BOT PREVENTION FOR ONLINE GAMING & BETTING

PROTECT YOUR WEB APPLICATIONS, MOBILE APPS, AND APIS AGAINST AUTOMATED ATTACKS IN REAL-TIME

- Highest accuracy
- Filter bots from analytics
- Customizable actions against bot signatures
- Fast and flexible deployment

Online gaming and betting websites and mobile applications are growing at the highest rates ever, with average user time having substantially increased during the current Covid-19 pandemic. Bot masters always follow the money, and the growing popularity of online gaming has led to large spikes in bad bots targeting gaming and betting portals.

User accounts are targeted by bots to cash out on accumulated credits or referral bonuses. New accounts are created to obtain discounts and other offers such as free spins and trials. Bots also scrape data on betting lines that are proprietary to each business, in order to sell the data to nefarious parties and competitors. Arbitrage techniques are increasingly being used to game betting systems, increase betting odds in favor of bots, and maliciously disrupts the level playing field.

SYMPTOMS OF A BOT ATTACK ON GAMING & BETTING PORTALS

- User complaints about payment fraud
- Reports of theft of loyalty points, stored credits, and gift vouchers
- High number of failed login attempts
- Sudden increases in account creation rate
- Complaints about limited availability of tournament slots
- Reduced website performance and service degradation
- Players reporting automated game play and other signs of cheating
- Reduction in average betting margins and increase in payouts due to cheat-bots
- Advertisers reporting fraudulent impressions
- Unexpected changes in website and application metrics

IMPACT OF BOTS ON ONLINE GAMING & BETTING PORTALS

Account Takeover

Credential stuffing and brute force attacks are used to gain unauthorized access to customer accounts and cash out player credits, vouchers, and points.

Application DDoS

Attackers deploy thousands of bots to exhaust web servers, third-party APIs, inventory databases and other critical resources.

Poor user experience

Bots steal users' credits, snap up exclusive tournament slots, and leverage their speed to cheat at games.

Scraping of proprietary content

Bots scrape critical betting line data and other valuable content.

Lower retention rates

Frustrated gamers quickly abandon gaming and betting portals that are infested with bots programmed to cheat at games and take over accounts to steal stored credits ot points.

Spam messages and comments

Bots create nuisansce by posting unwanted comments and commiting troll-like activities.

Skewed Analytics

Bots create nuisansce by posting unwanted comments and commiting troll-like activities.

INTEGRATION OPTIONS

- Web Server Plugins
- Cloud Connectors
- JavaScript Tag
- Virtual Appliance
- SDKs for PHP, Java, C#, .Net, Ruby, Django, Node.js, CloudFusion, Android & iOS

WHY RADWARE BOT MANAGER

Radware Bot Manager protects over 80,000 internet properties owned by global online brands across 70 countries. We use a combination of technologies to accurately distinguish bots from human users. Some of these technologies include user behavioral analysis, device fingerprinting, browser fingerprinting, intent-based deep behavioral analysis (IDBA) and machine learning. We also provide gaming and betting portals with comprehensive analytics detailing the most targeted webpages and categories on their properties.

Radware's Bot Manager defends online gaming and betting websites, applications, and their APIs against automated attacks and ensures that only legitimate users and devices can access their services. Bot Manager prevents unauthorized log-ins by analyzing the API call made during a log-in attempt.

Bot Manager leverages proprietary intent-based deep behavioral analysis (IDBA) to understand the intent behind every request and blocks all malicious activity. It relies on collective intelligence of bot profiles and fingerprinted devices to optimize detection accuracy and integrates into existing infrastructure without any change in the technology stack.

BENEFITS

- Prevent user account takeover and theft of credits and bonus points
- Log-in tracking alerts users about unauthorized log-in attempts
- Eliminate fraudulent purchases, protect rewared programs, and improve customer loyalty
- Reduce payment card chargebacks and penalties, and improve merchant reputation
- Improve customer satisfaction through fair game play and betting
- Increase customer loyalty and positive word-of-mouth with a bot-free gaming portal
- Obtain accurate analytics across all user touchpoints
- Achieve better ROI from marketing spends and go-to-market strategies

About Radware

Radware® (NASDAQ: RDWR), a leading provider of cyber security and application delivery solutions, acquired ShieldSquare in March 2019. ShieldSquare is now Radware Bot Manager.

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, LinkedIn, Radware Blog, Twitter, YouTube, Radware Mobile for iOS and Android, and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.