The Final Boss: Cybercrime in Gaming

From on-the-go mobile games, to VR and competitive e-sports, the gaming industry is booming. With progression comes a whole host of new challenges, and one that can't be ignored is cybercrime in gaming.

With the global gaming market forecast to be worth $250 billion by 2025, gaming companies and consumers are becoming a prime target for cyber-attacks. These attacks have soared recently (the pandemic acting as the perfect catalyst) with web application attacks against gaming companies rising by as much as 415% between 2018 and 2020.

A challenger appears

The past couple of years has seen a barrage of attacks on gamers and gaming companies alike, including (but not limited to) credential stuffing, distributed denial of service (DDoS) attacks, and cracked games containing crypto-mining malware.

In March 2020, Blizzard, the company behind popular games Overwatch and World of Warcraft, suffered four DDoS attacks in under a week. Similarly, the stadium-filling game League of Legends, one of the highest revenue-producing free-to-play games, was hit with a DDoS attack in January 2021, rendering players unable to use the game.

In 2021, some companies experienced having their games' source codes stolen. CD Projekt Red announced in February that the code for their successful games Cyberpunk 2077, The Witcher 3, and more had all been stolen. EA was another victim, with Fifa21's source code being advertised for sale online in June.

One of the most prolific kinds of cybercrime in gaming is data theft. With free-to-play games comes every kind of purchasable add-on; accounts decked out with the most skins, upgrades, and virtual currency can be sold online.

In June 2020, shortly after the release of the highly anticipated Animal Crossing: New Horizons, Nintendo announced that 300,000 accounts had been hacked. Large amounts of private customer information had been compromised and the attackers were able to use this to purchase in-game currencies.

Good game, hackers. Well played.

It's no surprise that gaming companies and consumers are being targeted by hackers. As a large portion of the userbase are casual users – mobile games are some of the highest grossing – and those not-so-cyber-savvy, attacks can be quick and effortless.

Poor password hygiene and using the same login credentials for different accounts is something that is so easily exploited, and yet still so commonplace. On internet forums and

social media platforms such as Reddit and Discord, you can find people selling stolen accounts and teaching others how to hack accounts for themselves. Young people seem to be particularly impressionable, often being roped into the scene without knowledge or understanding the consequences.

Time to rank up

As the gaming industry grows and cyberattacks become more profitable, the need for effective and easily implemented cybersecurity practices will continue to grow.

Games companies and platform providers need to take a proactive approach, by putting their customers first. The more customers experience being hacked, are denied access due to DDoS attacks, or simply just read about large-scale company data breaches, the more they will shy away from gaming. If the industry wants to progress and become a contender with traditional sports, essential changes must be made to reduce cybercrime in gaming.

Gaming is an entertainment activity. No one wants to be constantly fearing their private information being stolen whilst trying to unwind.

The casual user needs simple solutions for their cybersecurity concerns. There are security tools out there – multifactor authentication, password storage, etc. – but are they easy to use? Are they accessible for the masses?

How best can we, as an industry, encourage cyber safety for those who don't understand the jargon, struggle with apps, or simply don't know that they need to care? These are the questions that gaming companies need to be asking themselves, before it's too late.

For organisations in this sector, before being hacked by a malicious actor, having a friendly party test the security of their products could help to ensure the safety of their data – and protect their customers.

Read about our Penetration Testing service, and contact our experts to learn more about how Secarma can help.