REAL-TIME BOT PROTECTION API ABUSE

PROTECTION AGAINST AUTHENTICATION FLAWS, LACK OF ROBUST ENCRYPTION, BUSINESS LOGIC VULNERABILITY, AND POOR ENDPOINT SECURITY

- Highest accuracy
- Fast and flexible deployment
- Filter bots from analytics dashboards
- Feed fake data or take custom actions against bot signatures

"Together with Radware Bot Manager, we made our website a much safer environment for our users and their data, further branding Njuskalo.hr as a place to go for buying and selling online."

— BORIS NAĐ, TECHNICAL OPERATIONS MANAGER, NJUSKALO, CROATIA'S NO. 1 MARKETPLACE

The widespread adoption of IoT devices, emerging "serverless" architectures hosted in public clouds and the growing dependency on machine-to-machine communication are reasons for a change in the modern application architecture. Application programming interfaces (APIs) have emerged as the bridge to facilitate communication between different application architectures. APIs assist in quicker integration and faster deployment of new services. In addition, DevOps requires end-to-end process automation that often leverages APIs for service provisioning, platform management, and continuous deployment.

INTEGRATION OPTIONS

- Web Server Plugins
- Cloud Connectors
- JavaScript Tag
- Virtual Appliance

Despite their rapid and widespread deployment, APIs remain poorly protected, and automated threats are mounting. Personally identifiable information (PII), payment card details, and business-critical services are at risk due to bot attacks.

KEY API VULNERABILITIES

Authentication Flaws

Many APIs do not check authentication status when the request comes from a genuine user. Attackers exploit such flaws in different ways, such as session hijacking and account aggregation, to imitate genuine API calls. Attackers also reverse engineer mobile applications to discover how APIs are invoked. If API keys are embedded into the application, an API breach may occur. API keys should not be used alone for user authentication. Radware Bot Manager blocks attempt to scan APIs for vulnerabilities and protects business-critical APIs against automated attacks.It also analyses API requests to detect and block malicious attempts to evade device profiling and directly access the API.

Lack of Robust Encryption

Many APIs lack robust encryptions between the API client and server. Attackers exploit such vulnerabilities through man-in-the-middle (MITM) attacks. Attackers intercept unencrypted or poorly protected API transactions to steal sensitive information or alter transaction data. Also, the ubiquitous use of mobile devices, cloud systems, and microservice patterns further complicates API security because multiple gateways are now involved in facilitating interoperability among diverse web applications. The encryption of data flowing through all these channels is paramount. Radware Bot Manager provides edge-to-endpoint API security to ensure a secure data exchange.

SYMPTOMS OF BOT ATTACKS ON APIS

- Single HTTP request (from a unique browser, session or device)
- An increase in the rate of errors (e.g., the HTTP status code 404, data validation failures, authorization failures, etc.)
- Extremely high application usage from a single IP address or API token
- A sudden increase in API usage from large, distributed IP addresses
- A high ratio of GET/POST to HEAD requests for a user/session/IP address/API token compared to the ratios of legitimate users

BENEFITS

- Ensure exclusivity of your classified ads
- Eliminate spam leads
- Restore advertisers' confidence by securing their contact details from scrapers
- Strengthen product and marketing decision-making with accurate analytics

Business Logic Vulnerability

APIs are vulnerable to business logic abuse. Attackers make large-scale API calls on an application server or slow POST requests, resulting in a denial of service. A DDoS attack on an API can result in disruptions to a front-end web application. Radware Bot Manager applies challenge-response authentication and CAPTCHA on suspected API calls to avert potential business logic abuse attempts. Responses to these challenges help Radware Bot Manager build a closed-loop feedback system, which dynamically improves Radware Bot Manager's machine learning models and assists in reducing false positives.

Poor Endpoint Security

Most IoT devices and microservice tools are programmed to communicate with servers via API channels. These devices authenticate themselves on API servers using client certificates. Hackers attempt to gain control over an API from the IoT endpoint, and if they succeed, they can re-sequence the API order, thereby resulting in a data breach. Radware Bot Manager uses intelligence gathered from its client base to take preemptive action against potential attempts to illegally access IoT endpoints and microservice tools.

WHY RADWARE BOT MANAGER

Radware Bot Manager defends APIs against automated attacks and ensures that only legitimate users and devices can access APIs, blocking any attempt to reverse engineer mobile SDKs. Radware Bot Manager leverages proprietary intent-based deep behavioral analysis (IDBA) to understand the intent behind an API request and block malicious activity. It relies on collective intelligence of bot profiles and fingerprinted devices to optimize detection accuracy and is integrated into the existing infrastructure without any change in the technology stack.

OWASP THREATS STOPPED BY RADWARE BOT MANAGER

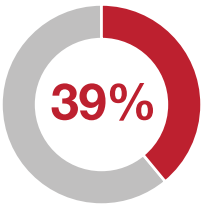
- **OAT 001** – Carding
- **OAT 007** – Credential Cracking
- **OAT 008** – Credential Stuffing
- **OAT 011** – Web Scraping
- **OAT 015** – Application DDoS
- **OAT 016** – Skewing
- **OAT 021** – Denial of Inventory

AN API SECURITY CHECKLIST

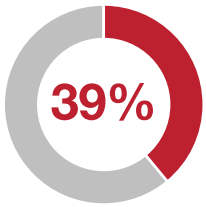
These top nine best practices are a must for protecting your API infrastructures against hacking and abuses:

- Monitor and manage API calls comingfrom automated scripts (bots)
- Drop primitive authentication
- Implement measures to prevent APIaccess by sophisticated human-likebots
- Robust encryption is must-have
- Deploy token-based rate limitingequipped with features to limit APIaccess based on the number of IPs,sessions, and tokens
- Comprehensive logging of requestsand responses
- Scan the incoming requests formalicious intent
- Support clustered API implementationto handle fault tolerance
- Track usage and journey of API calls tofind anomalies

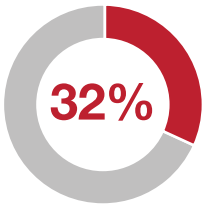
SEVEN COMMON ATTACKS AGAINST APIS



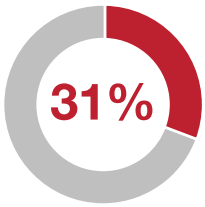
ACCESS VIOLATIONS



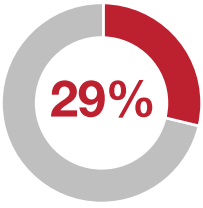
PROTOCOL ATTACKS



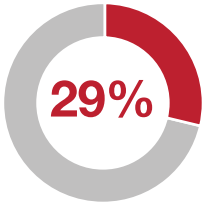
BRUTE FORCE



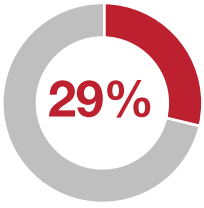
DENIAL OF SERVICE



IRREGULAR JSON/XML EXPRESSIONS



INJECTIONS



PARAMETER MANIPULATIONS

FIVE ADVANTAGES OF RADWARE BOT MANAGER

Broad Attack Detection and Coverage

Radware Bot Manager protects all channels (web, mobile and APIs) against sophisticated attacks in real time and helps organizations accurately distinguish between good bots, bad bots and genuine users.

Edge-to-Endpoint API Security

Secure edge gateways, micro gateways and microservices for comprehensive API security.

Collective Bot Intelligence

A repository of bot signatures and fingerprints from a global customer base allows for preemptive action against infiltration attempts by bad bots. Collective bot intelligence initiates pre-attack notifications gathered from continuously mining data across the web and darknet.

Comprehensive Reporting and Analytics

Radware Bot Manager offers out-of-the-box granular reporting for all bot families, including token-based offline analytics. Organizations can track automated activity based on user agents, geographies, referrers, and pages targeted. Visualization APIs for data collection, management and reporting are available.

Flexible Deployment Options

Radware Bot Manager offers flexible deployment options, which include on-demand, on-premise, and cloud-based for different infrastructures. Integration options include CDN plug-ins, JavaScript tags, web server plug-ins, and API cloud connectors. Other options are the mobile SDK and a virtual appliance.

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 thi document. The technologies, functionalities, services or processes described herein are subject ro 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.