ActiveFence

The Cheating Industry:

Unmasking sophisticated cheating enterprises

March 2022

Unmasking Cheating Enterprises

Gaming companies are being abused by fraud actors creating and selling cheat codes. This activity, which is estimated to cost companies ~$29B in lost revenue, is perpetrated by coordinated criminal enterprises that capitalize on the popularity and success of the gaming industry.

Today, the average user can easily access and purchase cheats online, with vendors promoting their activities professionally.

This damaging activity has financial consequences for the exploited services, causing:

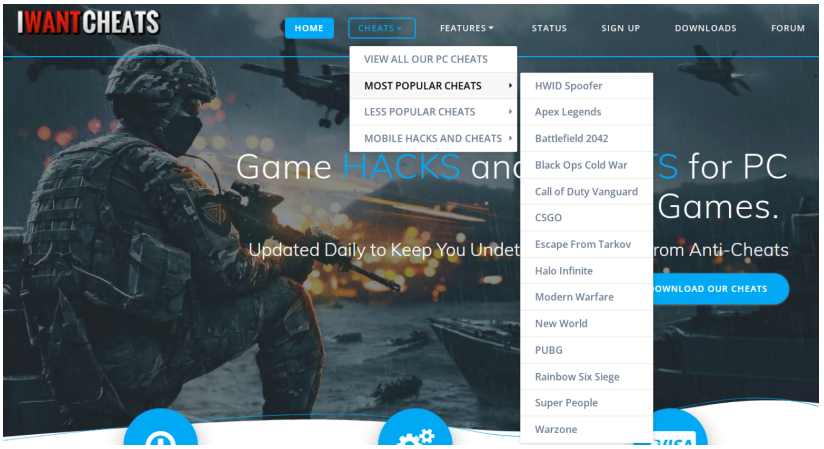
- **The loss of revenue from in-game stores:** The fraudulent acquisition of in-game tools and digital assets prevents platforms from selling such digital goods through their in-game store.
- **Devaluation of digital assets:** The sale of digital assets acquired fraudulently can see platforms undercut, 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 draws upon ActiveFence's intelligence coverage to demonstrate the sophistication of those enterprises promoting their exploitation of the gaming industry. This is important as it is only by understanding the mechanics of cheat enterprise operations that they can be identified at scale and their methods and tactics be countered.

Cheat Enterprise Quasi-Legitimate Activities

Promotion on Social Media and Video

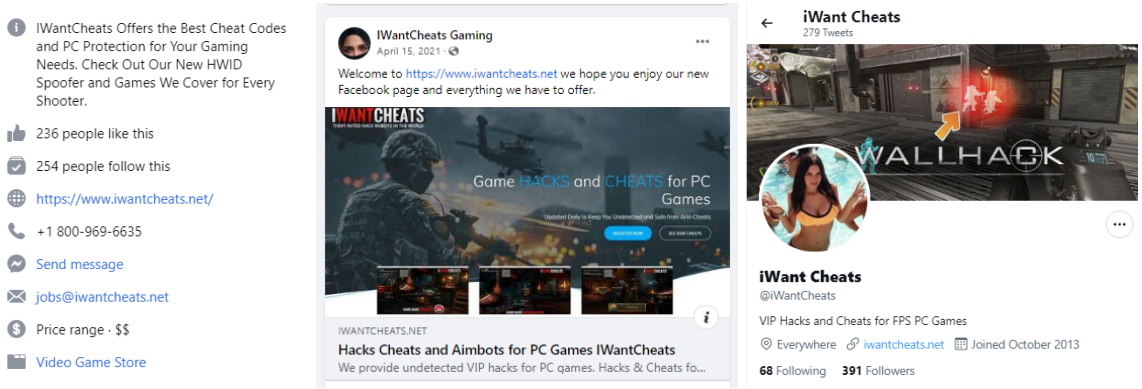
IWantCheats (IWC) is a sophisticated enterprise that sells commercial cheats, hacks and add-ons to gaming users. It operates an e-commerce website, forum as well as multiple social media and other digital entities to promote its products and services.



IWantCheats website screenshot

ActiveFence was able to detect this enterprise from multiple nodes in its promotional network. These included social media and video-hosting accounts that promote cheats for specific games, either in posts utilizing hashtags that refer to popular games, or as videos. These accounts are active on mainstream platforms and are used to post links to **iwantcheats.net.** The network activity is particularly interesting on video-hosting platforms, where both individual gamers and official enterprise accounts have uploaded video content to demonstrate the effectiveness of IWC cheats.

To garner trust, the operators not only display positive reviews on their main website, but also have a Customer Reviews thread on its forum, which is sorted by the different cheats offered. In addition, IWC owns business accounts on **Trustpilot** and **reviews.io** to collect and present customer reviews. Both of these accounts link to the IWC domain.

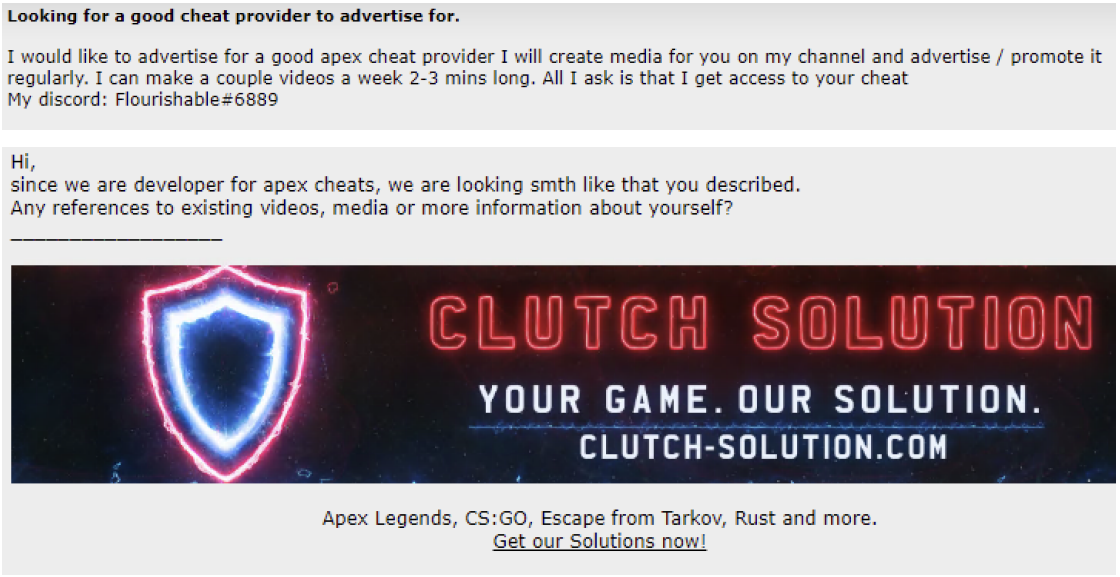


IWantCheats off-domain online entities

Use of Paid Influencers

Recently, ActiveFence has detected a new phenomenon of cheating enterprises seeking out gaming live-streamers who will sell promotional videos. These promotional livestreams advertise newly released cheats or other in-game assets such as coins and skins, and are arranged through black market forums.

To demonstrate this activity, ActiveFence assessed the chatter from one such forum. We identified a user seeking out a cheat enterprise that created cheats for a specific game. The user shared a post titled, **Looking for a good cheat provider to advertise for**. In return for access to cheating services, they offered to make a number of two to three minute videos each week to promote the cheat enterprise. The user was contacted by a representative from **Clutch Solution**, enquiring about references to proceed.



[Top] Cheat enterprise seeks users willing to promote their website on social media;
[Bottom] User promotes on Gaming Black Market his SMM services

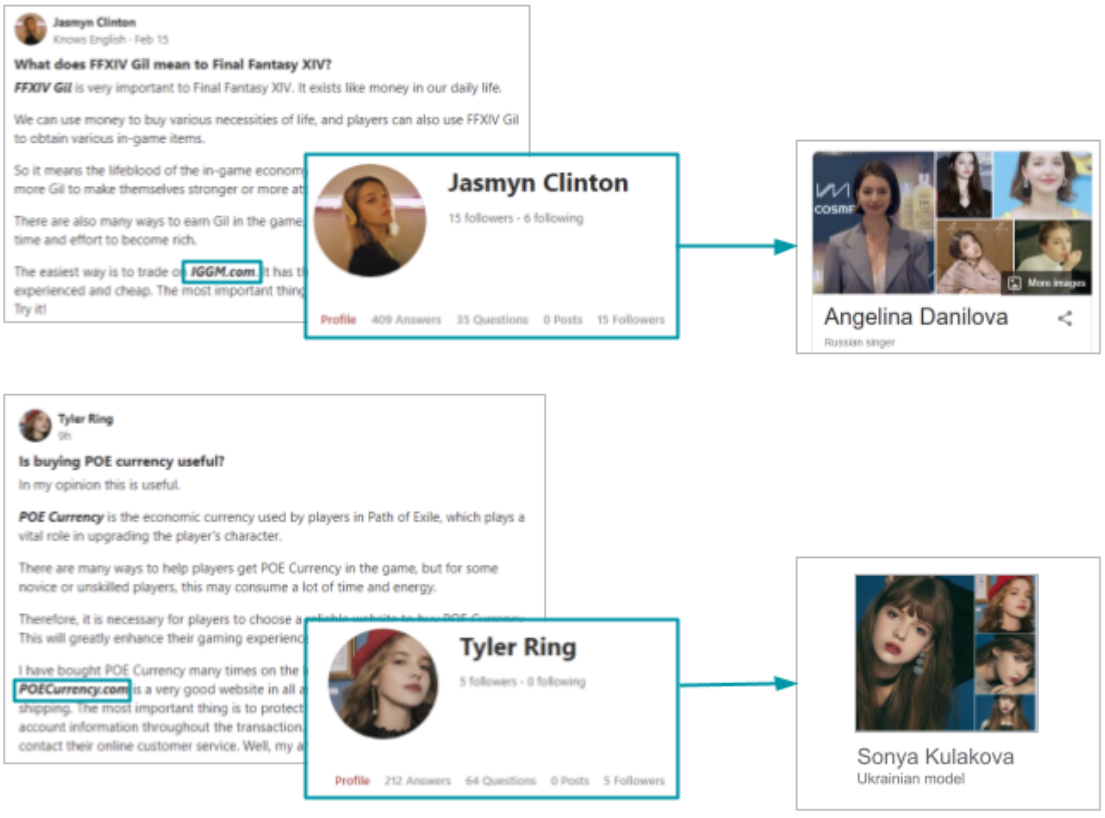
Automated Promotion at Scale

Cheating enterprises have developed their promotion of their products in an increasingly lucrative and competitive market. This promotional development has extended from the maintenance of a website, to the possession of social media entities, and now includes the use of coordinated inauthentic networked accounts that share farmed reviews.

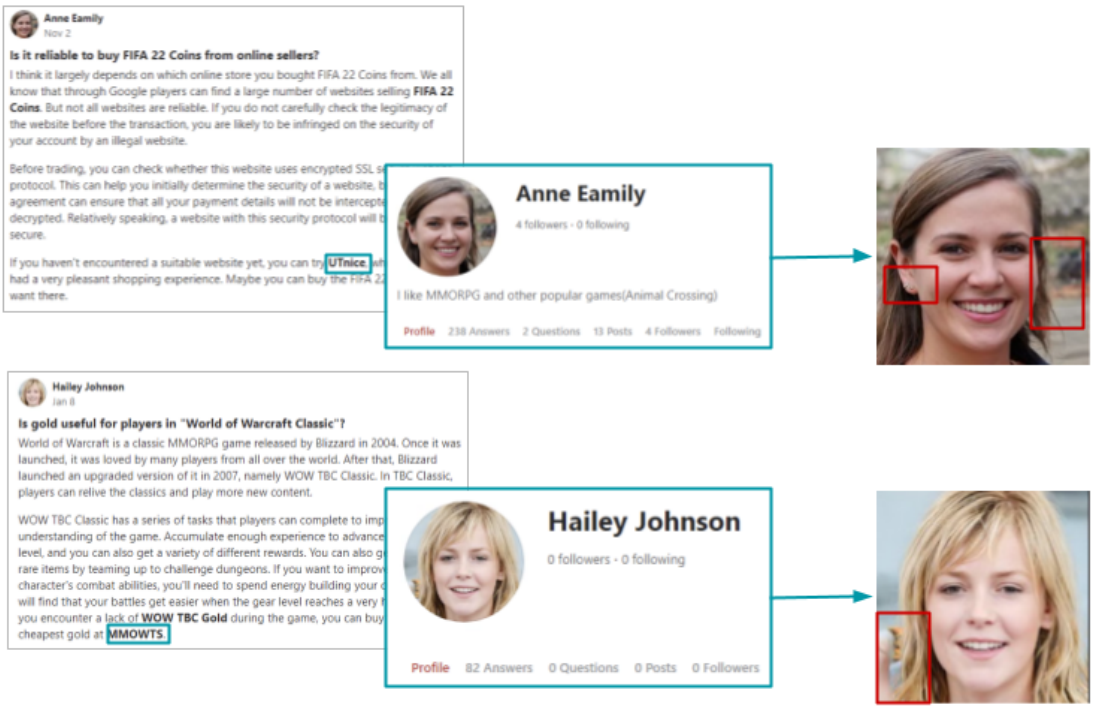
Coordinated Inauthentic Behavior (CIB)

It is essential for cheating enterprises that potential clients believe that their work is high quality, will not lead to their account being banned, and that they will not be defrauded. As a result, enterprises seeking to engage with prospective customers utilize bot networks that are active on social media.

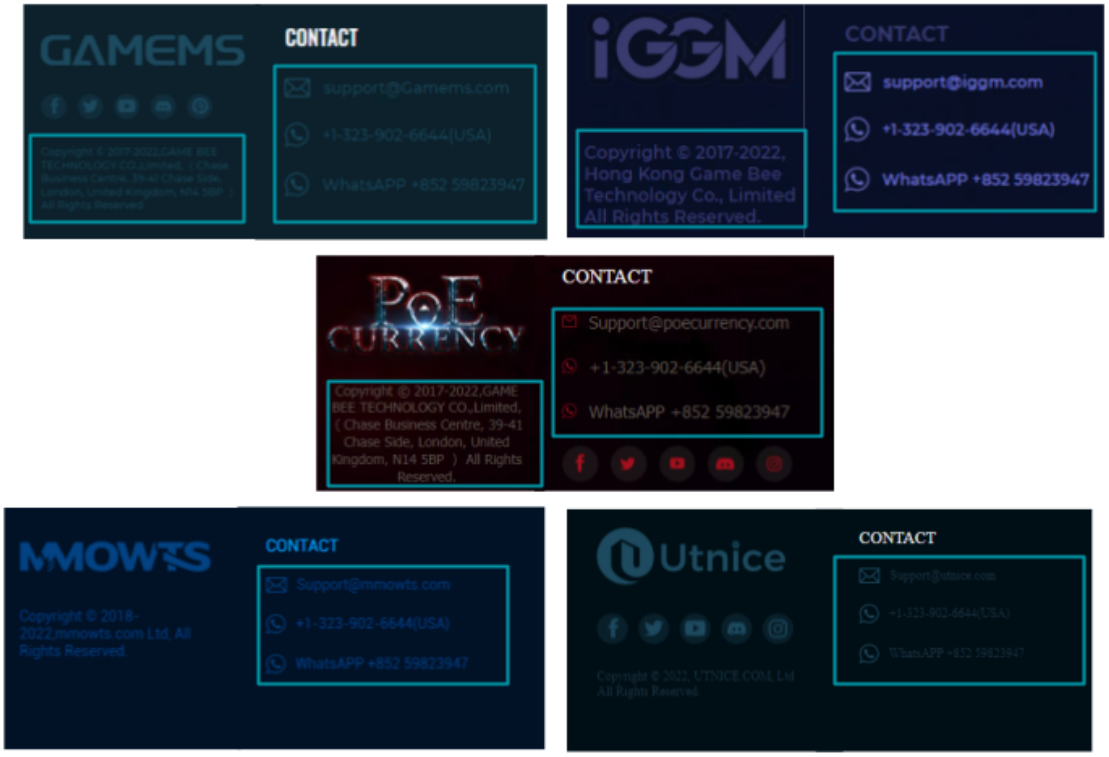
ActiveFence has identified a network of inauthentic accounts that operate on one question-and-answer social website to promote multiple associated domains of cheating enterprises. These accounts utilize high quality images to appear authentic. However, when their site activity is analyzed, it is apparent that all their questions and comments are repeated, and they use near-identical quotes in their text. Their profile pictures are either taken from the internet, or appear to be computer generated.



Inauthentic accounts promoting different websites associated with the network, which use stolen images



Inauthentic accounts promoting different websites associated with the network, which use suspected GAN images[1]



Five websites promoted by the bot network. These sites all present overlapping contact information

[1] Images created by generative adversarial networks (GAN) are artificially generated.

Next Steps

As the gaming industry grows, those seeking to exploit it will develop sophisticated methods to perpetrate abuse. However, these gaming exploiters need not have a free reign. ActiveFence's intelligence capabilities allow us not only to detect cheat enterprise networks, but also new targets and TTPs employed by these networks.

These insights enable our partners to secure their platforms from trending abuse, and understand when and how they are targeted for abuse. ActiveFence helps our partners take decisive proactive action to counter and disrupt the business of enterprises selling cheats and hacks, and secure their games long into the future.

For more information on ActiveFence's work to secure the gaming industry, please contact sales@activefence.com.

The proactive approach to online integrity.

ActiveFence is pioneering the proactive approach to online integrity, and empowers the world's leading Trust and Safety teams to secure their platforms. ActiveFence protects billions of users across the world, in over 70 languages, from child abuse, disinformation, fraud, hate speech, spam and terror as well as other online harms and unwanted content. With a unique intelligence based, cross-platform approach, ActiveFence gathers multi-source data to detect threat actors and identify dangerous networks trying to abuse our partners' services.

ActiveFence is backed by leading Silicon Valley investors such as CRV and Norwest, raised $100M to date, and employs over 250 people worldwide.

ActiveFence