

Forum:[Hack Forums](#)

Thread: [I've done it!](#)

glitchgxd - July 21, 2015, 3:06 am

So I started playing around with C and Disassembling processes the other day, and I've managed to make my own 'Gold counter' in a separate window from the client. This is pretty much step one of a multi-step process to gather all the information about League and work on a scripting-interface / client.

Edit: No, I am not trying to "modify" gold in any way. This was only to attempt to READ data from the client. I'm trying to gather information, not modify it. Everything is basically server-side I think, so there's no point in modifying it.

The main intent is to build this information to lead to the creation of a scripting engine. I hope to be able to create in-game "Assists" for players (jungle timers, chance of survival in engage calculators, etc). All real-time and in-game.

Spoiler ([Click to View](#))

[\[img\]http://s14.postimg.org/5z4rewzbx/lolgold.jpg\[/img\]](http://s14.postimg.org/5z4rewzbx/lolgold.jpg)

For those interested in the details:

Spoiler ([Click to View](#))

```
Code #define PBASE 0x25AA2A0
```

```
#define OFFSET_A 0xF8
```

```
#define OFFSET_B 0xC
```

```
DWORD goldValue = *(DWORD*)(*(DWORD*)((DWORD*) PBASE) + OFFSET_A) +  
OFFSET_B);
```

Just thought I'd share since I'm pretty excited about this.

Anyone else have any projects they're working on?

Mann02 - July 21, 2015, 3:08 am

someone's just accused a certain "Glitch" of jacking their instagram account :P

lenaos - July 21, 2015, 3:09 am

Thought this was gonna be an instagram jacking troll thread

Balding - July 21, 2015, 3:09 am

Your image is broken. Please fix it.

movsx - July 21, 2015, 3:10 am

Great job. But I am confused about one thing.

```
Code DWORD goldValue = *(DWORD*)(*(DWORD*)((DWORD*) BASEGOLD) + OFFSET_A) +  
OFFSET_B);
```

How does that read memory from a remote process, like League, unless you're injected your code

into the same process as League?

Hash G. - July 21, 2015, 3:10 am

Your image doesn't work for me.

Edit : image link : <http://s14.postimg.org/qw0zjkxcv/lolgold.png>

And now OP, think about how you can turn this in a hack. :p

sweatpants - July 21, 2015, 3:11 am

Yeah vouch for the dude above me Picture is broken m8

TNF. - July 21, 2015, 3:12 am

(Jul 21, 2015 03:09 AM)Ren? Wrote: [\[CITE\]](#) Thought this was gonna be an instagram jacking troll thread

I really thought the same Ren.?

Balding - July 21, 2015, 3:12 am

(Jul 21, 2015 03:10 AM)Hash G. Wrote: [\[CITE\]](#) Your image doesn't work for me.

Edit : image link : <http://s14.postimg.org/qw0zjkxcv/lolgold.png>

And now OP, think about how you can turn this in a hack. :p

You can probably make this a hack like Hash said. Give it some thought.

Hash G. - July 21, 2015, 3:14 am

(Jul 21, 2015 03:12 AM)Bald Cat Wrote: [\[CITE\]](#) You can probably make this a hack like Hash said. Give it some thought. I'm not really sure since all is server based, I believe.

I'm contradicting myself lol

Balding - July 21, 2015, 3:14 am

(Jul 21, 2015 03:14 AM)Hash G. Wrote: [\[CITE\]](#) I'm not really sure since all is server based, I believe. I'm contradicting myself lol

You are lol. I'm sure it's possible. He just has to figure it out.

Mann02 - July 21, 2015, 3:19 am

editing the memory to change the gold value will do nothing on the server side, the client is there just to show you what happens and indicate things, but ultimately the server is checked for the real values, so it does not matter what you see if you alter it, it matters what the server has stored for you.

you probably could do that using cheat engine, never tried to hook it to the process, maybe it's not possible, but I think you waste your time with such "hacks"

glitchgxd - July 21, 2015, 3:21 am

It's definitely server based. I'm almost positive the data is coming directly from packets from the server and then updated in the thread.

Besides that, even if you modified the value for a second, it wouldn't matter since your item purchases are evaluated through the server. I don't think riot would let that go so easily, and if they did, there certainly would already be some sort of hack out for gold lol

I do plan on creating a struct with as much in-game information as I can, however. From there, like I said, I should be able to pass the data down through some sort of scripting engine to allow people to create in-game bots. I don't like the current "BoL". LUA isn't really my thing.

Hash G. - July 21, 2015, 3:38 am

(Jul 21, 2015 03:21 AM)?Glitch Wrote: [\[CITE\]](#) It's definitely server based. I'm almost positive the data is coming directly from packets from the server and then updated in the thread.

Besides that, even if you modified the value for a second, it wouldn't matter since your item purchases are evaluated through the server. I don't think riot would let that go so easily, and if they did, there certainly would already be some sort of hack out for gold lol

I do plan on creating a struct with as much in-game information as I can, however. From there, like I said, I should be able to pass the data down through some sort of scripting engine to allow people to create in-game bots. I don't like the current "BoL". LUA isn't really my thing. Good luck on this, it sounds really promising. Keep us updated man!

glitchgxd - July 21, 2015, 9:54 am

(Jul 21, 2015 03:19 AM)Mann02 Wrote: [\[CITE\]](#) -snip-

you probably could do that using cheat engine, never tried to hook it to the process, maybe it's not possible, but I think you waste your time with such "hacks"

Reading values out from processes by injecting a dll into the process and getting the values of memory at specific addresses + offsets is a waste of time?

This was an educational exercise. By your logic, learning anything is a "waste of time" ?