the skills to "reverse engineer" have 0 reason to contribute publicly

People like cloudsloth who are willing to selflessly sacrifice their time for the benefit of all are few and far between. Actually, cloudsloth is the only one on this whole website.

Other's with potential for contribution aren't so selflessly dedicated to the cause, instead choose to be toxic and make snide comments.

Beginners with limited or no knowledge who may have the interest, time, or dedication to meaningfully contribute have no opportunity to learn in such a toxic community of obnoxious elitists and veterens

Top



nesterdron

Post subject: CALL FOR ASSISTANCE Reverse engineers

Posted: Thu Apr 06, 2017 2:12 am

User



Joined: Fri Nov 22, 2013
2:42 pm
Location: Россия

How many are you seeing right now? Cause for me, it shows 3 ...and thats way too much.

без подписи

Top



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



Page 1 of 1 [11 posts]

[Board index](#) » [Diablo II Botting System](#) » [D2BS Help/Support](#)

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:

Jump to:

