Game Hacking as a Service

By Rinn Teo | 27 October 2021, 1.00pm SGT

What is Game Hacking as a Service

Game hacking as a service is when the hacker writes a user-friendly User Interface (UI), also known as a client, that allows the user to manipulate the game they intend to hack in in a way that "cheats" the game. For example, when the user should have failed to clear a level due to insufficient time, he can use the client to change the timer of said level to a longer time, or even unlimited time.

Or when the user should have died from an enemy kill, he could use the client to either revive on the spot or not have his health bar fall below a certain range, which equates to "immortality". By "lying" to the game, it is considered as game hacking, and it is a kind of service that hackers create to sell to their target audience, specifically, the players for the game that they are creating the hacking service for.

Difference Between Hacking and Botting

What is Hacking?

Hackers create a client that allows users of a certain game to manipulate its game memory such as data or codes to modify the original intention of the game play. Hacking in gaming context is basically *altering* the game codes that benefit the player to "win". It is also often caused by the game's anti-cheat function not being properly secured or having a bad logic in codes, for example, the server trusting client values. This means that the server trusts whatever the client says without its own validation checks. In simpler terms, it is when Friend A blindly trusts Friend B when Friend B declares that he obtained full marks in a math test without checking for himself, when he should have asked for his test papers as solid proof.

What is Botting?

Botting is repeating the gameplay in an automated way for users who would rather spend the time taken in doing their own things, but it *does not alter* the original game codes in any way.

It is sending inputs to "move" the character in game, for example image recognition and pixel/colors recognition of the game itself.

Copyright of Game Hacking

There are various types of copyrights, and these are two types as an example:

1. The files of a copied game, better known as a Private Server, are from the original and rightful developers. A private server exists when the original game files are leaked internally, or when someone hacks into the company servers.
2. The private server might be self-made by the server owner without stealing the game files directly from the original game. This can be made possible through reversing the original game client file, understanding the network part through reverse engineering, and proceeding to self-make the server files.

Through Method 2, it will *not* be considered as illegal since it is based purely on the skills of the hacker-developer and did not obtain the original game files through any other illegal means.

However, through Method 1, it will be considered as illegal, and against the copyright law. For example, Game 1 plants a trojan (a type of malware that is often disguised as legitimate software) to the original developing servers, thus whenever the original codes get updated, Game 1 can continue downloading them and self-maintain a copy of their own version of the game.

A trojan can be disguised as these service hosts in task manager, but one of these legit processes in the PC is actually coded to, in this case, copy out the game files to another server.

These versions of copied-games are generally known as private servers, and these hacker cum developers milk money from players by providing donation services for players to donate to them, either for better gameplay or for certain in-game exclusive items.

Players also opt to play these private servers instead of the original game usually because of the lowered difficulty in the private server. Custom contents that are not available in the original are also usually coded into the private servers to spice up the game, attracting more players.

Why Players Pay for Such Services

Players pay for these hacking and botting services for various reasons, but mainly for convenience, entertainment, and competition between friends or foes.

Convenience

Players who fall under the convenience section are usually the type that use botting service instead of hacking service. For example, in a game that the user is required to spend some time "farming" for resources, a botting service will immensely help the user such that there will be automated "farming", allowing the user to concentrate on other stuff, while only playing the game after they are free to reap the benefits of these automated farmed resources.

Entertainment & Competition

Players who fall under the entertainment and competitive section tend to lean towards the hacking service side. It allows them to surpass other players easily without wasting any more time and money than necessary. Take for example the aim-bot previously mentioned, if the user's skills are lacking, by making use of the aim-bot, they would not have to waste more time to hone their skills.

The prices for any hacking and botting services vary accordingly to the hacker, however the better the code is written for such services, the more expensive it tends to be.

Dangers of Engaging in These Services

The two most common ways that malware accesses your system are the Internet and email. So basically, anytime you’re connected online, you’re vulnerable.

Malware can penetrate your computer when you surf through hacked websites, view a legitimate site serving malicious ads, download infected files, install programs or apps from unfamiliar provide, open a malicious email attachment (also known as ‘malspam’), or pretty much everything else you download from the web on to a device that lacks a quality anti-malware security application.

Examples of Dangers Involved

1. **Trojan/Virus:** Once a Trojan lands on a target computer, the next thing it does is reach out to the attacker's command and control server (C&C) to download a secondary infection, often ransomware. The performance of your PC might also slow down or crash more often than usual. This is usually known as the "blue screen of death". Unexpected pop-up ads that you did not allow permission for may also constantly appear.
2. **Money Wasted**: Another more common issue from engaging in these services is having your money wasted on these gaming services that may or may not be harmful or would shut down anytime as per the hacker's mood.
3. **Compromised Private Information**: Lastly, since these hacks and bots require you to create an account, some users might use the common username or email and password that they often use. Even if said hack or bot was created by a hacker that genuinely wants the player to have fun or help out the player in their gameplays, they would still undoubtedly have access to these passwords. Thus, should the hacker's PC get hacked by another hacker, all the passwords would be compromised, leading to another level of risk.

Conclusion

Is it worth it to hack or to bot for a game that might or might not compromise your personal information? At the end of the day, gaming is only just a side entertainment to keep you relaxed or will the time away. Even if the hacking service that is being used is reputable, the hacker himself is just a player, like any of us. He isn't bound by any contract to safekeep anyone's personal information. Risking our personal information on a platform solely based on entertainment and wasting time won't be worth it at all. It is up to us to protect our own crucial private information and not fall victim to any traps laid out online.

Note: The opinions expressed in this blog post are those of the author. They do not purport to reflect the opinions or views of the Asia Internet Coalition (AIC) or its members.