ActiveFence

(Un)Fair Play: Cheating and Exploitation in Online Gaming

January, 2022

Contents

Executive Summary

It is estimated that cheating costs the video gaming industry ~$29 billion each year in lost revenue.[1] This financial damage can be attributed to three distinct harms:

- **The loss of revenue from in-game stores:** The fraudulent acquisition of in-game tools and digital assets prevents platforms from selling such digital goods through their in-game store.
- **Devaluation of digital assets:** The sale of digital assets acquired fraudulently can see platforms undercut, and the digital assets they list devalued.
- **Weakened player retention**: The presence of users manipulating multiplayer games to gain an unfair advantage harms legitimate player retention. Loss of these players could significantly harm the profitability of a game.

This report showcases how **threat actors** who perpetrate this damaging activity can be identified and how **the novel software** and **cheat codes** threat actors offer can be **detected.** It also provides examples of our ability to **identify and access the markets where these services are sold,** enabling our partners to take decisive, proactive action.

The report provides examples of:

- The professional sale of cheat packages
- The promotion of software to **alter or hack a game's code**
- Markets that sell **modded accounts containing currency** and **items**

While the harm outlined is significant, platforms can counter this activity through targeted and proactive intelligence gathering. The cost of doing nothing or reacting to each new exploitation as it occurs is severe—the activity attacks the abused platform's business model, and jeopardizes their market share.

[1] https://www.gamedeveloper.com/business/does-the-video-game-industry-have-a-29-billion-cheating-problem-

Introduction: Monitoring the cheating industry

It is well known that online gaming has grown dramatically in recent years. In fact, it is estimated that the global number of online gamers has reached just over 1 billion gamers in 2021, an increase of 32% over 2019.[2] However, as this industry grows in popularity, so does the demand for cheats which provides gamers with an unfair advantage. In response to this demand, threat actors, otherwise known as **gaming exploiters**, have made a business of selling codes that leverage weaknesses in game design. These cheats negatively impact the experience of other gamers and harm potential revenue streams of legitimate gaming platforms.

Gaming platforms that seek to stay ahead of these threats and maintain the integrity of their games and the experience of players must be aware of the constantly evolving landscape of gaming exploiters. Monitoring the cheating industry, including the **types of cheats** being sold, **where they are sold**, and **by whom**, allows platforms to stay ahead of these threats. Using off-platform intelligence about this ecosystem, platforms are able to to immediately detect new cheats, assess their impact, and take action against their creators and users.

[2] https://www.statista.com/forecasts/456610/video-games-users-in-the-world-forecast

Gaming exploiters: Types of vendors

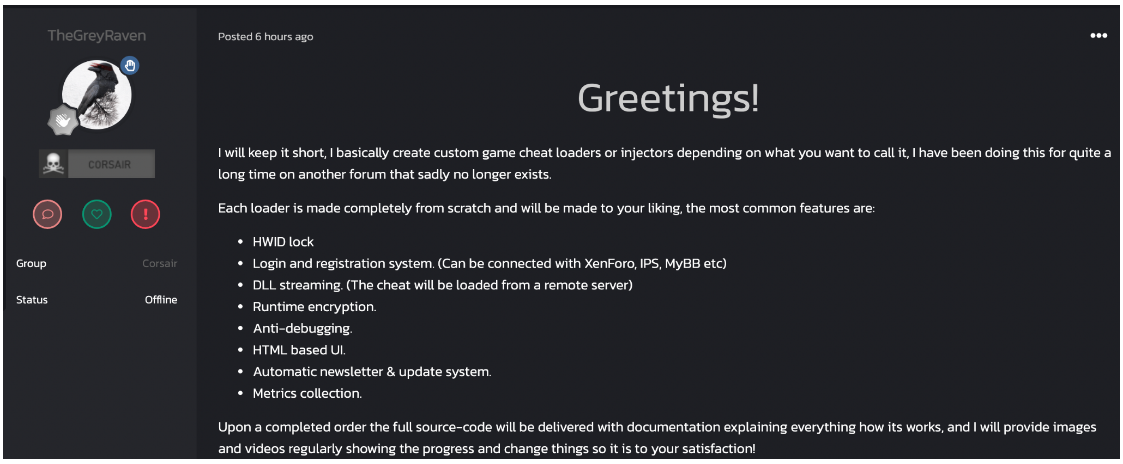
The first step to stopping a threat actor operation is to know your adversary, their motives, and means of operation. This section will provide a detailed description of the types of vendors engaged in the sale of gaming exploits.

The motive for any of these operations is assumed to be financial. The business of gaming exploitation is a lucrative one, demonstrated by the March 2021 raid of a China-based cheating ring with an estimated worth of **$750 million**.[3] However, the operation's size and tactics tend to differ, ranging from small, independent vendors selling one-time codes, professional vendors, and ongoing service-based vendors.

Individual vendors

The smallest, and often less sophisticated vendors of gaming exploitations are individual vendors. These are often members of cheating and hacking groups who collect or create cheat codes and cheating methods for sale. Given the independent nature of their operations, these vendors generally list their services in groups across social media, though they will also post in dedicated dark web forums. They typically do not run their own website and often use direct messaging platforms to facilitate a sale.

Shown below, an individual vendor promotes their services on a dedicated forum.



TheGreyRaven

CORSAIR

Group Corsair

Status Offline

Posted 6 hours ago

Greetings!

I will keep it short, I basically create custom game cheat loaders or injectors depending on what you want to call it, I have been doing this for quite a long time on another forum that sadly no longer exists.

Each loader is made completely from scratch and will be made to your liking, the most common features are:

- HWID lock
- Login and registration system. (Can be connected with XenForo, IPS, MyBB etc)
- DLL streaming. (The cheat will be loaded from a remote server)
- Runtime encryption.
- Anti-debugging.
- HTML based UI.
- Automatic newsletter & update system.
- Metrics collection.

Upon a completed order the full source-code will be delivered with documentation explaining everything how its works, and I will provide images and videos regularly showing the progress and change things so it is to your satisfaction!

A gaming exploiter promotes their paid-for services to hack games

[3] https://www.bbc.com/news/technology-56579449

Professional vendors

Professional gaming exploiters run more sophisticated operations, generally running dedicated websites across the clear web. These websites feature catalogs of cheating codes and software available for purchase, with packages and subscriptions to different cheats offered at a range of price points. These websites are professionally managed and are used as marketplaces which often leverage mainstream payment platforms to facilitate a transaction.

In some cases, these professional vendors will promote their products and services through dedicated social media posts, or use mainstream services marketplaces to sell their services.

“Cleaners:” unbanning services

A third type of gaming exploiter services is known in the exploitation ecosystem as “cleaners.” These individuals use sophisticated social-engineering techniques to bring a player who was previously caught by anti-cheating engines or moderators back into a game. While professional and individual vendors sell codes and hacks, these individuals sell a service that assists previously banned players rejoin their gaming platform of choice. This service is described in gaming forums as “unbanning” a player.[4]

[4] The online chatter about the safety of unbanning services is mixed. Many users recommend the use of these services, while others claim that they are in reality often fraudulent “unbanning” as-a-service scammers that seek to make a profit from defrauding cheaters.

Methods of game exploitation

While all exploitation vendors are motivated by potential financial gains, the types of services they offer vary greatly. ActiveFence has identified a wide range of cheating methods which threat actors can implement, ranging from in-game cheat codes to runtime game modification techniques.

These methods often capitalize on platform vulnerabilities and policy loopholes to provide users an unfair advantage. Trust & Safety teams must gain a deep understanding of these exploitations, identifying the vulnerabilities that are exploited to stop their abuse and maintain platform integrity.

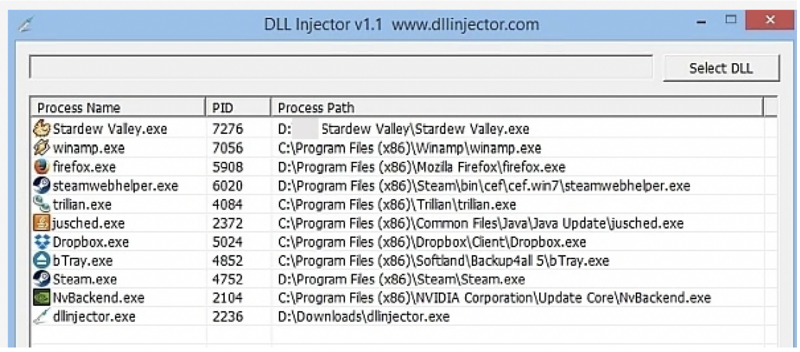
Runtime game modification

1. DLL Injection

> A DLL injection is a technique used for running code within the address space of another process by forcing it to load a dynamic-link library (DLL) file.

In video-game cheating, DLL injections are used to hack games, and then modify their rules to take advantage of a specific player during gameplay. Users can also access items that are behind a paywall, upgrading their avatar with additional in-game health, currency, and special abilities. ActiveFence has detected significant volumes of users sharing recommendations and advice on how to use DLL injections successfully, as well as advertise other fraudulent software for download.

Such runtime modifications undermine a company's earning potential. The damage is caused by the reduction of purchases through in-game stores, the loss of players due to degraded user-experience (in multiplayer settings), and the potential devaluation of digital assets (through the resale of illicitly acquired assets). Rapid intelligence about new codes developed by gaming exploiters for injection is essential to protect games from such harmful interference.



DLL Injector v1.1 www.dllinjector.com

Process Name	PID	Process Path
Stardew Valley.exe	7276	D: Stardew Valley\Stardew Valley.exe
winamp.exe	7056	C:\Program Files (x86)\Winamp\winamp.exe
firefox.exe	5908	D:\Program Files (x86)\Mozila Firefox\firefox.exe
steamwebhelper.exe	6020	D:\Program Files (x86)\Steam\bin\cef\cef.win7\steamwebhelper.exe
trilian.exe	4084	C:\Program Files (x86)\Trilian\trilian.exe
jusched.exe	2372	C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe
Dropbox.exe	5024	C:\Program Files (x86)\Dropbox\Client\Dropbox.exe
bTray.exe	4852	C:\Program Files (x86)\Softland\Backup4all 5\bTray.exe
Steam.exe	4752	D:\Program Files (x86)\Steam\Steam.exe
NvBackend.exe	2104	C:\Program Files (x86)\NVIDIA Corporation\Update Core\NvBackend.exe
dllinjector.exe	2236	D:\Downloads\dllinjector.exe

Examples of DLL Injector software for download

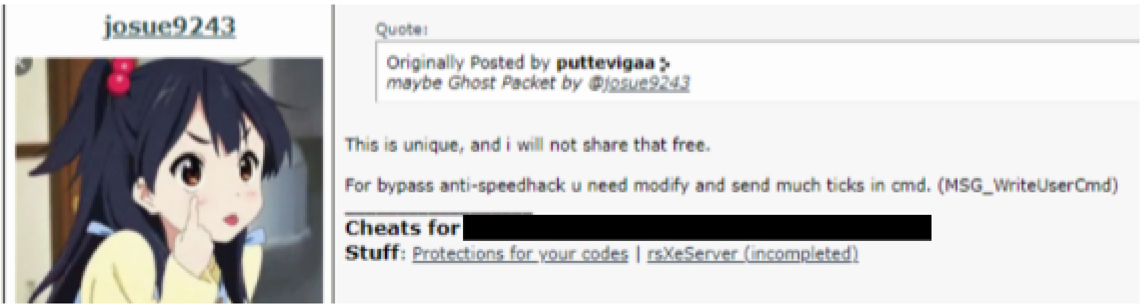
2. Cheat Engine (CE)

Cheat Engine is a relatively well-known software among gaming exploiters, which is frequently used to input cheat codes on popular gaming platforms. The software works similarly to DLL injections, but enables relatively novice users to exploit a games' code.

3. Game modification techniques

While many actors look for weaknesses in game's code to exploit, others create novel cheats by editing the game files while they are loaded in RAM, or by modifying a game's saved files to create favorable playing conditions. Below are examples of three known groups of runtime game modification techniques used to enable players to manipulate common core functions in video games to gain unfair advantages in gameplay.

- **Aimbot:** A cheat that allows players to shoot their enemies without having to aim their weapon, enabling them to shoot accurately without skill.
- **ESP** (**Extra Sensory Perception**): The cheat allows the player to see other players and items at all times. This gives the player using this a significant advantage over other players.
- **Speedhack:** Allows the player in the game to run or fly at high speed, providing an unfair advantage against other players in a multiplayer setting.



josue9243

Quote:

> Originally Posted by **puttevigaa**
> *maybe Ghost Packet by @josue9243*

This is unique, and i will not share that free.

For bypass anti-speedhack u need modify and send much ticks in cmd. (MSG_WriteUserCmd)

Cheats for [redacted]
Stuff: Protections for your codes | rsXeServer (incompleted)

A user in a cheating forum posts about selling a bypass to anti-speedhack

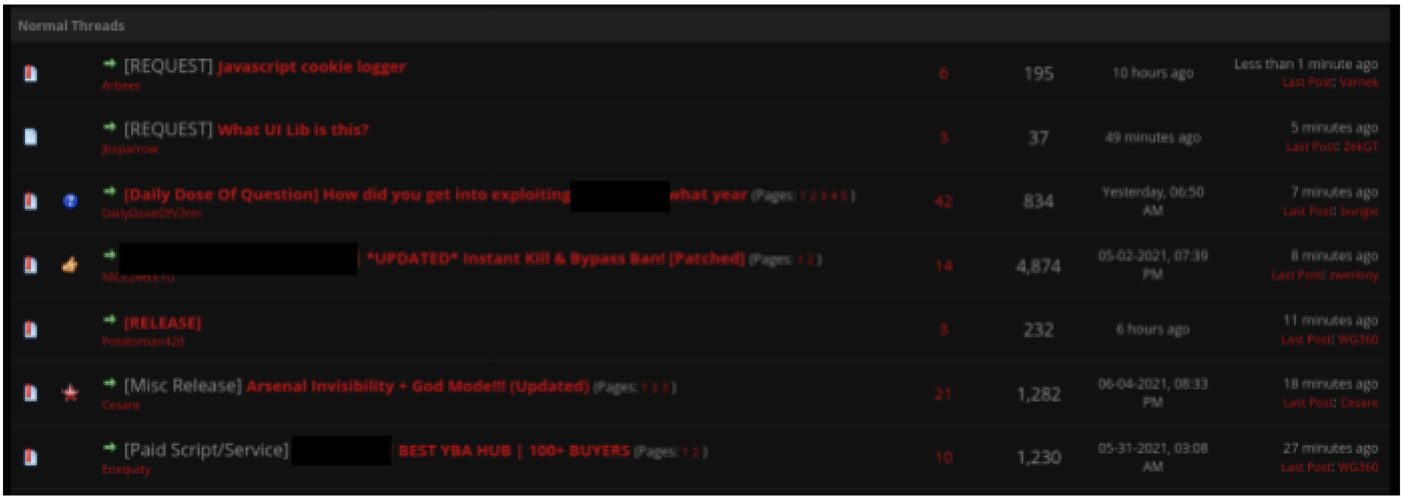
Distribution methods

Cheats are sold and distributed over many different platforms, ranging from dedicated forums to owned domains. To reach new clients, threat actors may also list their services in gaming-related social media channels on the clear web, though this occurs less frequently. Gaining full visibility of the services offered requires access to hidden forums and groups on the clear and dark web, as well as invite-only channels.

By tapping into these marketplaces, gaming platforms can identify new cheat trends and services as they are created and sold, enabling a proactive approach to stopping platform exploitation.

Forums

Forums and threads specifically dedicated to the sale and distribution of cheat codes and services exist on the deep and dark web. Members of these forums gather information about available codes, while participating in and searching for chatter emanating from threat actors who actively promote the sale of private, custom, and unique cheats for gaming platforms. Requests made on these forums usually specify the game and type of cheat requested.



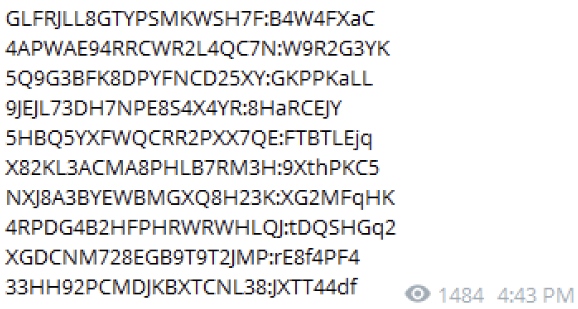
Normal Threads				
[REQUEST] Javascript cookie logger Arbees	6	195	10 hours ago	Less than 1 minute ago Last Post: Varnek
[REQUEST] What UI Lib is this? Jbsparrow	3	37	49 minutes ago	5 minutes ago Last Post: ZekGT
[Daily Dose Of Question] How did you get into exploiting [redacted] what year (Pages: 1 2 3 4 5) DailyDoseOfV3rm	42	834	Yesterday, 06:50 AM	7 minutes ago Last Post: bungie
[redacted] *UPDATED* Instant Kill & Bypass Ban! [Patched] (Pages: 1 2)	14	4,874	05-02-2021, 07:39 PM	8 minutes ago Last Post: zwenboy
[RELEASE] Potatoman420	3	232	6 hours ago	11 minutes ago Last Post: WG360
[Misc Release] Arsenal Invisibility + God Mode!!! (Updated) (Pages: 1 2 3) Cesare	21	1,282	06-04-2021, 08:33 PM	18 minutes ago Last Post: Cesare
[Paid Script/Service] [redacted] BEST YBA HUB | 100+ BUYERS (Pages: 1 2) Enequity	10	1,230	05-31-2021, 03:08 AM	27 minutes ago Last Post: WG360

Hacking forum where users are discussing cheats and exploits for online games

Social media and instant messaging communities

Social media platforms are often abused by gaming exploiters who seek to promote their services to new clients. These individuals are active within dedicated communities, through which they are able to evaluate the effectiveness of specific cheating methods and advertise various products. An additional “advantage” of promoting these services on social media platforms is that it allows these cheats to be accessed by even the most novice player, and effectively normalizes this harmful activity.

Unmoderated instant messaging platforms are also frequently used by actors to sell cheat codes. ActiveFence has mapped numerous dedicated channels and groups that have significant numbers of engaged users. In many of these channels, free and paid cheat keys, hacks, and methods are shared and distributed.



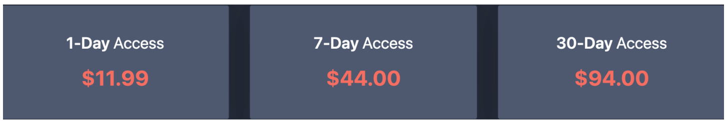
```
GLFRJLL8GTYPSMKWSH7F:B4W4FXaC
4APWAE94RRCWR2L4QC7N:W9R2G3YK
5Q9G3BFK8DPYFNCD25XY:GKPPKaLL
9JEJL73DH7NPE8S4X4YR:8HaRCEJY
5HBQ5YXFWQCRR2PXX7QE:FTBTLEjq
X82KL3ACMA8PHLB7RM3H:9XthPKC5
NXJ8A3BYEWBMGXQ8H23K:XG2MFqHK
4RPDG4B2HFPHRWRWHLQJ:tDQSHGq2
XGDCNM728EGB9T9T2JMP:rE8f4PF4
33HH92PCMDJKBXTCNL38:JXTT44df
```

Example of cheat codes, which are frequently shared in unmoderated messaging platforms

Dedicated marketplaces for cheat codes and hacks

Run by professional vendors of gaming exploitations, marketplaces are dedicated websites that operate as stores, selling cheating and hacking products for popular games. These cheats are created by the vendor operating the store, and are customized to the specific game.

Services are offered as packages based on the enabled functionality, the game build, and the operating system on which it’s run. Pricing for these packages varies by the options chosen and the duration of access, with daily, weekly, or monthly packages available. An additional type of service is a one-time “cheat key” (also referenced as “keys”), which is used by dedicated software to enable the player to modify their statistics in a game.



1-Day Access	7-Day Access	30-Day Access
$11.99	$44.00	$94.00

Example of hack pricing, ranging from $11.99 for one day, to $94.00 for 30 days

Another service offered on these sites is scripts which are used to carry out fraud through spam or manipulate in-game mechanics, allowing players to cheat. These actors also sell methods to log into games remotely, bypassing the platform's detection of suspicious account activity. These sites are hosted on mainstream website hosting and payment processing platforms, but can only be reached using the URL links shared on hacking forums.

Mainstream services marketplaces

Threat actors are not only using dedicated domains, forums, and social media platforms to promote the sale of cheating hacks. ActiveFence has also identified that users are abusing mainstream services marketplaces to sell cheating hacks directly to users. This activity is especially damaging, as the use of mainstream services to promote gaming exploitation provides a sense of legitimacy to this damaging activity.

Selling digital assets on the black market

As discussed in **Volume 1**, there are many online marketplaces that specialize in the sale of online gaming accounts.

ActiveFence has identified that gaming exploiters often use various cheats and exploitations to modify these accounts, and then resell them in virtual marketplaces. By selling these modified accounts, threat actors essentially undercut the market, bypassing the game's official stores, an act that not only cuts the gaming platform's potential profits, but may lead to the drastic devaluation of digital assets.

Conclusion

The financial risks identified in this report are consequential for the business models of video game companies. Platforms that are regularly abused by players who manipulate games to acquire an unfair advantage over competitors, will see legitimate users migrating to those where the playing field is even. The loss of players will naturally reduce the monetization possibilities within a game. Added to this issue of player retention, we've highlighted how users can abuse the coding of video games to access items that are chargeable, undercutting and devaluing the in-game stores.

While the threats facing video game platforms are complex and advanced, a proactive based approach can allow platforms to act fast and reduce their exposure. To learn about how our AI-powered technology and intelligence experts identify threats as they emerge, please contact research@activefence.com.

Proactive Online Integrity

ActiveFence is the leader in online integrity, protecting billions of people worldwide from disinformation, child abuse, terror, hate speech, fraud and other online harms. The company's customers include trust and safety teams at some of the world's leading technology platforms. ActiveFence empowers these and other abuse prevention professionals with a unique, proactive approach to the detection of and protection against malicious activities on the internet. By searching across the darkest corners of the web where bad actors chat, share and plan, ActiveFence spots known and unknown threats to online platforms before they reach the platforms themselves and cause real damage. Backed by leading investors, ActiveFence numbers almost 200 employees globally—all working together towards the shared mission of enabling a safer world by preventing online evil.

ActiveFence