REAL-TIME BOT PROTECTION AGAINST CARDING

DETECT AND BLOCK CREDIT CARD, GIFT CARD AND LOYALTY PROGRAM FRAUDS

"Radware Bot Manager solution met our stringent latency and false-positive requirements, and has virtually eliminated the threat we were facing from bots. Radware Bot Manager is a rare example of a company whose product exceeds the marketing promises"

– BRENT STACKHOUSE, DIRECTOR OF SECURITY AND COMPLIANCE, ZULILY

Fraudsters deploy bots on merchant's payment processes to either test stolen-credit-card-numbers or build complete cardholder dataset. Web application firewall defenses are not capable of detecting carding and card cracking attempts. Gift cards and loyalty programs are highly susceptible to token cracking. Such attacks decipher valid coupon numbers, voucher codes, etc.

Symptoms of a Carding Attack

Increased Chargebacks and Transaction Disputes

High Cart Abandonment Rates

Reduced Avg. Basket Value

High Ratio of Failed Payment Authorizations

Impact of Carding and Online Frauds

Chargebacks & Loss of Revenue

Accepting stolen-credit-cards can cause businesses to lose products/services and incur chargeback penalties. Radware Bot Manager prevents malicious bots from programmatically targeting checkout pages. We detect any suspicious surge in bot activity on payment processing pages and report such incidents as potential carding attacks.

Poor Merchant & Brand Reputation

Excessive chargebacks can result in termination of merchant's account, and stolen reward points can tarnish a brand's reputation. Our bot management solution is powered by an expert team of data scientists who are always scouting for ever-evolving approaches of fraudsters. Radware Bot Manager can be relied on to safeguard consumers' data and protect your reputation as a merchant and brand.

Ineffective Gift Card and Loyalty Programs

Tokens used in coupons/vouchers/gift-cards don't follow complex patterns and are easy to crack using an automated program. Fraudsters use this vulnerability to siphon off reward points. Radware Bot Manager collects more than 250+ parameters from the end user's browser to identify thousands of highly sophisticated bots that mimic real user behavior. Radware Bot Manager can identify and stop token-cracking attacks.

KEY BENEFITS

Reduce Financial Risks by Eliminating Chargebacks and Penalties

Stop Gift Card Fraud and Online Coupon Abuse

Protect Merchant and Brand Reputation

WHY RADWARE BOT MANAGER

Radware Bot Manager has a non-intrusive API based approach to detect bot activities on e-commerce websites. Our bot detection engine uses device fingerprinting, user behavior modeling, collective bot intelligence and machine learning techniques to spot any suspicious activity across payment processing pages. We block carding attempts before they cause a financial fraud.

OWASP THREATS STOPPED BY RADWARE BOT MANAGER

- **OAT-001– Carding**
  Multiple payment authorization attempts used to verify the validity of bulk stolen payment card data
- **OAT-010 – Card Cracking**
  Identify missing start/expiry dates and security codes for stolen payment card data by trying different values
- **OAT-010 – Token Cracking**
  Mass enumeration of coupon numbers, voucher codes, discount tokens, etc.

Success Story

The e-tailer was continuously targeted by account takeover attacks and carding fraud. Radware Bot Manager stopped account takeover activity in its tracks and eliminated carding attempts that resulted in reduced chargebacks.

Read How A Top 5 E-tailer of US Defeated Carding Attacks

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.