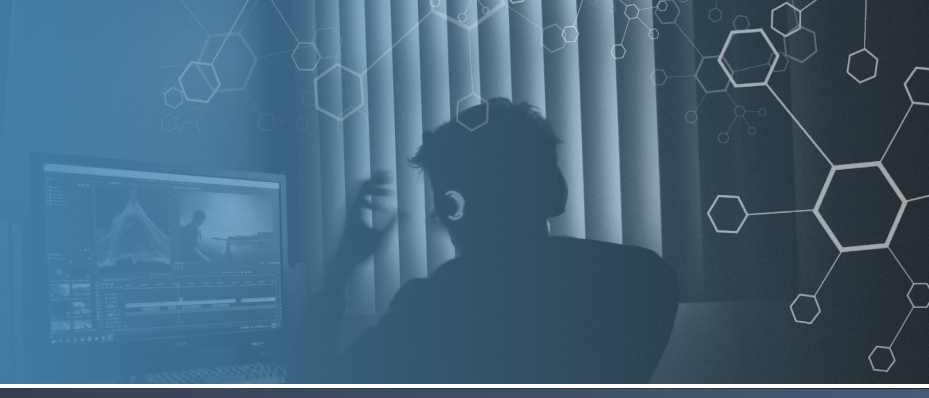
CYBERLINX
People | Process | Technology



GAMING AND THE THREATS GAMERS FACE

The online gaming industry has grown immensely in the last couple decades, with an estimated 2.7 billion players worldwide, officially making it the world's largest entertainment industry. It therefore comes as no surprise that the gaming community is increasingly under attack by malicious actors. There are many techniques attackers use to find victims to profit from in the gaming community, whether it be through phishing campaigns, malware distribution, data breaches or exploiting vulnerabilities in the gaming platforms themselves.

What do hackers stand to gain by targeting the gaming community?

1. Sensitive Data Theft

Primarily it is gamers' accounts that hold the most value to hackers, and thus is the most often targeted. Online games, regardless of the platform, gather a substantial amount of data on their consumers. The more personal or sensitive the data, the more valuable it is to hackers. The increased prevalence of in-game transactions and subscription-based payment methods for online games has resulted in financial information being included with a consumer's data.

2. Virtual Valuables

In-game economies are on the rise, exemplified by the prevalence of virtual currency and rare, prestigious in-game items being traded freely on various gaming platforms. This has created an environment in which malicious actors are continuously targeting user accounts to gain access to these valuable items as they can fetch large real-world prices. A moderator for RuneScape, one of the most established online games, recently took advantage of his elevated privileges to steal virtual currency with a real-world value of $100,000 from users.

Three common threats that gamers should be aware of

1. Phishing

Phishing is an attack that consists of a malicious message or email that masquerades the sender as a legitimate source or entity in order to trick the recipient into sharing sensitive information or data.

Phishing campaigns orchestrated by hackers target gamers in different forms. In most cases the target for hackers is simply to obtain access to account credentials. These accounts usually hold credit card information or have rare items attached to it that can be utilised for financial gain. In other cases, the target is a full account takeover which allows hackers to carry out their attacks from a trusted account for a higher success rate. Lastly, attackers utilise the lure of rare in-game items to trick gamers into buying fake products from a fake website masqueraded as a legitimate website. This allows hackers to obtain financial gain even without access to a gamer's account or credentials.

It is important to note that hackers aren't limited to traditional phishing techniques. A common way for attackers to get as much coverage as possible throughout the gaming platforms are with bot accounts. These bot accounts are set up to add and send automated messages to users. These messages often contain inappropriate adult content that redirects users to unwanted or malicious pages.

2. Malware

Malware is a collective term for harmful computer software that is designed to disrupt, damage, or gain unauthorised access to a computer or device.

Just like phishing, the goal for hackers remains the same - to gain access to sensitive data. It is just the technique in obtaining this data that is different. Attackers utilise malicious code or software to infect computers, devices, applications, and even games themselves. This allows hackers the opportunity to obtain account credentials and spread malicious content via malicious software, essentially making the software do the work for them.

An example of a well-known gaming platform that has been targeted for this type of usage is Discord, a voice and text chat application. In 2019 the Spidey Bot Malware was used to exploit Discord and gain access to personal information such as clipboard data, username, email address, IP address, phone number and discord user tokens. The Spidey Bot malware is a sophisticated attack since it injects its code into Discord and masquerades itself as part of the application which makes this malware hard to detect against the naked eye.

3. Data Breaches

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment or individual.

Data breaches are on the rise in all industries, and the gaming industry is no exception. Thus far we have spoken about hackers targeting gamers individually by means of phishing and malware, however we have not spoken about hackers targeting gaming companies themselves; this is where data breaches become relevant. By targeting gaming companies, hackers have the opportunity to gain access to a large amount of gamers' credentials all at once. This essentially makes gaming companies a gold mine for hackers seeking financial gain. Due to the majority of gamers using the same credentials across all gaming platforms, websites, applications, and communication forums, a credential leak can be extremely damaging for gamers and extremely profitable for attackers.

How to minimise risk against these threats

1. Phishing

To minimise the risk of a successful account credential phish, gamers can utilise the following advice: First, never click on links without knowing exactly where it goes, even if it's from a friend as their account may be compromised. Second, legitimate emails received from gaming companies or platforms will never ask you for login credentials or personal data – if you are unsure whether the email is legitimate or not, rather play it safe and call the gaming company's support desk to make sure. Third, websites or fellow gamers offering in-game items or products that are much cheaper than market prices, is most likely a phishing scam and should be avoided.

2. Malware

To minimise the risk of a successful malware attack, gamers can utilise the following advice: First, make sure you have a quality Anti-Virus program installed on your devices, preferably one that includes a "game mode" feature to limit false positives without impacting on gaming performance. Second, make sure to stay away from pirated games as they are almost always riddled with malware. Instead purchase games and in-game items from reputable gaming platforms like Steam, Origin, Uplay and GoG.

3. Data Breaches

To minimise the risk against successful data breaches, gamers can utilise the following advice: First, make sure to never re-use the same password on any gaming platform so that if a data breach occurs the damage is limited to one gaming platform. Second, make use of Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA). Most gaming platforms now support and encourage the use of Two-Factor Authentication or Multi-Factor Authentication. This should always be enabled as it adds an extra step to the login process, thus making it more secure. Third, be proactive in confirming whether you have been involved in a data breach. You can visit Haveibeenpwned.com and enter your email address to see if your credentials have been in a publicly known data breach.

Wrapping Up

With the gaming industry growing so rapidly, so will the threat landscape. Therefore, gamers must be aware, vigilant and understand the threats that they might encounter in order to alleviate the risks associated with the online gaming world.

Article - Dane Stoltz