Safeguarding digital playgrounds: cyber insights for gaming and eSports

BY ELEANOR BARLOW · OCTOBER 17, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **How to identify and understand the cyber risks unique to gaming and esports ecosystems**, and why these environments are desirable targets.
- **How common security weaknesses can be exploited in real-world gaming scenarios**, enabling you to recognise warning signs and potential impact better.
- **How to apply practical cybersecurity best practices** to improve protection for players, platforms, and organizations operating in the gaming and esports space.

According to Statista, revenue for the gaming and esports industry is expected to demonstrate an annual growth rate (CAGR 2025-2029) of 5.56%, resulting in a projected market volume of US$5.9bn by 2029. While this scale, visibility, and monetization have been fantastic for creators, developers, and providers, this same growth comes with amplified cybersecurity risk.

Throughout 2025, threat actors have been increasingly targeting gaming platforms, tournaments, and individual players. This blog aims to provide an overview of trends, attack vectors, and real-world incidents, and deliver practical guidance to gamers and organizations alike.

Surge in cyber threats: evidence and trends

Data shows a clear upward trajectory of cybercrime across all industries, with cybercrime predicted to jump from $10.5 trillion in 2025 to $15.63 trillion by 2029 (207 Cybersecurity stats for 2025).

But while cybercrime has increased across the board, gaming and esports environments in particular have become a battleground for threat actors. If we take a look at popular games such as Minecraft, Call of Duty, or GTA, a recent report from Kaspersky shows that between Q2 2024 and Q1 2025, there were 19,038,175 attempted attacks via malware and chat installers. During that same timeframe, 408,550 individual gamers were targeted. The report continues to state that downloaders made up 93% of those attempts, followed by adware and trojans.

In addition, SQ Magazine shows that 'gaming platforms experienced a 39% year-on-year rise in credential stuffing attacks in 2025, targeting players for monetizable credentials and in-game assets'.

The incentive: why do threat actors invest in targeting gaming assets?

It's probably no surprise that the chief benefit of a successful attack within the gaming industry is down to financial gain. Compromised accounts often contain payment methods or in-game currency that can fetch

hundreds or thousands of pounds/dollars in other markets. Not only are direct financial payments made, but items, skins, and in-game currencies all have direct monetizable value. If money cannot be directly accessed, threat actors can resell compromised assets or access premium services.

When threat actors can't access money directly, sensitive data and intellectual property become the next big payoff. An organization's internal game development files, roadmap docs, early builds, and user data are all valuable for resale, corporate espionage, or ransomware leverage. What's more, many forms of attack can be automated at scale, making each successful attack multiplicative.

Tournaments, streaming overlays, and betting or transaction platforms create opportunities not only for financial gain but also for real time disruption and data exposure, risks that can cause serious reputational damage when major events, launches, or competitions are affected.

Regardless of their objective, the balance between effort and reward offers skilled threat actors a significantly high return on investment in this industry.

But it's not just what's available to a hacker that makes targeting gaming and eSports an enticing option; it's the consistency of vulnerabilities coming from both customers and companies that make it a relatively low-lift, high-reward option.

Weakness 1: Cheat sheets, overlays, and patches

Players will often seek unofficial patches, modifications from forums or file-sharing sites, and gaming cheat sheets. Not only are these an easy vector to disguise malware or trojans as useful tools and gaming directions, but gamers will often reuse their data across platforms, which means any emails, passwords, or data entered in one game will likely be applicable in others, and then the breach can cascade from one platform to another.

Example: Dropper malware via Arcane InfoStealer

Arcane InfoStealer (not related to the dark web trojan Arcane Stealer V) is a type of malware that, in March 2025, targeted a series of YouTube and Discord channels via the distribution of game cheat sheets advertised as game modifications or enhancements.

Threat actors embedded malicious scripts within these cracked or modified archives. Once installed, the malware would operate silently, while payloads, keyloggers, and credential stealers harvested sensitive data, including usernames, passwords, and credit card details.

Over time, the campaign evolved from promoting basic cheat sheets to advertising ArcanaLoader as a handy tool to install cheats and other useful gaming tools. Instead, ArcanaLoader further infected devices with the Arcane stealer malware.

Kaspersky estimates that 26 million devices running Windows were compromised by infostealers throughout 2023 to 2024 alone.

Weakness 2: Large user bases

With millions playing mainstream games simultaneously, compromising even a tiny fraction can expose thousands of users' data. Another way that the sheer size of the user base can be manipulated is by damaging reputation in one move. An example of an attack that relied on the activity of thousands of users to do just this can be seen in the April 2025 attack against a popular gaming site known as Blizzard.

Blizzard Battle.net DDoS attack

Blizzard confirmed in early April that Battle.net was the target of a DDoS attack, which caused issues with latency, disconnection, and faulty logins. The goal of a DDoS attack is to overwhelm the target's environment with a flood of illegitimate traffic from compromised devices, making it hard and sometimes impossible for legitimate users to access the platform. While the company reported that they were actively working to mitigate the threat, players continued to struggle to access the site.

The purpose of this form of attack is the disruption of a significantly large user base, which could have an impact on both reputation and brand value.

Weakness 3: Lack of focus on security maturity

Smaller eSports organizations often lack robust cybersecurity, including layered defenses, proactive safeguards, and incident response plans, to counter modern threats. Compared to industries like finance, which employ complex security frameworks, this makes it far easier for threat actors to infiltrate systems, steal data, and demand ransoms.

'Ransomware extortion attacks similarly leverage the esports sector's high uptime requirements and the reputational, regulatory, and financial risks of such attacks. Combined ransomware and data leak extortion attacks enable criminals to put additional pressure on victims by threatening to leak or sell information stolen from video game production environments at all stages of the development process – design, artistic, programming, and testing – on the deep and dark web.' - ControlRisks

An example of such a ransomware attack can be seen in the WEMIX breach that occurred earlier in 2025.

HellCat credential stuffing attack against WEMIX gaming company

In a breach targeting the South Korean blockchain gaming company, WEMIX, a total of 8.64 million tokens, equivalent to $6 million, were stolen.

In a press conference, CEO Kim Seok-Hwan confirmed the attack, stating that...

"As soon as we identified the hack on February 28, we immediately shut down the affected server and began a detailed analysis. On the same day, we filed a criminal complaint with the Seoul Metropolitan Police Agency's Cyber Investigation Unit, and the National Office of Investigation is currently conducting an investigation. Since the exact infiltration method was not initially identified, an immediate public disclosure could have exposed us to further attacks. Additionally, most of the stolen assets had already been sold, impacting the market. Given the difficulty in guaranteeing that there were no further risks, an immediate disclosure could have caused market panic." – Full press release here.

The cause was down to the HellCat ransomware group, which emerged during mid to late 2024 and combined high-ranking members of breach forums. According to SentinelOne, 'these personas, including Rey, Pryx, Grep, and IntelBroker, have been affiliated with the breaches of numerous high-value targets.'

Weakness 4: weak supply chain

The supply chain of the gaming industry is multifaceted. Gaming and eSports environments are complex ecosystems that contain many interconnected components. Everything from hardware manufacturing to software development, launch support, marketing, and distribution, cloud services, physical components, code libraries, and outsourced vendors: all are potential avenues for exploitation.

Data from Cyble confirms that supply chain attacks have doubled in 2025. The report states that 'The uptick in supply chain attacks began in April 2025, when Cyble dark web researchers observed claims of 31 such attacks. Since then, cyberattacks with supply chain implications have averaged 26 a month, twice the rate seen from early 2024 through March 2025.'

If we return to the HellCat example explored earlier, we can see just how the group targeted vulnerabilities in platforms such as project management tool Jira, as well as other DevOps tools used across industries, to escalate privileges until they reached the crown jewels of the company.

Weakness 5: Misconfigurations and insider threats

An employee might commit malicious behavior, such as fraud, by using their insider knowledge to fix a match or an eSports betting system. They might work with external threat actors and provide them with information regarding access to data, networks, or systems. Employees with privileged access might sell player accounts or in-game currency on the black market. A discontented employee might even provide documents, code, or data to competitors or purposefully introduce security vulnerabilities.

Quick tips to gamers

For players, it is recommended to:

- Use different strong passwords on every platform. Never reuse passwords on gaming platforms and monitor account activity for any unusual or unexpected logins or activity.
- Ensure multifactor authentication is enabled and keep systems and devices updated.
- Don't use cheat sheets/codes from untrusted sources. Only download from trusted sources and official stores.
- Isolate configurations and limit plugins and overlays.

Recommendations to organizations

To enhance security posture and adopt a flexible security program:

- Use PTaaS to test your environment within a specific scope. For instance, PTaaS can be used in preparation for securing systems before any new code release, product update, or new game release date.
- Use a bug bounty program to harness the external researcher community's expertise and insights. Simulate world threats on everything from authentication systems to tournament platforms to help identify your weaknesses. Uncover critical vulnerabilities within servers, marketplaces, and platforms, while building trust with the gaming community.
- Use a VDP for transparency and clear guidelines for responsible disclosure. Encourage coordinated disclosure and provide a structured and safe way for researchers to report vulnerabilities.

With these measures in place, gaming companies can shift from a reactive security posture to a defense-in-depth strategy, reducing the likelihood and impact of attacks.

To better understand how BB, VDP, and PTaaS can be layered and used in conjunction with one another to enhance your security maturity, read '**Layered security in action: How VDP, Bug Bounty, and PTaaS combine to protect your business'**.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.