digicert®

Game Over:

Why the Gaming Industry Is a Prime Target for DDoS Attacks

WHITE PAPER

Game Over:
Why the Gaming Industry Is a Prime Target for DDoS Attacks

You're in the final, critical moments of a competitive, high-stakes match. Your team is perfectly coordinated, the objective is within reach, and your hard-fought victory seems all but guaranteed. Then, without warning, your character freezes. The world around you stops responding, and a "Connection Lost" error message flashes across your screen. In that instant, you've not only lost the match, you've also lost your competitive rank, your patience, and your trust in the game's stability.

It's a familiar and deeply frustrating experience for millions of gamers around the world. But for game developers and publishers, it represents a catastrophic business failure with far-reaching consequences. The online gaming industry has become a veritable playground for Distributed Denial of Service (DDoS) attacks. Recent attacks in late 2025 and early 2026, which resulted in major service disruptions to large gaming platforms underscore a volatile reality—if you build a successful online service, attackers will inevitably try to take it offline.

DDoS attacks are not merely nuisance events in the gaming world. They're sophisticated, high-volume assaults, meticulously designed to cripple server infrastructure, extort money from operators, and manipulate competitive outcomes.

To understand why games are such an attractive target, it is necessary to examine the history of these attacks, the mechanics of modern botnets like the notorious Aisuru and Kimwolf, and the immense pressure placed on server operators to maintain constant uptime and a seamless player experience.

The Evolution of Disruption: DDoS and Gaming History

The relationship between online gaming and denial-of-service attacks is almost as old as the internet itself. As soon as multiplayer games transitioned from the controlled environments of local area networks (LANs) to the public World Wide Web, malicious interference and competitive manipulation emerged.

In the early 2000s, these attacks were often crude and isolated incidents. They were typically the work of lone individuals seeking personal notoriety within small communities or pursuing petty revenge against a specific server administrator. But as global broadband speeds increased and the underground black market for cybercrime matured, the complexity and scale of these attacks grew exponentially. What began as minor disruptions by individual hobbyists evolved into large-scale, coordinated assaults capable of overwhelming sophisticated network infrastructures.

The Era of Early Booters

The democratization of DDoS attacks took off with the emergence of "booters" or "stressers." These are web-based services that, while often marketed as legitimate tools for network and server stress-testing, have a darker side: they allow individuals to carry out DDoS attacks for a small fee. They require minimal technical knowledge and don't require users to contribute resources to the stresser service. By simplifying the process, these services made cyberattacks accessible to anyone with a motive and a willingness to pay.

In the early days of console gaming and peer-to-peer (P2P) PC gaming, booters became a significant problem. At that time, many multiplayer gaming architectures relied on direct connections between players rather than centralized servers. This setup inadvertently exposed players' IP addresses to others in the lobby, making them vulnerable. Malicious users could easily employ packet sniffers to uncover an opponent's IP address and then use a booter service to overwhelm that specific connection with traffic. For just a few dollars, they could disrupt an opponent's ability to play, often at critical moments.

This practice, commonly referred to as "booting," became especially rampant in competitive gaming environments, such as online shooters and strategy games. It allowed less skilled players to gain an unfair advantage by forcing opponents to disconnect. By knocking others offline, these players could climb ranking ladders and achieve higher standings without actually improving their gameplay. Titles with a strong competitive edge, where rankings meant status or rewards, were particularly plagued by this tactic.

Although online games have since moved away from P2P networking in favor of centralized servers to mitigate these vulnerabilities, the legacy of booters remains deeply ingrained in gaming culture. The use of DDoS attacks as a tool for gaining a competitive edge hasn't completely disappeared. Instead, it continues to surface as a lingering issue, reflecting a troubling aspect of the gaming community where some players prioritize winning at any cost, even through unethical means.

Why Are Games Targeted?

The gaming industry is a primary target, attracting a higher volume of DDoS attacks than most other sectors. The motivations behind these attacks are varied, ranging from large-scale financial extortion attempts against game publishers to smaller, personal vendettas between players. However, all these attacks exploit one critical vulnerability: online gaming is a highly latency-sensitive service. Unlike a banking website, which can still function adequately despite a two-second delay in loading a page, a competitive online game becomes entirely unplayable with even a few hundred milliseconds of added latency. This sensitivity makes gaming an ideal target for disruption.

Knocking Other Users Offline

At the micro-level, these attacks are often personal and malicious. In high-stakes competitive matches, where ranking points or tournament qualifiers hang in the balance, there's an outsized incentive to gain an unfair advantage by any means necessary. This pressure can motivate some players to cheat.

Attackers often target individual players with the goal of forcing a disconnect from the game server. In team-based games, successfully removing even a single opponent creates an immediate numerical advantage, such as a 5v4 or 4v3 scenario. This imbalance can be enough to all but guarantee a win for the attacker's team. This tactic is not limited to casual public matchmaking; even professional esports tournaments, which can feature prize pools exceeding millions of dollars, face constant threats from such disruptive activities.

To execute these attacks, bad actors rely on obtaining the victim's IP address through leaks. Although game developers make efforts to mask player data and protect their privacy, vulnerabilities can still exist. These are often found in integrated voice chat protocols (VoIP) or third-party communication tools like Discord or TeamSpeak, which may inadvertently expose a user's IP address. Once the IP is known, the attacker can flood the victim's home network with malicious traffic, creating a bottleneck that renders the game completely unplayable due to extreme lag or a total loss of connection.

Financial Extortion and Ransom

At a broader level, cybercriminal groups execute attacks targeting the game publishers themselves. Their strategy is straightforward: they recognize that any period of downtime directly translates into financial losses for the company. When a highly popular game is forced offline, the publisher immediately begins losing revenue from various streams, including in-game microtransactions, subscription renewals, and potential new game sales that are lost during the outage.

These criminals leverage this significant financial vulnerability by threatening to take game servers offline during periods of high player traffic. These critical windows can include a holiday weekend, the launch of a new game season, or major esports final, all times when server stability is paramount. In exchange for not launching the attack, they demand a substantial ransom payment. Because the reputational damage resulting from a high-profile, launch-day failure can be severe and potentially irreversible, some companies feel immense pressure to comply with the demands, paying the ransom and fueling the ongoing cycle of digital extortion.

More, the rapid growth of the esports betting industry, now valued around $3.5B billion, introduces an additional layer of financial motivation for these attacks. In this context, attackers might disrupt a live match to directly influence its outcome, either to protect a large bet they've placed or to manipulate the betting odds in real-time for financial gain.

Chaos and “Random” DDoS

Not all cyberattacks are financially motivated. Some are driven by a desire to create chaos, gain notoriety, or advance a cause through “hacktivism.” In many cases, groups or individuals compete for dominance, aiming to take down the largest, highest profile targets as a way of showcasing the power and scale of their botnets. This competition isn't just about disruption. It's about proving their capabilities to the broader cybercriminal community.

Prime examples of this are the Aisuru and Kimwolf botnets, which gained significant attention in late 2025. Security researchers closely monitored their activity, noting their ability to generate unprecedented levels of traffic—peaking at an astonishing 30 terabits per second (Tbps). Attacks of this scale are not subtle by any means. They are engineered to overwhelm infrastructure, causing widespread disruptions while simultaneously making headlines. The sheer magnitude is a deliberate choice, designed to demonstrate the botnet's capacity to cripple even the most robust networks.

In October 2025, this destructive power became evident when massive disruptions hit several game services all at once. These attacks were not random acts of chaos but strategic demonstrations. For botnet operators, these high-profile takedowns act as a form of marketing, showcasing their infrastructure's ability to incapacitate some of the world's largest technology companies. This serves as a powerful sales pitch, proving to prospective buyers in the cybercriminal market that their tools can deliver devastating results.

Vulnerable Targets in Gaming Infrastructure

Protecting a game server is far more complex than safeguarding a standard web server. Unlike web traffic, which typically relies on the Transmission Control Protocol (TCP) for reliability and connection management, game traffic primarily uses the User Datagram Protocol (UDP) for speed and low latency. However, UDP is inherently connectionless and lacks the built-in verification mechanisms of TCP, making it much harder to secure against attacks. This vulnerability creates multiple entry points that attackers can exploit to disrupt gameplay. Defensive strategies must address these vulnerabilities at every level, from lobby protections to match session stability and infrastructure-level safeguards. Without robust countermeasures, attackers can exploit these weak points to severely harm the player experience and the game's long-term success

Individual Users

As we mentioned previously, one of the more insidious tactics employed by attackers involves targeting individual users by identifying their source IP addresses and attacking them directly with a DDoS. When an attack is directed at a player's IP address, it can severely disrupt their internet connection, leading to latency, disconnections, or complete inability to access the service. This not only frustrates the targeted user but can also erode trust in the game's ability to provide a secure and stable environment.

The process typically begins when an attacker gains access to a player's IP address, often through packet sniffing, exploiting vulnerabilities in communication channels, or other illicit means. Once the IP address is obtained, the attacker launches a DDoS attack, overwhelming the target's network with traffic and effectively rendering it inoperable. This type of attack has highly personalized consequences, as it singles out individual players for harassment, potentially driving them away from the game entirely.

The Game Lobby

The game lobby serves as the waiting room where players gather, form teams, and prepare before a match begins. This makes it a critical choke point for the entire game experience. If attackers manage to flood the lobby server with malicious traffic, players cannot connect, form matches, or even access the game, effectively rendering it unplayable.

Protecting the lobby is particularly challenging due to the complexities of login and authentication systems, which are often encrypted for security. This encryption makes it difficult to distinguish between a surge of legitimate players logging in during a new event or game update and a flood of malicious bots attempting to crash the login server. Sophisticated traffic analysis and filtering are required to differentiate between these scenarios. However, overly aggressive filters risk blocking genuine players (resulting in false positives), frustrating the player base. On the other hand, lenient filters may allow malicious traffic to overwhelm the server, leading to a complete lobby shutdown.

The Game Session

Once the game moves past the lobby and into the match itself, the attack vector shifts to the actual game session. Here, attackers often target the specific ports on the game server responsible for processing real-time player actions, such as movement, shooting, or communication.

By flooding these ports with garbage data, attackers force the server to waste valuable resources sorting legitimate player inputs from the noise. This creates a noticeable impact on gameplay, including "rubber-banding" effects, where players are abruptly snapped back to previous positions due to server lag, and eventual player disconnections. These issues can degrade the overall player experience, causing frustration and potentially driving users away from the game. The server, in this scenario, is essentially fighting a losing battle to keep up with both legitimate and malicious traffic under significant resource strain.

Server Network Saturation

The most brute-force method attackers use is a volumetric attack, designed to overwhelm the hardware and network capacity of the data center hosting the game servers. Every server and datacenter has a bandwidth limit—essentially the size of the internet "pipe" connecting it to the wider network. For example, if a server's connection can handle 10 gigabits of data per second and an attacker sends 100 gigabits of traffic, the connection becomes completely clogged. This kind of saturation leaves no room for legitimate traffic to pass through.

In these cases, software defenses, network firewalls, and protocol optimization are powerless against the sheer volume of data. The only solution is to divert the traffic to a scrubbing center to drop the excess traffic.

Download and Update Sites

The release of new games, mods, or downloadable content (DLC) is a vulnerable time for a game publisher. These launches spark a surge in player activity, creating a much higher demand for software downloads. This is an opportunity for cyber attackers to exploit by targeting primary download and update servers.

By taking advantage of the increased traffic from legitimate users, attackers can execute Distributed Denial of Service (DDoS) attacks. These attacks overwhelm servers with excessive traffic, causing widespread disruptions. Players are unable to access the content they were eagerly anticipating, leading to frustration across the community. For publishers and developers, such disruptions can ruin their critical game launch and damage their reputation.

The Evolution of DDoS Defense for Games

Initially, the gaming industry lacked robust measures to counteract DDoS attacks, because these threats were often considered low priority or infrequent. Early strategies relied heavily on basic firewalls and on-premises solutions, which were insufficient against the growing scale and sophistication of attacks. But as online gaming gained widespread popularity and became a lucrative industry, the stakes increased considerably.

The rise of persistent online worlds, competitive gaming, and live-streamed events amplified the impact of service disruptions, demanding more sophisticated defenses. Concurrently, attackers adapted with more advanced tactics, leveraging botnets and exploiting vulnerabilities in real-time services. This evolving threat landscape pushed the industry to adopt proactive and comprehensive DDoS defense mechanisms, combining cloud-based solutions, AI-driven detection, and continuous monitoring. Gradually, combating DDoS has become a central concern for game developers and publishers, integrating resilience into both infrastructure design and operational planning.

The escalating scale of attacks, like the unprecedented size of attacks from the Aisuru and Kimwolf botnets, highlights the need for a robust and scalable solution to mitigate the risks associated with modern DDoS campaigns. Game publishers and platform operators face a critical challenge as they strive to safeguard their online platforms while managing the financial burden of cybersecurity measures. Advanced strategies, including globally distributed traffic management, are becoming essential for ensuring uninterrupted service.

By employing sophisticated tools designed to identify and neutralize malicious traffic in real time, organizations can protect their infrastructure without diverting critical resources away from core priorities like game development and user engagement. This approach not only enhances security but also preserves the seamless user experience that players and communities expect.

Keeping Up the Fight

The war between game publishers and cybercriminals is unlikely to end soon. As internet speeds increase and the number of connected devices grows, botnets will become larger and more powerful. For the gaming industry, DDoS attacks are now an inevitable operational risk.

But the industry is adapting. Through the adoption of proactive vulnerability testing, decentralized cloud infrastructure, and sophisticated traffic analysis, game publishers and their platforms are building resilience. The goal is not to prevent every packet of malicious traffic, but to ensure that when the attack comes, the game goes on.

For the players, the best defense is awareness. By securing their own connections and understanding the nature of these attacks, the community can deny attackers the satisfaction of a reaction. In the end, the only way to truly defeat a DDoS attacker is to ensure their efforts result in nothing but a wasted effort and a stable connection.

About DigiCert UltraDDoS Protect

DigiCert UltraDDoS Protect offers advanced, state-of-the-art solutions to safeguard gaming platforms against the growing threat of Distributed Denial of Service (DDoS) attacks. Our robust mitigation tools and real-time traffic analysis provide unparalleled protection designed specifically to minimize disruptions to online gaming properties. By leveraging adaptive technologies and scalable infrastructure, DigiCert UltraDDoS Protect ensures continuous uptime and a seamless experience for gamers, even during high-volume attack attempts.

Additionally, our tailored strategies are designed with the gaming industry in mind, ensuring both speed and resilience without compromising performance. Whether you're managing a single multiplayer server or a large-scale gaming network, DigiCert UltraDDoS Protect empowers your platform to withstand and neutralize attacks at any scale.

Take the first step toward securing your gaming property today. Contact DigiCert to learn more about how UltraDDoS Protect can help defend against threats and preserve your community's trust and engagement.

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.