WHITEPAPER

Cyber security best practices for online gaming and igaming companies

Overview

Online gaming and igaming (i.e. online betting) companies have boomed in recent years. The COVID-19 pandemic saw a surge of online activity from players across the globe, while notable advances in mobile gaming and igaming services have driven user demand.

By one estimate, over three billion players spent approximately $182.98 billion on gaming in 2022, with an anticipated growth to $206.4 billion by 2025.

This growing value has also attracted the attention of cyber criminals and malicious players. Attacks against companies in these sectors can have a variety of potential effects, ranging from a degraded gameplay experience to financial losses for companies and their customers.

Top cyber security threats for online gaming and igaming

For online gaming and igaming companies, lightning-fast performance and uptime are critical. Even milliseconds of lag can frustrate players, while more significant disruptions may lead to a mass exodus of users. Additionally, these sectors hold a great deal of valuable data, ranging from players' financial information to details of the next release in a major franchise.

Cyber criminals and cheaters can capitalize on these factors for their own benefit. Here are some of the top methods they use:

DDoS attacks

Distributed denial-of-service (DDoS) attacks, which flood websites or services with malicious traffic, can be leveraged in various ways. The gaming and igaming industry is one of the most targeted industries for both network-level and application-level DDoS attacks.

One threat to gaming companies is a ransom DDoS (RDDoS) attack, where attackers carry out DDoS attacks (or threaten to launch attacks) against gaming servers unless they receive a payment, or ransom. By rendering the game inaccessible, an attacker could cause gamers to leave a game due to non-availability — costing the company more than the ransom payment.

Another application of DDoS attacks — especially in the esports industry — is to use the attack to influence the outcome of a match for profit. An attacker who bet on the underdog of an esports match might perform a DDoS attack against their opponent, rendering them unable to play. If this team is forced to forfeit, the attacker may receive a significant payout.

One example of this occurred in 2015 in a League of Legends match between Dignitas and Denial. Denial was targeted by a DDoS attack that forced the team to forfeit the match since one of their team members was unable to play for more than 10 minutes. Betting was 12:1 in favor of Denial, providing the attacker with the ability to make a tidy profit by betting on Dignitas.

Web application and API attacks

The web applications and APIs which support online gaming and igaming platforms can contain vulnerabilities attackers can exploit. Some of the most common goals of these attacks include:

- **Data theft:** Attacks against a gaming platform's web applications and APIs can yield a wealth of valuable data. For example, exploitation of cross-site scripting (XSS) vulnerabilities may allow an attacker to harvest the personally identifiable information (PII) of other gamers. This data may be used in account takeover attacks, result in financial fraud, or be sold on the dark web.
- **Cheat development:** The high stakes of online gaming and esports have made it common for some gamers to seek out cheats to gain an edge over their opponents. In fact, 47% of gamers admit to cheating sometimes, and 60% have been negatively affected by cheating. XSS vulnerabilities and other security flaws in a gaming platform may allow an attacker to embed scripts or steal sensitive data that grants them an advantage when gaming.
- **Denial of service (DoS):** Web application or API vulnerabilities can also be used for DoS attacks, which may target the resources or gameplay of a single player. For example, an attacker may launch a DoS attack to cause their opponent to be kicked out of the game at a critical moment, allowing them to gain a significant competitive advantage or even win outright.

Malicious bots

Automated, malicious bots pose a significant risk to gaming and igaming platforms' security and user experience. In 2022, over half of traffic to online gaming and igaming websites came from malicious bots. Attackers can use bots to gain unfair advantages and threaten users' account and data security in various ways:

- **Spamming:** In-game messaging systems can be used to blast out links to a wide range of undesirable or malicious sites.
- **In-game farming:** Games often require users to perform simple, repetitive tasks to build up currency or other resources. By automating these tasks using a bot, a player can rapidly build up resources while they're not playing, enabling them to cheat.
- **Fake account registrations:** Bots can be used to create duplicate accounts, enabling players to evade blocks imposed in response to spam or other inappropriate or malicious in-game behavior.
- **Data scraping:** Scraping bots can collect data from gaming and igaming websites, such as the posted odds for various matches. Not only does scraping allow players to potentially exploit the odds for their benefit, but it also places an additional load on a company's systems.
- **Account takeover:** Bots can be used to carry out credential stuffing or similar attacks used to gain control over legitimate users' accounts, and access or steal currency, in-game resources, or other valuable items and rewards.

Data breaches

Data breaches can be particularly damaging for gaming and igaming companies, which hold a great deal of sensitive information in the form of intellectual property and customer data.

Attackers can carry out data breaches against gaming companies in various different ways. Phishing and social engineering attacks can provide access to the organization's internal infrastructure. In addition, the exploitation of web application and API vulnerabilities — such as SQL injection or cross-site scripting — can enable an attacker to extract sensitive data from servers.

One of the most famous examples of the effects of a data breach in the gaming industry is the hack of Rockstar Games in 2022. The attacker allegedly gained access to the source code of Grand Theft Auto (GTA) V and VI, as well as 90 clips of footage from prerelease test builds of GTA VI, which they released online.

Account takeover attacks

Account takeover attacks are another common threat since gaming and igaming accounts can be extremely valuable — and contain a wealth of personal data like payment card information.

Cyber criminals perform account takeover attacks in various ways. Successful exploits of company servers and applications can leak users' personally identifiable information (PII) for use in these attacks. Attackers will also use phishing and social engineering attacks to trick users into handing over their sensitive data.

A successful account takeover attack can have significant financial repercussions. In June 2022, the hack of a Counter Strike: Global Offensive player's Steam account allowed the attacker to steal the player's full collection of skins and cosmetic inventory. The value of the stolen goods was estimated at $2 million, since the player owned some of the rarest items available.

Managing online gaming and igaming security threats

To manage the risks associated with all of these attacks, companies should consider the following cyber security best practices:

Enterprise-scale DDoS mitigation

To ensure that their services remain online and operational, a gaming company requires high-performance, robust DDoS mitigation capabilities. To manage the threat to online gaming and igaming companies — which require high-performance, reliable connectivity, a DDoS prevention solution must offer:

- **Multi-layer scrubbing:** DDoS attacks can occur at multiple layers of the OSI model. In addition to the ability to Layer 2/3 DDoS attacks, DDoS scrubbers must be able to detect and remediate the more sophisticated Layer 7 application-level attacks that are common in the online gaming space.

- **Always-on protection:** DDoS attacks can happen at any time. Minimizing lag and downtime requires always-on protection that can begin scrubbing attack traffic with no delay.

- **Scalability:** The growth of DDoS botnets and the availability of booter and stresser tools means that an online gaming or igaming company can face record-breaking DDoS attacks. DDoS mitigation solutions must be capable of scaling to address large and growing attacks.

- **Locality:** Backhauling traffic to a DDoS scrubbing center increases latency and lag for gamers. DDoS scrubbing functionality should be located near an organization's servers to minimize the impact on performance.

Bot management

Malicious bots' significant impact on the gameplay experience makes anti-bot protection essential for gaming companies. However, correctly identifying malicious bots can be complex. Effective bot detection without blocking legitimate players require a multi-pronged strategy:

- **Allowlisting:** Some automated bots — such as Google's and Bing's bots — are known to be benign. These and other known-good bots should be automatically allowed.

- **Heuristic-based detection:** Bots attempt to mimic human behavior, but small variations commonly exist between them and normal user traffic. A bot management solution should include a range of heuristics designed to identify automated traffic based on hard-to-fake attributes.

- **Anomaly detection:** Within a particular gaming or igaming site, legitimate user traffic is likely quite similar. Any deviations from the norm are more likely to be automated bots or other attack traffic.
- **Machine-learning:** Heuristics can identify automated traffic based on known deviations from human traffic. Machine learning — trained on large datasets — has the potential to extract new differentiators and use them to detect more subtle automated traffic.
- **Javascript challenges:** Client-side JavaScript enables a bot detection engine to collect a greater range of data from a browser. This increases the difficulty for automated bots to masquerade as human users.

Web app and API security

Exploitation of web apps and APIs on gaming platforms poses a significant risk to users' gaming experience and security. A successful attack could have a range of potential effects, ranging from a degraded gameplay experience — if a cheating opponent has an unfair advantage in gameplay — to the exposure of sensitive personal information leaked from the gaming platform via a vulnerability.

These attacks often exploit vulnerabilities that have reached production systems. Some best practices for managing the cheating risk include:

- **Attack surface detection:** Unmanaged apps or APIs are common targets of attack. An important first step to defending a platform is identifying the full scope of its publicly-accessible web services.
- **Web application firewall (WAF):** Most attacks targeting online gaming and igaming companies exploit common vulnerabilities such as SQL injection, cross-site scripting, and local file inclusion. A WAF deployed in front of a gaming platform can detect and block attempts to exploit these vulnerabilities.
- **Security testing and bug bounties:** Regular security testing can help to identify vulnerabilities before they can be exploited by an attacker. Also, implementing a bug bounty program may motivate players and security testers to report vulnerabilities that they discover in return for a reward.
- **DevSecOps:** The most effective method of managing security threats to corporate web applications and APIs is to be proactive. Integrating DevSecOps practices into development lifecycles can help to identify and block vulnerabilities from reaching production.

Account security

The account of a successful gamer commonly has real-world value and may lack the same defenses as a similarly-priced account in the financial or healthcare sectors. As a result, there is consistently a thriving market in compromised gaming accounts.

Account takeover attacks in the gaming sector use various tactics to gain access to user credentials. Some best practices to improve the security of gamers accounts include:

- **Bot management:** Malicious bots are commonly used in credential stuffing attacks designed to identify accounts with weak and reused passwords. Anti-bot protections can prevent these automated, malicious requests from reaching login pages and carrying out their attacks.
- **Behavioral analytics:** Attempted account takeover attacks likely originate from different locations and devices and at different times than a user's normal gameplay. Account monitoring and behavioral analytics can help to identify likely attack traffic.
- **Web application and API security:** Web app and API exploits can leak sensitive information used in account takeover attacks. Web app and API security solutions that block these exploits can deny an attacker the information needed to carry out their attacks.
- **Multi-factor authentication (MFA):** MFA requires an attacker to gain access to multiple authentication factors before they are granted access to a user's account. Implementing MFA for user accounts can reduce the risk of account takeover attacks. Organizations can manage the impact of MFA on the user experience by implementing step-up authentication, which only requires additional authentication if a request is deemed risky or potentially malicious.

Secure access to critical corporate applications

Gaming companies are common targets of cyber attacks, especially those focused on data theft. In addition to troves of customer data, gaming companies also have extremely valuable intellectual property. The leak of a pre-release game can have a substantial impact not only on sales but on the value of the company's stock.

One of the most effective methods for reducing the risk of these attacks is to implement a Zero Trust security architecture. Zero Trust manages access to corporate networks, resources, and data by evaluating access requests on a case-by-case basis.

With Zero Trust network access (ZTNA), an organization can implement and enforce least-privilege access controls, reducing the risk of unauthorized access to sensitive company and customer data. Additionally, ZTNA can incorporate MFA to require stronger user authentication if an access request is deemed risky or anomalous.

Online gaming and igaming security with Cloudflare

Cloudflare offers solutions to address the main cyber security risks gaming and igaming companies face, including:

- **DDoS Protection:** Cloudflare has blocked some of the largest DDoS attacks in history, ensuring that malicious traffic doesn't reach a company's sites and impact their users' gaming experience.
- **Bot Management:** Cloudflare assigns bot scores to each request, enabling companies to block automated traffic or apply CAPTCHAs based on a predefined threshold.
- **API Security:** Cloudflare helps detect shadow APIs and protect legitimate APIs via client certificate-based identity verification and strict schema-based validation.
- **Web Application Firewall (WAF):** Cloudflare protects web applications and APIs against both common and emerging application-layer attacks, such as SQL injection and XSS.
- **Advanced Rate Limiting:** Advanced rate-limiting technology prevents credential stuffing, DDoS attacks, and abuse of APIs and applications that could cause crashes or unpredictable costs.
- **Zero Trust:** Cloudflare Zero Trust reduces the risk of data breaches and other damaging attacks by enforcing least privilege security controls within an organization's infrastructure.

References

1. newzoo.com/resources/blog/the-latest-games-market-size-estimates-and-forecasts
2. blog.cloudflare.com/ddos-threat-report-2023-q1/
3. securityhq.com/blog/cyber-security-threats-in-gaming-industry-at-an-all-time-high/
4. resources.irdeto.com/irdeto-global-gaming-survey/irdeto-global-gaming-survey-report-2
5. imperva.com/blog/five-ways-the-gaming-gambling-industry-is-targeted-by-bad-bots/
6. securityboulevard.com/2022/09/what-we-know-about-the-grand-theft-auto-vi-data-breach/
7. eurogamer.net/hackers-steal-2m-worth-of-csgo-skins-from-collector

1 888 99 FLARE | gaming@cloudflare.com | Cloudflare.com