Radware Bot Manager Prevents International Revenue Share Fraud (IRSF) for Leading US-Based E-Commerce Platform

CUSTOMER:

A US-based global e-commerce platform.

INDUSTRY:

E-Commerce.

CHALLENGES FACED:

- Automated fake account creation.
- OTP verification exploitation leading to IRSF.
- Financial losses estimated at hundreds of thousands of dollars weekly.
- High bot traffic volume overwhelming existing solutions.

Overview

This US-based organization is a leading multinational e-commerce platform operating in markets across the world, with billions of live listings and millions of active buyers. As a digital marketplace connecting millions of buyers and sellers, the company relies critically on robust digital infrastructure and secure transaction mechanisms. Their digital systems included multiple touchpoints including customer registration, product listings, payment processing, and order management. These factors made the e-commerce portal an attractive target for a wide range of sophisticated malicious bot activities that threatened their digital infrastructure and business operations.

The organization had already deployed Radware Bot Manager earlier, to mitigate the risks of large-scale sophisticated bot attacks such as account takeover (ATO), price and content scraping, and carding attacks on their key applications.

The client's positive experience with Bot Manager led to them also deploying it to prevent International Revenue Share Fraud (IRSF) activities, a relatively new threat surfacede that was causing financial losses and threatening customer trust.

WHY RADWARE BOT MANAGER?

- AI-powered bot detection and mitigation.
- Minimal false positives to preserve user experience.
- Real-time behavioral analysis for sophisticated threats.
- Proven expertise in mitigating advanced bot-driven fraud .
- Comprehensive analytics and reporting for full visibility.

Challenges

IRSF represents one of the most sophisticated and financially damaging fraud mechanisms that involves telecommunications fraud within e-commerce digital transactions. Fraudsters use malicious 'bad' bots to target the registration, authentication, and transaction processes used by online marketplaces to generate illicit revenue in partnership with rogue telecom providers in foreign markets.

The specific IRSF attack vectors targeting the e-commerce platform included:

Automated Fake Account Creation: Sophisticated bots created thousands of fake user accounts to trigger account verification or upgradation workflows. These accounts were abandoned after executing fraudulent activities.

OTP Verification Exploitation: The e-commerce platform used an OTP verification process as a security measure to complete the account creation process and for authentication and transaction processing workflows. This process was being abused by fraudsters running bots to trigger calls to premium international numbers operated by nefarious telecom providers which were associated with the attackers and based in countries like Ukraine and Russia. The artificially inflated service charges from these calls to premium numbers were then charged to the e-commerce platform by these shady telecom firms who in turn shared the fraudulent proceeds with the attackers.

The company had earlier engaged another security vendor to secure the OTP processing layer to provide intelligence on the risk profile of entered phone numbers and block the OTP authentication process in case of abuse. However, they were still confronted with high volumes of malicious bot traffic on their OTP flows, and wanted a solution that could proactively mitigate malicious bot attacks and protect against this type of bot-driven fraud.

Most concerning for our client was the fact that they were experiencing large financial losses through these **fraudulent IRSF-related activities estimated at hundreds of thousands of dollars every week**. Their internal security and risk teams had attempted to mitigate these losses by strengthening the account verification and phone number validation processes, but were unsuccessful in combating the high volume and sophisticated nature of these bot-driven attacks.

Solution

The client's internal security and risk teams decided to activate Radware Bot Manager on affected applications including its account creation and OTP workflows, having already used Bot Manager to protect against other types of attacks such as ATO and scraping. To this end, a multi-layered protection strategy was deployed to protect against IRSF attacks:

Preemptive Blocking

Radware Bot Manager's Active Attackers feed and global threat intelligence repository immediately blocked malicious sources from the client's account creation and OTP workflows, significantly reducing the number of bad bot hits on target applications.

Behavioral-Based Detection

For sophisticated humanlike bots that evaded preemptive protection mechanisms and attempted to create fake accounts or trigger OTPs, Bot Manager's AI-driven behavioral-based detection algorithms generated signatures in real-time to accurately analyze user behavior and identify malicious intent without impacting legitimate users.

Advanced Mitigation

Though malicious attacks on the e-commerce firm's OTP workflows were initially mitigated by serving CAPTCHAs, Radware Bot Manager detected the use of third-party CAPTCHA farm services by analyzing signals in the post-CAPTCHA-solving stage. Radware's advanced mitigation strategies completely neutralized these bot-driven attacks on targeted applications.

Comprehensive Reporting and Analytics

Bot Manager provided granular classification and detailed analytics around the IRSF-related malicious bot activities detected, giving the e-commerce platform real-time visibility into bot attack patterns and mitigation performance.

Benefits

Implementing Radware Bot Manager delivered immediate and measurable results:

- **90% Reduction in IRSF Bot Traffic**
  The advanced bot mitigation strategies led to a drastic drop in malicious bot hits on account creation and OTP workflows.
- **$5 Million in Annual Fraud Prevention**
  Real-time mitigation prevented further IRSF-related financial losses, saving an estimated $5 million annually.
- **Improved User Experience**
  Minimal false positives ensured legitimate customers experienced smoother registration and verification processes.
- **Reduced Operational Costs**
  Optimizing OTP verification workflows reduced unnecessary telecom charges and customer support workloads.
- **Enhanced Security Posture**
  With real-time insights into emerging attack vectors, the platform adopted a proactive, intelligence-driven approach to counter evolving bot threats effectively.

By securing its digital infrastructure against IRSF and other bot-driven fraud, the e-commerce platform improved customer trust, operational efficiency, and platform reputation—ensuring continued business growth across its global markets.

To learn more about how Radware Bot Manager and other solutions comprehensively protect your organization from cyber-attacks, click here to contact us.

RWI 413 | 01.02.2025