Mobile Gaming Attacks on the Rise

As mobile gaming continues to be increasingly connected, sophisticated attacks are proportionally increasing at an alarming rate that shows no signs of stopping. By employing techniques such as reverse engineering, attackers can tamper with the app to cheat and gain competitive advantages.

Players value fairness in games and expect everyone to compete on the same terms. Excessive cheating negatively impacts the honest gamers' experience and can destroy a game's success and reputation and cause players to abandon the game. A study shows that 77% of players are likely to stop playing a game if they think other players are cheating.

Controlling the growing risks from attackers and cheaters is required to fully protect a gaming company's business model. You need to take mitigating action against reputational risk, loss of intellectual property and revenue, and potentially damaging customer trust and brand reputation. Rampant cheating in one game can damage the game's reputation, but also indirectly influence the success of a publisher's future games.

Mobile gaming apps require In-App Protection to protect against app tampering and cheating and to maintain app integrity.

TAMPERING AND CHEATING

Attackers can take control of your app by cheating the studio or taking unfair advantage in multiplayer games. Cheaters are willing to pay large amounts of money for hacks that allow players to rack up major win statistics or steal in-game virtual winnings. As most players want fair competition, cheating can hurt a game's reputation, and result in a loss of players. A hacker's success can sink a game publisher's chances of striking a mega-hit or even force a gaming company to write off a total product failure.

Gaming publishers should also be aware of:

ACCOUNT TAKEOVER FRAUD

CREDENTIAL THEFT

UNAUTHORIZED ACCESS TO PAYMENT ACCOUNTS

PROMON

Turn your gaming apps into self-protecting apps

With Promon SHIELD™ you can quickly turn your gaming apps into self-protecting apps - helping to identify cheaters and without compromising the gaming experience. Our technology will help you protect your game and react in real-time to threats. Promon SHIELD™ will protect your gaming app against:

REVERSE ENGINEERING

To prevent attackers from reverse engineering your app to tamper with it and cheat in games, Promon SHIELD™ offers security mechanisms such as integrity checking, which prevents modification of an app, and code obfuscation. Obfuscating the app code will make it harder for an attacker to reverse engineer your app and can prevent hackers from gaining insight into your game's app logic and modifying the code.

THEFT OF SENSITIVE APP ASSETS

Game apps that provide in-game currency or wallets need solutions for securely protecting app assets stored locally on the device. Promon SHIELD™'s feature Secure Local Storage, will store app assets, such as personally identifiable information and API keys, locally on an end-user device in a secure and encrypted manner to prevent theft of currency and other sensitive app data.

REAL-TIME HACKING

Cheaters deploy various types of methods in order to gain access to the game's runtime logic and data. This allows the gamer to achieve an unfair advantage by enabling super powers such as making walls appear to be invisible. Promon SHIELD™ is able to both detect and block these styles of attacks that allow special powers such as these to be enabled.

APP CLONING

There's a lot of money in gaming, which makes gaming apps an appealing target for hackers. As a mobile gaming app provider, you need to take measures to prevent hackers from cloning your app and stealing revenue. Promon SHIELD™ offers the possibility to detect and react when an application has been repackaged.

! DID YOU KNOW?

Research of the highly popular game Among Us shows a lack of security measures - making the game trivial to cheat at. Cheats include killing players when you're not the imposter or accessing paid content without actually paying for it, just to name a few. While there are mechanisms that could prevent many of the possible cheats, they are simply not in place.

GET IN TOUCH!

For more information, please visit www.promon.co, or sign up for a free demo.