

Forum:[Hack Forums](#)

Thread: [Proxy server to beat screenshare??](#)

MadZ - March 25, 2017, 9:54 am

Hi friends,

I was looking into the Minecraft protocol between Client and Server (wiki.vg) and wrote a basic proxy server with a public library that routes a client connection to a target server of your choice. A neat thing I would like to point out is that the minecraft account you use to connect to the server can be different from the actual account being connected to the final destination (You might be able to see this in the following video as I was actually logged onto "Eistaria" on the right side/huzuni client, but when logging in to the proxy, I ended up on odie as "brgr.")

Anyways, you can see that I was hacking away with Huzuni but then I "froze" myself (brgr/logged in as Eistaria) through the client on the left hand side (slugtastic), which we will call the moderator in this case. Not having access to any ghost client like vape (or similar) with a self-destruct feature, I was able to close the Huzuni instance while having the proxy server maintain a connection by responding to the server with the proper keep alive packet and ID. I then relaunched a "vanilla" instance of Minecraft (optifine) under the account that the proxy server had logged in as (brgr, not Eistaria) in order to undergo the screenshare process that will follow in an actual PVP server with freezing and screensharing. After logging back in through the vanilla client and actual account, you can then close the proxy server and delete/move any of the hacked clients you have in your Minecraft directory in the 5 or so minutes most staff give you to setup.

Overall, this was just a test and I don't expect this to replace the injectable ghost clients that you Minecraft hackers/pvpers crave, as this method is more tedious. However, this could be a solution to using a client like Huzuni that is not considered a "ghost client" and still being able to get away with a screenshare by never "logging out" when frozen.

Without further ado, here is the short video I recorded (raw footage; unedited).

Quality is very bad. Apparently I don't know how to use OBS.

[Video: <https://www.youtube.com/watch?v=QUIkcHab2S8>]

Feedback, criticism, shittalk, bring it here.

Ethylene_ - March 25, 2017, 9:59 am

WOW THIS IS AMAZING HONESTLY I WOULD LOVE TO USE THIS

// great fucking job this is fantastic!

MadZ - March 25, 2017, 10:02 am

Just an additional note: this could easily be turned into a web service hosted on a server (requires very little resources per instance; different proxy on different ports) This would make it even more effective in that you don't need to setup your own proxy server and close it when SS; however, I don't have the monetary funds to do this.

SIM-852088 - March 25, 2017, 10:52 am

Pretty cool concept, but you also still 'relog' in the video. When you join on the vanilla client it shows just reshows the Essentials MOTD and stuff. So this wouldn't actually work for more servers. It won't

work since the Freeze plugins alert staff when a player 'relogs', and this is what happens. Some also auto-ban for that, and it'll be fishy that you relogged. Also this concept probably won't work on a BungeeCord server since it prevents you from logging in when you're already on the server.

catgorl - March 25, 2017, 10:59 am

(Mar 25, 2017 09:54 AM)MadZ Wrote: [\[CITE\]](#) Snip

Good job, I had this idea planned ages ago and was suprised no one publicly used it / talked about it from what I saw (besides codecub having a video on his channel with a proof of concept (not being used in this way though)) although as neon said it's probably not very practical due to various reasons.

Black?jack - March 25, 2017, 11:56 am

Energetic has had this idea since around the first time ghost clients became popular - the plan was to offer it as a web service, but I was honestly just too lazy to finish the code :P

WOLGA - March 25, 2017, 4:11 pm

When the vanilla client connects to the actual server so that the proxy server connection gets kicked, isn't that evidence left behind?

Undividable - March 25, 2017, 8:27 pm

Also wouldn't they just check your logs to see when your MC was launched and also in last activity viewer couldn't they check that a new instance of MC was launched?

Rigamorti\$ - March 28, 2017, 4:36 am

Code cub made this shit like 10 years ago

[Video: <https://www.youtube.com/watch?v=LjVEuNzRpEk>]

Codingq - March 29, 2017, 9:35 am

Damn, I don't really know how to code but I will use totally use that.

SIM-2735155 - March 30, 2017, 1:19 pm

Is it currently available as in a compiled or source code version?

MadZ - March 30, 2017, 2:30 pm

(Mar 30, 2017 01:19 PM)ShayBox Wrote: [\[CITE\]](#) Is it currently available as in a compiled or source code version?

It is very easy to do with 'node minecraft protocol' library

PHP Code

```
<?php
```

```
npm install minecraft-protocol
```

In fact, they have a similar proxy server example that work's as is, but you need to make some adjustments to login to premium/online servers and to maintain keep alive communication between C <--> S.

But, note that there are certain plugins that apparently (most?) servers use that automatically detects reconnect (which the proxy server does do to hand over communication back to the user, albeit in a split second) [see posts by TehNeon and others on first page for his explanation].

Perhaps a heavily modified minecraft client could rework the protocol (seamless handoff between client and server), but that defeats the purpose of being screenshared on a vanilla client.

BFCE - March 30, 2017, 2:30 pm

Pretty sweet concept. Good job

MadZ - *March 30, 2017, 2:32 pm*

(Mar 30, 2017 02:30 PM)BFCE Wrote: [\[CITE\]](#) Pretty sweet concept. Good job
I appreciate it