Hybrid play: Leveling the playing field in online video gaming and beyond

DUBAI, UNITED ARAB EMIRATES, January 25, 2023 /EINPresswire.com/ -- Rene Holt, security writer at ESET discusses whether VALORANT's approach to cheating signal a turning point in how we deal with the continued hacks afflicting our hybrid world of work and play

First social apps, now gaming? The growth of cloud-powered apps like Telegram and Teams has created mega communities out of their users. Many of these apps have opened the door to personal self-expression and the types of risk-taking notorious on social media platforms. Oversharing, connecting with strangers, clickbait, and phishing are now part and parcel of our work, and social and gaming lives; the lines are far too blurred in our hybrid lives for the risks to disappear.

But what about the free server space in the cloud, where millions of gamers, educators, and students are participating in a brave new world of digital possibility and risk? In Discord's now well-established platform, we find a kind of "natural selection" manipulated by moderators and bots, and an "evolution" happening in real time as communities adapt to new members' expectations for performance, fun, profitability, gameplay, fairness, and security.

What is Discord?
Born as a communication platform for the gamer community, Discord offers any community a cloud server with text and voice channels, along with screen sharing and file upload capabilities. Each community can set its own rules for and moderate how members interact with each other. Discord even offers developers a programming interface for creating bots and webhooks. Because of its rich collaboration features, threat actors have increasingly been abusing Discord for malware distribution, data exfiltration, and Command and Control (C&C) communication.

To highlight the changes taking place in the gaming space, let's look at what the members of one of Discord's largest gaming communities have been up to in their hybrid lives – sharing their

passion for VALORANT while fighting against the tide of cheating spreading across the gaming landscape.

VALORANT: Gaining popularity in a hybrid world

For some businesses, 2020 brought lockdowns that triggered a renewed look at the cloud as a transformation needed for business continuity. But for others, like Riot Games, who had already been using the cloud as the core enabler for their business model, plans rolled ahead with Riot Games releasing VALORANT, a free-to-play online multiplayer first-person shooter. Two years later, around 700,000 fans are playing this game daily, and a million have joined the official VALORANT Discord server – making it the most popular server since August 2022.

Does the rapid growth of VALORANT's popularity indicate uniquely attractive gameplay? If yes, how has VALORANT approached the perennial problem of cheating? Finally, how will this approach affect other parts of our hybrid, cloud-enabled world, and is there a link?

The gameplay attraction

VALORANT is attractive because it demands accountability. If a player dodges the queue, goes Away From Keyboard (AFK), or commits friendly fire, the game may impose a penalty of a timeout or a loss of points. Repeated offenses merit increasing penalties.

The game also demands fairness. Players can go up against each other in Competitive matches only if they are of similar rank and skill. Smurfing, where experienced players go on a killing spree of amateurs to boost their stats, is limited by requiring Account Level 20 to play competitively.

Finally, VALORANT promotes skill and teamwork. As novices, players hone their aim, the different Agents' special abilities, and their familiarity with the game maps. But as more experienced players, who each have a similarly high level of aim, teamwork and strategy become increasingly critical to winning matches.

Protecting the game with anti-cheat software

All of this effort to promote fair, competitive gameplay is safeguarded by requiring players to run the anti-cheat software Vanguard at the same time as VALORANT. Vanguard uses a kernel-mode driver to identify vulnerable drivers on the gamer's computer and either block them from running or prevent VALORANT from running. Since this driver runs when the computer boots up, it can detect attempts to load cheats prior to starting the game. Vanguard also has a user-mode client application that monitors gameplay for the use of cheats such as aimbots.

Cheating is also handled by the security features built into VALORANT. For example, the game uses a Fog of War system to prevent wallhacks, where cheaters see opponents through walls. The punishment for cheating could go as far as a hardware ban of the cheater's computer.

The discussions around this aggressive approach to the tech's implementation and how players feel about the implications to the independent function of their PCs have been active. Although

some may criticize anti-cheat software as spyware, putting the Vanguard client application under the microscope of a detection and response tool like ESET

Inspect reveals a different picture. The ESET Inspect console only flags Vanguard injecting a thread into the virtual address space of the VALORANT process, thus giving Vanguard a deep look into VALORANT. Considering the purpose of anti-cheat software, this is an entirely unsuspicious action.

Ultimately, the attractiveness of VALORANT lies in its focus on skill development, teamwork, and strategy to win matches – a focus that is secured by its strong approach against cheating and sabotage.

Rippling effects in a hybrid world

The shift from playing games offline to an age of online multiplayer games and esports has dragged in the curse of cheating. Cheats are the plague of the esports world, just as malware is of the internet. Indeed, the relationship runs deeper because the development of cheats requires the same tools and know-how used by vulnerability researchers and malware developers. Some even consider cheat development as the gateway drug to malware development.

This places anti-cheat software in a comparable role to security software and, indeed, in the same role of confronting some of the same exploitation techniques used by malware authors. Tackling the problem of cheats thus has strong parallels with tackling the problem of malware, requiring the identification and monitoring of the techniques used to gain an illicit advantage or control over another.

As we progress in a world transformed by the continued cloudification of traditionally offline activities, holding cheaters and hackers accountable will be critical to securing that progress. Only in this way can the excitement of the game, or whatever hybrid activity we participate in, keep its unalloyed appeal.

All these cloud-powered apps, platforms, and environments have created mega communities out of their users, with one of the largest being gamers. And where are the gamers? Well, probably on Discord servers for their favorite games. But just as the cyber-battle against hacks threatening our hybrid lives persists, so does the battle against cheating in games. It is a phenomenon looking at itself in the mirror.

Can the gaming community's response to cheating be instructive for our own hybrid world? Using anti-cheat software is one approach, but are there broader implications to in-game surveillance by algorithms that monitor behavior, relationships, and playing patterns? The same question is potentially applicable beyond gaming, regardless of the cloud-powered environment we might belong too.

By running through these popular cloud-powered apps, platforms, environments, and games, we hope to have shown how deeply we have become entrenched in our hybrid lives. Although fusion can improve our human and social experience, it is a reminder that well-defined limits can help ensure we continue to enjoy the benefits via a continued focus on privacy and security, just like we do in the physical world.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
