

REAL-TIME BOT PROTECTION AGAINST ACCOUNT TAKEOVER

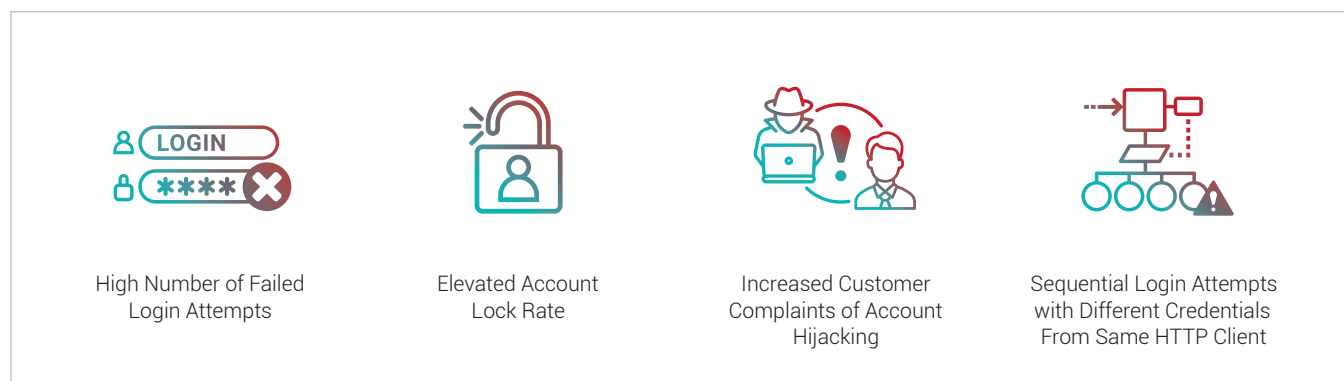
BLOCK CREDENTIAL STUFFING AND BRUTE FORCE ATTACKS

“We onboarded Bot Manager in the midst of our peak season, and saw immediate results/benefits. Our customers’ experiences are our top priority. By working with Radware, we are able to better secure and improve the shopping experience.”

– DANIEL PADEVET, HEAD OF WEB & IT OPERATIONS TEAM, ALZA.CZ

Account takeover is a necessary step for a variety of online frauds involving e-commerce, payments, reward programs and financial services. Credential stuffing and brute force methods are the two most common techniques used by fraudsters. Credential stuffing exploits users’ propensity to use same username and password at multiple websites, and brute force method is a way to identify valid credentials by trying different values for usernames and passwords.

Symptoms of an Account Takeover Attack



Impact of Account Takeover

Fraudulent Transactions & Abuse of Reward Programs

Financial fraud via compromised accounts doesn't only cause a loss of revenue but also sabotages customer loyalty efforts. Radware Bot Manager blocks illegal account access before it is used for fraudulent transactions. Our algorithms are battle-tested for higher accuracy during peak hours.

Damage to Brand Reputation

Reputational damage undermines customer's confidence and can cause loss of revenue. With collective bot intelligence, Radware Bot Manager continuously adapts to evolving bot patterns and can block sophisticated account takeover attacks.

KEY BENEFITS



Eliminate Account Takeover Attempts and Avert Financial Loss



Protect Reward Programs & Improve Customer Loyalty



Defend 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 login and signup pages. We have a proven track record in blocking advanced distributed attack and highly sophisticated 'slow & low' attacks.

OWASP THREATS STOPPED BY RADWARE BOT MANAGER

- ▶ **OAT-008 – Credential Stuffing**
Mass log in attempts used to verify the validity of stolen username/password pairs
- ▶ **OAT-007 – Credential Cracking**
Identify valid login credentials by trying different values for usernames and/or passwords.

About Radware

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.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services or processes described herein are subject to change without notice.

© 2021 Radware Ltd. All rights reserved. Any Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: <https://www.radware.com/LegalNotice/>. All other trademarks and names are the property of their respective owners.