Use Case:

How Criminals are Profiting from Cheaters and Destroying Games
WHAT IS THE MOTIVATION TO CHEAT IN VIDEO GAMES?

“The more people win, the more likely they are to cheat; and the more they cheat, the more likely they are to win,” said Amos Schurr, professor of psychology at Ben-Gurion University of the Negev in Israel.

When you put humans in an environment where there’s competition, people are motivated to win at all costs. From Russian athletes doping for the 2016 Olympics, to the Enron scandal, to Watergate, to the steroid era of professional baseball, people have been cheating to get ahead since the beginning of time. While there aren’t gold medals or presidential wins at stake, cheating platforms and tools in online video games are proliferating as fraudsters increasingly recognize the massive financial benefits associated with selling cheats and hacks to gamers who want to gain an unfair advantage over their competitors.

Today, cheating in video games primarily occurs through hacking, or modifying the game client itself. Video game hacks are readily available for free or sale online, and enable botting, including auto-leveling and goldfarming, and straight-up cheating. Automation (i.e. botting) hacks facilitate around-the-clock game play designed to quickly level up characters or amass in-game virtual items and currency, a process known as gold farming. Virtual items earned this way can be used to make a character more powerful, or can be sold for real-world money on the gray market - a technically legal, but very shady underground business.

In addition to botting, hacking the game client allows cheaters to get around core rules and controls designed to keep games fair for all players. For example, a hack may allow players to move through the virtual world faster than other players or reach inaccessible locations. Other hacks enable cheaters to see through walls, or pull off nearly-impossible head shots with inhuman precision.
WHAT’S THE MOTIVATION? (cont’d)

At their worst, game client hacks have the potential to defeat core privacy and login controls, opening up players’ game accounts to account takeover, virtual item and currency theft, credit card fraud, and identity theft. Worse, many hack programs – regardless of whether or not they actually deliver the competitive advantage they promise - are also delivery vehicles for malware that quickly and comprehensively compromise the player’s computer or mobile device with the goal of exposing the user’s stored login and security credentials, from email and banking, to ecommerce.

So, what is the motivation for cheating? It most often involves individual players’ frustrations. If a player determines that the game itself is too difficult, or that the players faced in player-versus-player matches are too hard to defeat, that individual can purchase a hack that offers a competitive advantage over players using an unaltered version of the game. Even if there is no financial gain, players will actually pay a lot of money to gain access to the latest build of a hacked client. Further, the more lucrative cheating platforms offer subscription services, where players pay a monthly fee in exchange for regular updates to game cheats and hacks. 

Unfortunately, this turns into a cat-and-mouse game between hackers and video game developers and publishers. Good players soon grow frustrated as they continually lose battles to god-like opponents who never seem to miss. Eventually, good players leave the game, taking their money and goodwill with them.

Yet, despite increasingly shrill warnings about the dangers of using unauthorized hacks, as well as pleas from publishers begging players to be honorable and play fair, new cheats for successful games are being released faster than ever before. Game developers understand that the client is a weak link in the chain, but combatting these vulnerabilities and getting ahead of hackers has proven incredibly challenging. While game publishers have taken on the strategy of continuously updating the client to cut off hackers, they are not able to do it fast enough to keep ahead of the agile, motivated, and resourceful team of cheat sellers who are poised and ever-ready to take advantage of online video games’ vulnerabilities.
HYPOTHEtical USE CASE: The Rise & Fall of HoneyPot

HoneyPot, a new MMO with a small base of a few thousand loyal players, was developed using a popular, commercially available game development toolkit. The game is free to download and play, and its revenue is dependent on micro-transactions from players willing to pay for small cosmetic upgrades, character costumes and animations, and other features that the developers have carefully chosen to offer at certain points during gameplay.

Recognizing weaknesses in HoneyPot’s game client, and the potential popularity of the game, hackers developed an application that provides players with automation-based cheats that help them build top-level characters with minimal effort. The hack application is also riddled with malware, which silently embeds itself in both the PC and mobile devices that run the game client.

Through smart marketing, continuous community engagement, and a series of glowing player reviews, HoneyPot gains mass traction and becomes a viral success with more than half a million daily active players. However, the in-game automation cheats developed in the game’s earliest days are still viable and more attractive than ever to the growing number of players seeking an unfair advantage. The hack authors also realize that these same automation tools can be used to create a widespread gold farming operation for the game’s in-game currency, and quickly spin up large numbers of free-to-play bots, which begin running around the clock.

As more and more cheaters enter the game and begin to compete against similarly superhuman opponents, cheating subscriptions surface with even more players paying to gain unfair advantage in the game. Normal players, unable to compete, begin to get squeezed out. Popular YouTubers and top-ranked player guilds release videos complaining about the cheating situation and call on the developer and publisher to do more to protect the game world and its players.

Meanwhile the developer, already struggling to create new content to keep up with player demand, begins to feel pressure from the publisher to fix the security holes, hacks, and cheats that are eroding the game’s financial performance. Instead of spending their time building new game features, the developer becomes mired in a never-ending list of tasks to help the publisher track down and ban bad player accounts and patch game client vulnerabilities upon which the hackers have built their tools.
Introducing a better solution: Watchtower from Panopticon Laboratories is the first and only in-game security product that provides video game publishers with a 360-degree overview of player behavior over time. Using proprietary anomaly detection and behavioral analytics, Watchtower enables video game publishers to identify and alert on suspicious behavior, such as cheating, by modeling normal, historic player behavior and looking for activity that varies from what is normal. The SaaS-based product's real-time, actionable alerts and research tools allow analysts to make quick and informed decisions that stop malicious in-game behavior before damages can occur.

Hackers and fraudsters are expert liars, but history never lies. Historic player behavior can be a powerful tool in a game operator’s arsenal, but only when it can be easily accessed and interpreted. Contact us today for a Watchtower demo or to get started. Don’t let cyber criminals ruin the gaming experience for your players.

Contact us for a Watchtower demo today.
sales@panopticonlabs.com

The Rise & Fall of HoneyPot (cont’d)

Soon, loyal players begin to grow frustrated and begin questioning whether the game’s developers care about anything except making money. The truth, however, is that the developer’s manual remediation process takes much longer than it does for the bad guys to hack the updated game client, pushing the developers further and further behind. It’s a vicious cycle that leaves the players frustrated and the publisher strapped for in-game revenue.

As frustration grows, honest players begin to abandon the game and, as a result, the game essentially becomes cheaters playing against other cheaters until the game goes under for good. The hackers simply move on to another, similar game where the same tools and techniques used against Honeypot will likely prove equally effective.

Unfortunately, HoneyPot’s story is not isolated. In fact, it’s trending to become even more prevalent with the growing popularity of player-versus-player game modes, the ever-increasing skill of hackers, and the proliferation of real-world money flowing through online games. Cybercriminals know that cheating in online video games is financially and reputationally damaging to the developers, and that it ruins the gaming experience for the players, but they simply don’t care. For them, games are simply another business opportunity, one that they will keep exploiting to its fullest at everyone else’s expense until they are forced to stop.

DISCOVER ANOMALOUS IN-GAME BEHAVIOR & QUICKLY REMEDIATE RISK

Introducing a better solution: Watchtower from Panopticon Laboratories is the first and only in-game security product that provides video game publishers with a 360-degree overview of player behavior over time. Using proprietary anomaly detection and behavioral analytics, Watchtower enables video game publishers to identify and alert on suspicious behavior, such as cheating, by modeling historic player behavior and looking for activity that varies from what is normal. The SaaS-based product’s real-time, actionable alerts and research tools allow analysts to make quick and informed decisions that stop malicious in-game behavior before damages can occur.

Hackers and fraudsters are expert liars, but history never lies. Historic player behavior can be a powerful tool in a game operator’s arsenal, but only when it can be easily accessed and interpreted. Contact us today for a Watchtower demo or to get started. Don’t let cyber criminals ruin the gaming experience for your players.

Contact us for a Watchtower demo today.
sales@panopticonlabs.com

USE CASE: Cheating in Online Video Games
Panopticon Laboratories is the first and only in-video game cybersecurity company, built to protect online video game publishers from the financial and reputational damages that can result from cyber attack.

Through proprietary technology that is uniquely focused on gameplay itself, Panopticon sets a baseline of activity for every player who participates in online play. Upon discovering anomalous behavior, Panopticon alerts publishers with more than 98 percent accuracy, along with providing recommendations for incident investigation and immediate remediation. Panopticon was founded in 2013 and is based in Columbus, Ohio.

Hackers, cheaters, and scammers won’t stop their cyber attacks unless you make them. Contact us for a Watchtower demo today.

sales@panopticonlabs.com

For more information about Panopticon, visit www.panopticonlabs.com and follow @PanopticonLabs on Twitter.