Real-time Bot Protection for APIs

Protection Against Authentication Flaws, Lack of Robust Encryption, Business Logic Vulnerability, And Poor Endpoint Security

The Challenge in Potecting against Bot Attacks

The growing adoption of IoT devices, emerging "serverless" architectures hosted in public clouds and the growing dependency on machine-to-machine communication have introduced many changes to modern application architecture. Application programming interfaces (APIs) have emerged as crucial bridges to facilitate communication between different application architectures, helping lead to 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.

Despite their 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. 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 encryption 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. In addition, 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 secure data exchange.

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 its 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.

Integration Options

- CDN
- App Server SDKs
- DNS Diversion
- Other Third-party Integrations
- Web Server Plugins
- ADC
- On-premise Sensor

Symptoms of an Account Takeover Attack

- 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.

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 log-in and signup pages. We have a proven track record in blocking advanced distributed attacks and highly sophisticated 'low and slow' attacks.

Radware Bot Manager has the widest mitigation option available to its users, and now with Crypto Challenge, Radware Bot Manager adds another mitigation option to stop sophisticated bot attacks, while providing a CAPTCHA-less mitigation option with Blockchain-based Cryptographic Proof of Work.

Crypto Challenge is a behavior-enforcing mechanism that detects anomalies against a baseline of normative behavior. When an anomaly is detected, the mitigation method challenges the user device by creating CPU-intensive browser-based challenges with gradually increasing difficulty, forcing the attacker's CPU to work harder every time it is challenged, eventually choking the device, thereby transferring the cost of the attack to the attacker.

Radware Bot Manager SDK provides a comprehensive solution for mobile app protection. It includes a unique attestation feature for Google (Android) and Apple (iOS) devices that ensures device authenticity, preventing emulators, modified applications, or modified OS from accessing your resources. Additionally, the SDK offers Secure Identity by creating a unique identity for each user, which is used to validate every request, protecting against identity spoofing, tampering, and replay attacks. The combination of secure identity and integrated device authentication provides enhanced protection against bot attacks on mobile apps, preventing them from affecting your infrastructure.

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 Nad, Technical Operations Manager, Njuskalo, Croatia's No.1 Marketplace

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-premises, 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.

An API Security Checklist

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

- Monitor and manage API calls coming from automated scripts (bots)
- Drop primitive authentication
- Implement measures to prevent API access by sophisticated human-like bots
- Robust encryption is a must-have
- Deploy token-based rate limiting equipped with features to limit API access based on the number of IPs, sessions, and tokens
- Comprehensive logging of requests and responses
- Scan the incoming requests for malicious intent
- Support clustered API implementation to handle fault tolerance
- Track usage and journey of API calls to find anomalies

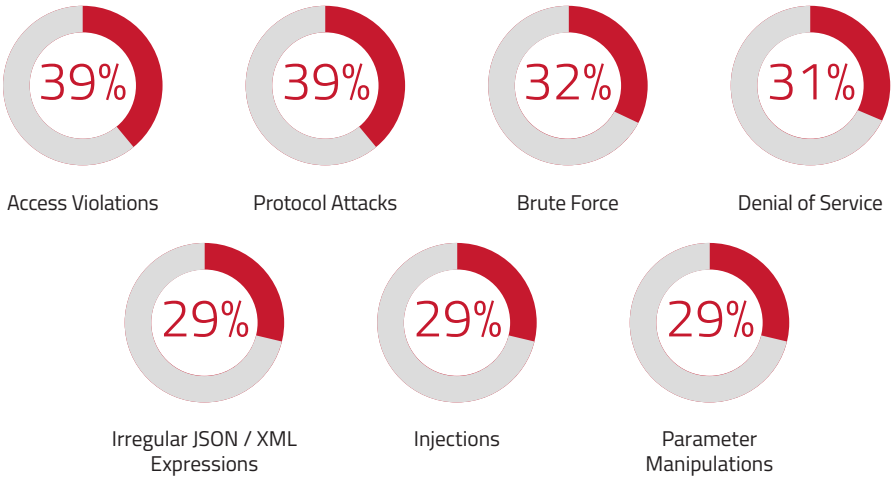
Radware Key Benefits

- 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

Widest Mitigation Options

- Allow
- Challenge CAPTCHA
- Block
- Feed Fake Data
- Throttle
- Drop
- Session Termination
- Redirect Loop
- Log Only
- Custom Response
- Crypto Challenge

Seven Common Attacks Against APIs



HK-116 | 20.4.2023