



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 12:57 pm

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

[Board index](#) » [Diablo II](#) » [Diablo II Hacking Development](#)

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

Extra-work, stagec.dll

Moderator: [Diablo Mods](#)

[newtopic](#)



[postreply](#)

Page 1 of 3 [34 posts]

[Go to page 1](#), [2](#), [3](#) [Next](#)

[Print view](#)

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

Author	Message
chrisseybho	Post subject: Extra-work, stagec.dll Posted: Tue Dec 26, 2017 4:37 pm
<div>User  Joined: Sat Jan 29, 2011 4:45 pm</div>	<p>So, blizzard finally got their finger out and surprised 99% of us lol, let's get started on figuring this new anticheat out and developing a safe workaround guys. If any can do it, it will be from this site imho.</p> <p>Merry Xmas and happy New year to all.</p>
Top	profile
77920	Post subject: Re: Extra-work, stagec.dll Posted: Wed Dec 27, 2017 7:40 pm
<div>User Gold </div>	<p>I would not count on something public being released to fix it.</p> <p>There are only a select few who can and will reverse it but would likely</p>

Joined: Mon Dec 14, 2009
1:40 pm

keep to themselves.

Top



chrissybhoy

Post subject: Re: Extra-work, stagec.dll

Posted: Thu Dec 28, 2017 2:40 am

User



User

Joined: Sat Jan 29, 2011
4:45 pm

Was Kinda hoping for the same sort of activity we had when dupe got patched and we were all chasing a workaround.

Was the most fun I've had @ d2 in YEARS lol

This could be fun too 😊

Top



WiseWolf

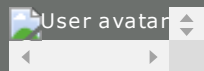
Post subject: Re: Extra-work, stagec.dll

Posted: Thu Dec 28, 2017 4:15 am

User



User

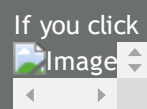


Joined: Mon Aug 09, 2010
12:37 am

Location:
/home/loser/.local/share/Tr

if other bots that ran in wow did not find a work around why is this game any different? I am just being realistic, and i am a person who loves botting with a passion. I am not sure if we can ever do that again :\

If you click "refresh" you will see in real time what is playing on my computer 😊



Top



micro\$oft

Post subject: Re: Extra-work, stagec.dll

Posted: Thu Dec 28, 2017 5:16 am

User



User

Joined: Tue Sep 25, 2007
12:54 pm
Location: Interweb

chrissybhoy » Tue Dec 26, 2017 10:37 am wrote:

So, blizzard finally got their finger out and surprised 99% of us lol, let's get started on figuring this new anticheat out and developing a safe workaround guys. If any can do it, it will be from this site imho.

Merry Xmas and happy New year to all.

Do you work for Activison-Blizzard

(ノ° °)ノミ★ ☆

Top

 [profile](#)

weiry6922

Post subject: Re: Extra-work, stagec.dll

Posted: Thu Dec 28, 2017 7:08 am

User



Joined: Thu Aug 04, 2005
1:12 am
Location: Australia

Mmbot botting meta is now

Top

 [profile](#)

chrissybhoy

Post subject: Re: Extra-work, stagec.dll

Posted: Thu Dec 28, 2017 3:57 pm

User



Joined: Sat Jan 29, 2011
4:45 pm






WiseWolf > Thu Dec 28, 2017 3:15 am wrote:

if other bots that ran in wow did not find a work around why is this game any different? I am just being realistic, and i am a person who loves botting with a passion. I am not sure if we can ever do that again :\'

But I already know 100% someone has already updated their bot/mods to run after stagec.dll was in place, I mean, he proved it barely an hour after reset.

Surely if enough of us are trying we can get there too, u never know, u might have fun and learn a few things whilst trying also 😊

Ever the optimist 😊

Top	 profile
77920	Post subject: Re: Extra-work, stagec.dll Posted: Thu Dec 28, 2017 4:17 pm
User Gold  Joined: Mon Dec 14, 2009 1:40 pm	<p><u>chrissybhoy » Thu Dec 28, 2017 9:57 am wrote:</u></p> <div><p><u>WiseWolf » Thu Dec 28, 2017 3:15 am wrote:</u></p><p>if other bots that ran in wow did not find a work around why is this game any different? I am just being realistic, and i am a person who loves botting with a passion. I am not sure if we can ever do that again :\ But I already know 100% someone has already updated their bot/mods to run after stagec.dll was in place, I mean, he proved it barely an hour after reset. Surely if enough of us are trying we can get there too, u never know, u might have fun and learn a few things whilst trying also 😊 Ever the optimist 😊</p></div> <p>If your talking about vamp you are probably correct.</p>
Top	 profile
chrissybhoy	Post subject: Re: Extra-work, stagec.dll Posted: Thu Dec 28, 2017 4:56 pm
User  Joined: Sat Jan 29, 2011 4:45 pm	<p>I am talking Bout vamp lol, he had it beat within an hour, surely we can too.</p> <p>Don't get me wrong, it won't be easy as vamp knows his shit.</p>
Top	 profile
77920	Post subject: Re: Extra-work, stagec.dll Posted: Thu Dec 28, 2017 5:17 pm
User Gold	



Joined: Mon Dec 14, 2009
1:40 pm

chrissybhoy » Thu Dec 28, 2017 10:56 am wrote:

I am talking Bout vamp lol, he had it beat within an hour, surely we can too.

Don't get me wrong, it won't be easy as vamp knows his shit.

This is very true. The problem is no one wants to invest the time into it like he does / can
Understanding the Stage A - B - C detection is step 1 . I've played with it a bit...
my problem is I don't know about about the FOG -10006 from 1.13d or Compress/Decompress the packets.

Quote:

Noah~ says: Blizzard has utilized bnet 0x4C 'extrawork' implementation to remotely download their new anticheat 'stage{a,b,c}' libraries which report hashes of d2 memory via 0x4B response.

Some ideas for potential work around (not recommended/short term):

- 1) block bnet 0x4C S->C and hope blizzard doesn't ban you for not responding
- 2) pretend to be a mac user by spoofing 'XMAC' when sending bnet 0x7 C->S response
- 3) reverse engineer the extrawork libs and properly respond using bnet 0x4B C->S, in addition, you must detect changes to the anti-cheat and make sure to exit if you haven't implemented a fix

Code: Select all

```
addEventListener('realmpacket',  
function (packet)  
{  
if (packet[0] == 0x4c || packet[0] == 0x4b) // check for some packet  
print(packet);  
  
// return true to block packet  
return true;  
}  
);
```

If you are interested in relevant d2 functions, feel free to look at FOG ordinals (1.13d) -10006 which is recv bnet packet and relevant compress/decompress ordinals: -10223 and -10224.

Note: the extrawork files utilize encryption and obfuscation. Also make sure to hook tls callback otherwise your debugger will just run and exit (and get you banned) without breaking at anything relevant.

Code: Select all

```
1.14d function 0040DC60 - BNETPacketRecv_Interception
1.14d function 0051C5C0 - BnetSend
1.14d function 00521B00 - BnetReceive
```

Code: Select all

```
{PatchCall,GetOffset(0xB260),(unsigned long)Decompress_Packet,5 }, //Updated 1.14d 0040B260-BASE

1.13d
FUNCPTR(FOG, CompressPacket, unsigned long __fastcall, ( unsigned char *dest,unsigned long memory_size,unsigned
char *source, unsigned long src_size) , -10223)
FUNCPTR(FOG, DecompressPacket, unsigned long __fastcall, ( unsigned char *dest,unsigned long memory_size,unsigned
char *source, unsigned long src_size) , -10224)

1.14d
FUNCPTR(FOG, CompressPacket, unsigned long __fastcall, ( unsigned char *dest,unsigned long memory_size,unsigned
char *source, unsigned long src_size) , 0xB1B0) //Updated 1.14d //0040B1B0-BASE (int __fastcall
CompressPacket(_BYTE *a1, int a2, char *a3, int a4)
FUNCPTR(FOG, DecompressPacket,unsigned long __fastcall, ( unsigned char *dest,unsigned long memory_size,unsigned
char *source, unsigned long src_size) , 0xB260) //Updated 1.14d //0040B260-BASE (int __fastcall
DecompressPacket(unsigned __int8 *a1, int a2, _BYTE *a3, int a4)
```

Anyways... only sniffed one login and it required extrawork: 4EC8B57C32A06A4E97C67CBB3A3AC6E2.mpq which inside was named as "d2stagea.dll"

B (un-encrypted) calls C Extrawork (encrypted) to my understanding its a daemon that never unloads. That's all for now. I don't know enough about this stuff to be any real help.

+ vamp will come here and call me an idiot and I don't know shit etc.

Last edited by 77920 on Fri Dec 29, 2017 2:52 am, edited 1 time in total.

Top

 [profile](#)

Ling

Post subject: Re: Extra-work, stagec.dll

Posted: Fri Dec 29, 2017 1:58 am

User



User



Joined: Thu Dec 19, 2002
12:04 am
Location: Ontario

inb4vamp



Top

 [profile](#)

chrissybhoy

Post subject: Re: Extra-work, stagec.dll

Posted: Fri Dec 29, 2017 4:32 pm

User



User

Joined: Sat Jan 29, 2011
4:45 pm

Well, my new year's resolution is now to find a way to beat this shit, I know am gonna have to geek the fuck out but has to be done. I am NOT letting blizzard beat us lol.

Don't hold ur breath tho guys it will take me a while 😊

Expect will have to learn shitloads to even comprehend most of it....

Top

 [profile](#)

77920

Post subject: Re: Extra-work, stagec.dll

Posted: Fri Dec 29, 2017 5:05 pm

User Gold



User

Joined: Mon Dec 14, 2009
1:40 pm

chrissybhoy » Fri Dec 29, 2017 10:32 am wrote:

Well, my new year's resolution is now to find a way to beat this shit, I know am gonna have to geek the fuck out but has to be done. I am NOT letting blizzard beat us lol.

Don't hold ur breath tho guys it will take me a while 😊

Expect will have to learn shitloads to even comprehend most of it....

I'm not holding my breath. lol.

Top



Alex-M

Post subject: Re: Extra-work, stagec.dll

Posted: Sat Dec 30, 2017 7:27 am

User



Joined: Tue Aug 31, 2004
11:39 pm
Location: WI

Quote:

which report hashes of d2 memory via 0x4B response

So is that all it's doing? Or is that just part of what it's doing?

Wondering because couldn't an easier workaround involve using a proxy rather than reading/writing/injecting the D2 process? Of course this would mean writing a new bot from scratch rather just modifying what is already available. But a proxy-based bot honestly sounds significantly easier than reverse engineering encrypted/obfuscated anticheat software.

Reading and modifying network data seems safe enough, so long as Blizzard isn't scanning beyond the D2 process and you don't fuck up by sending broken packets.

Pardon my ignorance if I'm shooting out shit ideas here, I'm not particularly in the loop with the state of D2 hacking these days. 😊



Joined: 16 May 2002



Top





Hecate

Post subject: Re: Extra-work, stagec.dll

Posted: Sat Dec 30, 2017 3:08 pm

<p>User</p> <p> User</p> <p>Joined: Mon Sep 12, 2011 3:49 am</p>	<p>If it "only" sends hashes of d2 memory, can't one always just start a clean instance on the side, duplicate all server traffic to it and send the hashes from that one? As d2 clients are pretty much accepting all (not sure) inputs without desynching, sending all S->C packets to the clean instance should put it close enough to what a clean instance should look like. Perhaps you can even box it a bit and redirect graphics calls so it doesn't open a real window - maybe a bit tricky without editing anything inside but likely possible.</p> <p>A bit messy to start two instances for one, but it's (soon) 2018, who cares about computing power for d2 unless you want to really mass bot (in which case you will need to bite into the sour apple and find a proper "fix").</p> <p>PS: i stopped playing d2 quite some time ago and don't really intend to come back unless there is a simple way to test some ideas i had.</p>
<p>Top</p>	<p> profile</p>

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

 [newtopic](#)  [postreply](#) **Page 1 of 3** [34 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

