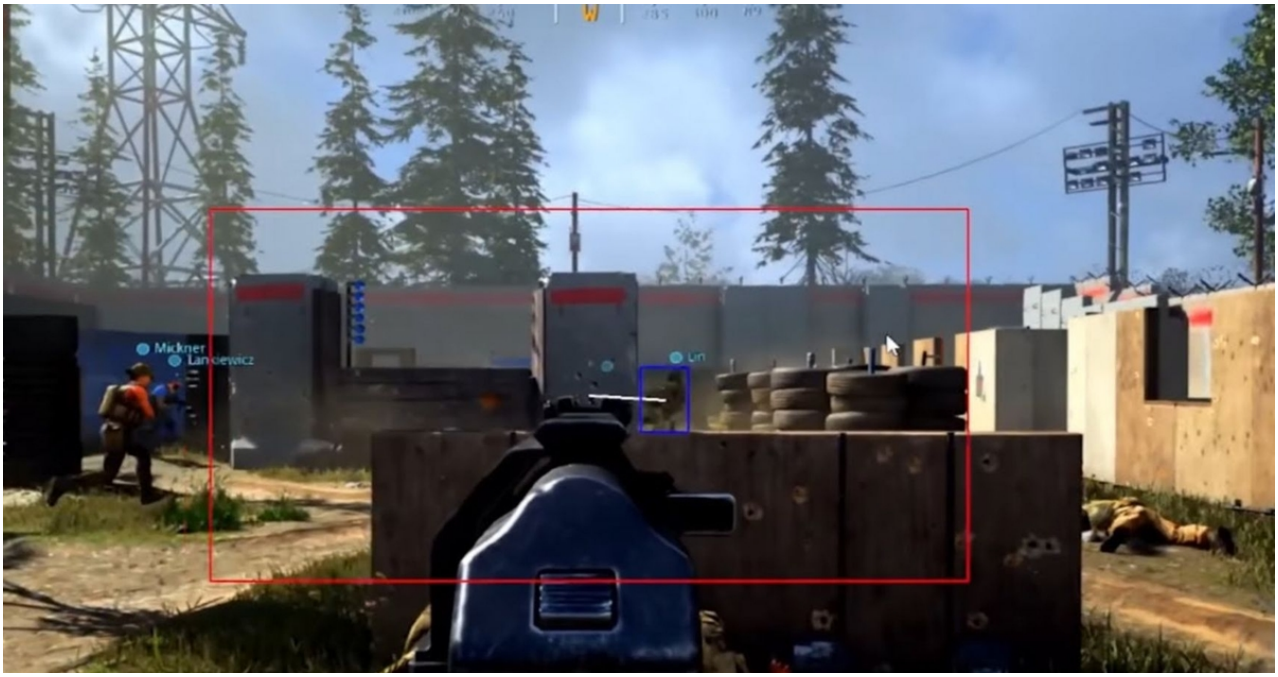
AI is Driving the Next Generation of Video Game Cheats & Exploits

aibusiness.com/computer-vision/ai-is-driving-the-next-generation-of-video-game-cheats-and-exploits



On August 11, Raven Software, one of the lead development studios behind the immensely popular Call of Duty: Warzone online video game, announced it had banned 50,000 player accounts.

The reason for the bans was simple – cheating. Tens of thousands of users had circumvented the game's mechanics to get an unfair advantage.

Warzone remains rife with cheaters making use of exploits to take down their opponents with ease. 'Aimbots,' common exploits used in first-person shooters, have turned the battle royale game into a cacophony of angry players.

Back in the heyday of Call of Duty, when Modern Warfare 2 and Black Ops ruled the waves, the biggest issue was excessive grenade launchers. Nowadays, there's something far more technological causing players to rage than 'noob tubes' — AI, and specifically, computer vision and emulated input devices.

A new kind of aimbot has taken games like Warzone and Apex Legends by storm. It uses computer vision to identify enemy players in a complex game world and then signal the player to shoot at a specific location.

Players use a PC to process the video feed from their games console, and then run the automation and machine learning scripts; they would also connect the console's controller to the PC via a hardware device, to emulate the controller's signals.

Players can set the extent of aim assist, and even input the system to select specific target zones on enemy bodies – headshots included.

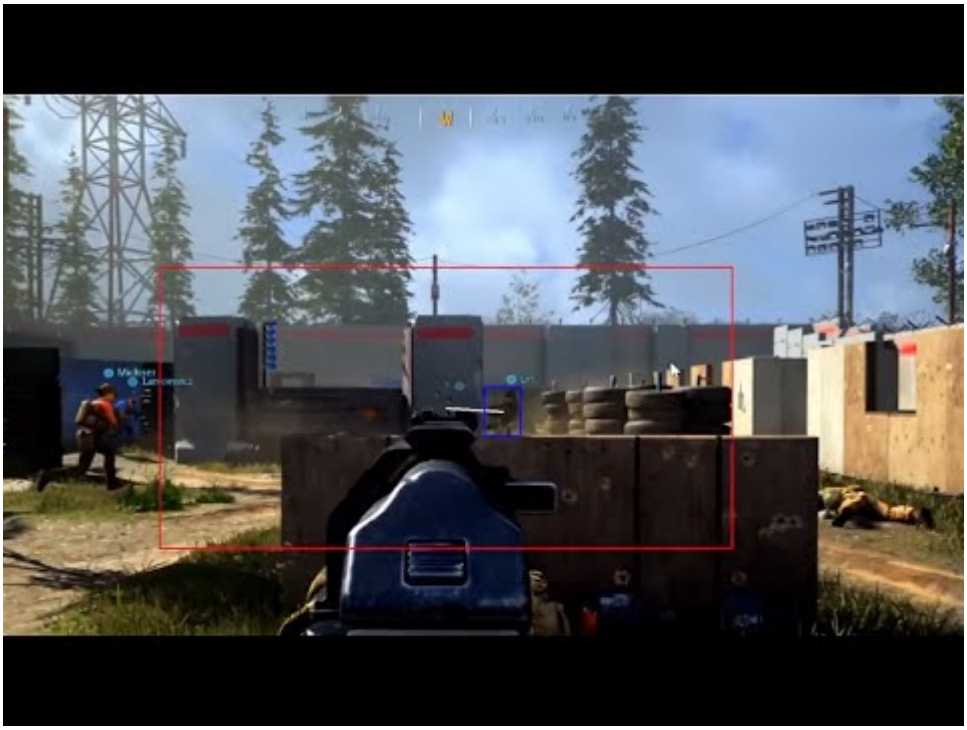
Warzone has been besieged by hackers since its debut in March 2020, with developers claiming hostile programmers were "ruining some of the best work" of their lives. And the fear of this new technological terror saw CoD publisher Activision request a cheat developer take down their AI-based exploit – successfully.

Dubbed "the next generation of cheating," Userviz was down, but AI-based aimbots aren't out yet. Just days after the news of Activision's request broke, AI Business was contacted by a Twitter user who created a proof of concept video for console cheats.

Sjas0a32 said they had trained an AI system in just two days "to show how far object recognition in games really is."

While the video looks like a simple system trained to draw bounding boxes on video – the overall idea can strike fear into the heart of any online gamer.

AI Business spoke with video game experts to see if such fears are justified, or about as grounded in reality as that infamous Infinite Warfare trailer.



Watch Video At: https://youtu.be/fk5MQOZRoWw

Short primer on video game cheats

Cheats were initially included in games as a way for developers to allow players to access deviations from the traditional in-game experience.

In some instances, these were gimmicks, like the unlimited money cheat from The Sims, or Doom's invincible 'god mode.' Players would simply input a code in a preset menu in order to get access to new features.

The first alleged video game cheat dates back to 1971's Computer Space, a coin-operated arcade game. Should the player hold down the two buttons on the left while the machine boots up, they could access the game with a top score.

Cheating itself isn't limited to players – developers would use the same commands to debug games.

And exploits that mess with the software itself aren't new either. In the grand old days of video games, plugin devices like Game Genie could edit the contents of games – much to the irritation of copyright holders and developers.

We get dirty and the world stays clean – that's the mission

Sometimes, a game becomes too broken because of cheaters. Take PlayerUnknown's Battlegrounds, notorious for players scoring endless, unlikely kills. In some instances, the allure of cheating software is also used by hackers to install trojans on would-be cheaters' PCs.

And if you were to revisit an older title like Call of Duty: World at War, you'd be greeted with players teleporting around the map, shooting you through walls, and calling in endless killstreaks to make your playtime a living hell.

Sometimes, enough is enough: a few gamers have taken the initiative to sort things out themselves. The Anti-Cheat Police Department Twitter account is run by a group of players that gather intelligence on cheats to detect and disrupt their development and distribution.

They're not affiliated with any publisher or developer – just a group of volunteers seeking to prevent cheats from getting out of hand.

The ACPD told AI Business that AI-based cheats have been around for a while – and can be monitored at will, if need be. The community is more concerned about memory-based cheats, specifically, those that work on the kernel-level, and type one hypervisor cheats that the makers of Call of Duty can't stop or even detect.

"We are focusing way ahead of the game while game companies, even with a kernel-level anti-cheat, can't detect various kernel cheats due to lack of talent and skill, and Call of Duty [with its] user-mode anti-cheat is a lost war already from the start."

So what's the ACPD's ideal method of tackling the problem? They pointed to Valorant, the free-to-play shooter, and praised developers Riot for their work in this area. When you download Valorant, Vanguard, an anti-cheat software application, is installed. It runs in the background, scanning your PC to check if you're running any cheat software while you play.

“Don't get me wrong, they have cheaters, but you meet them once in 500 games, and I’ll take those odds over any game I have played. Personally, never met a cheater since the launch of Valorant,” the Anti-Cheat Police Department said.

“They must be doing something correctly that other game companies aren't. Riot has delivered on their promise of a strong anti-cheat which is honestly unexpected.”

Your Honor, the defense is ready to present!

Developers could opt for the legal route to take down cheaters. Epic Games, the makers of the cultural phenomenon that is Fortnite, successfully litigated against a cheat seller.

Grand Theft Auto Online’s parent company, Take-Two Interactive, did the same – forcing the cheat maker to pass any profits on to charity.

The ACPD suggested the legal option requires time, money, and “a s**t-ton of investigative work” to find out who is behind a cheat, or the shop selling them.

Someone who knows full well about the difficulties of lawsuits involving video games is Nick Kempton, an IP lawyer from Osborne Clark. A gamer himself, Kempton has previously advised high-profile video game publishers and developers in respect to IP claims, particularly in contractual disputes with distributors and license holders.

The lawyer noted that sophisticated cheats like Userviz “are becoming quite a big issue for developers and publishers.”

“Thanks to new trends we're seeing around growing popularity in esports and streaming player content, there's this greater emphasis on competitive online gameplay.

“These cheats are affecting the balance within a game. One of the greatest challenges for game developers is fine-tuning an ecosystem to find a balance between items and weapons. That can be an internal pressure – but external pressures that also come on top of that are from third-party hackers developing cheat software.”

Kempton said that like most things in the legal world, the action developers can take is dependent on several factors. Cost, the jurisdiction of bringing the action, and what you're trying to achieve are all considerations developers and publishers need to take on board when deciding to take down cheaters through litigation.

He pointed to disruption tactics, like a notice and takedown regime, or sending a letter of complaint to a website host.

“These tend to be cheaper options,” Kempton said.

In the case of Activision, reaching out to the Userviz developer was enough. Bungie, the studio behind mammoth game franchises Halo and Destiny, managed to do the same with just a cease-and-desist letter.

But if a belligerent cheat provider refuses to comply, full-blown litigation, which can be costly and time-consuming, might be a game company's only option, said Dorsey & Whitney lawyer Ryan Meyer.

Upon reacting to the growing concern around AI and ML-enhanced cheats, Meyer reminded that console players are no longer safe from the once PC-dominated labyrinth that was exploits in video games.

“By connecting a PC with the right kind of capture card to a console, players can use machine learning to cheat on console games as well,” Mayer said – which is exactly what the Userviz cheat implemented.

Further outlining the steps games companies can take to quell the cheaters – he too pointed to tools like Valorant’s Vanguard.

And while no single anti-tampering measure is likely to be 100 percent effective all the time, the industry is evolving to potentially deploy AI to more accurately detect and ban or label cheaters.

Last November, computer scientists from the University of Texas at Dallas developed an AI-powered anti-cheat system design to detect exploits in the shooter game CS:GO.

With its developers currently employing Valve Anti-Cheat (VAC) software, the project sought to one-up the major games publisher – creating an AI-based anti-cheat system that can work in any MMO (Massive Multiplayer Online) game.

Detecting cheating in MMO games can prove tough since the data that travels from a player's computer to the game server is encrypted.

The research team opted to eliminate the need to decrypt data – with their system able to analyze encrypted traffic to and from the server in real-time.

"Players who cheat send traffic in a different way," said Dr. Latifur Khan, lead author of the study. “We're trying to capture those characteristics."

The video game industry has survived a lot – the crash of 1983, shady near-gambling mechanics for loot boxes, Gamergate, and increasingly devious microtransactions.

While AI-enhanced cheats do pose a threat, the likely reality is that they will make another notch on the industry’s ban-hammer.

Since penning this article, Call of Duty’s makers have promised there will be an anti-cheat software included in the next installment of the franchise, Vanguard, shipping this December.

Never before has a publisher advertised anti-cheat capabilities as a major selling point for a AAA title. But then there’s never been cheats quite like these.

And whether it’s through the hard work of groups like the Anti-Cheat Police Department, legal efforts led by lawyers like Kempton and Meyer, or fighting fire with fire via AI-based anti-circumvention measures, the video game industry will endure and thrive.

About the Author

Ben Wodecki

Ben Wodecki is the Jr. Editor of AI Business, covering a wide range of AI content. Ben joined the team in March 2021 as assistant editor and was promoted to Jr. Editor. He has written for The New Statesman, Intellectual Property Magazine, and The Telegraph India, among others. He holds an MSc in Digital Journalism from Middlesex University.