API BOT PROTECTION FOR AZURE APPLICATIONS

PROVIDING ADVANCED BOT DETECTION AND BLOCKING FOR APPLICATIONS IN AZURE UTILIZING AZURE FRONT DOOR AND AZURE APPLICATION GATEWAY

Bot attacks on web, mobile apps and APIs have significantly evolved from their origins as simple scripting tools using command line interfaces. In addition, attackers now reverse engineer mobile apps to understand the API communication sequence and target the APIs to scrape business critical data, perform Application Distributed Denial of Service attacks and takeover accounts.

Attackers exploit API vulnerabilities to steal sensitive data, including user information and business-critical content. Modern application architecture trends — such as mobile device API calls, use of cloud systems and microservice designs patterns complicate security of APIs because they involve multiple gateways to facilitate interoperability among diverse web applications. Today's extensive deployment of internal APIs, combined with mobile access and increased dependence on cloud-based APIs, means that web application security defense systems that protect only the external perimeter are ineffective.

Despite 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.

SYMPTOMS OF BOT ATTACKS ON APIs

- Single HTTP request (from a unique browser, session or a device)
- An increase in the rate of errors (e.g., HTTP status code 404, data validation failures, authorization failures, etc.)
- Extremely high application usage from a single IP address or API token
- A sudden uptick 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 legitimate users

Figure 1: Most common automated threats targeting APIs

HOW DOES RADWARE SAFEGUARD APIs AGAINST BOT ATTACKS

How does Radware safeguard APIs against bot attacks?

Radware has pioneered API protection from bots by introducing enhanced detection capabilities that protect vulnerable APIs from malicious attacks:

1. M2M Protection – API Client SDK

In the case of regular website access, most forms of bot protection leverage the capabilities of the web browser to store and track cookies, fingerprinting the user system using the browser's JavaScript capabilities and analyzing various parameters and headers that every browser generates.

Radware's Client SDK for Machine-to-Machine API protection is a simple SDK that needs to be integrated into client libraries used to access API services. This Client SDK collects several parameters from the interacting client devices and implements a logic similar to what browsers use to maintain cookies. Details of every transaction are communicated to Radware's analysis engine to analyze the authenticity of the access. The parameters collected provide the bot detection engine with the information required to implement device fingerprinting and identify authentic access patterns to block malicious access attempts.

2. ATO Protection for APIs

In conventional bot protection systems, only the requests to API services are analyzed. This often requires additional forms of confirmation to know if the authentication was successful. For websites, the page that is called up next confirms successful authentication, but this is difficult to confirm when logging in via mobile or device APIs. Radware Bot Manager intercepts the response from the API service to collect relevant data for the bot detection engine to analyze. The bot detection engine accurately tracks every log-in and authentication process to ensure high levels of protection for all API end-points.

3. API Flow Control

Radware Bot Manager prevents abuse of APIs by providing a fair API access model that is automatically built by studying patterns of access to a given application over time. The API flow control module is based on a statistical model of API access to analyze expected probabilities of transitions across different nodes during a period of time. Once the model is ready, access patterns are then analyzed against this model to check if the sequence is suspicious and needs to be blocked. This provides unprecedented detection capabilities against malicious API access patterns.

4. Invocation Context-Based Protection

By analyzing how users engage with applications, their usage patterns, and the overall invocation context, it is possible to identify bots targeting APIs. Malicious bots try to bypass 'regular navigation processes' on an application to access APIs and get information in the shortest time possible. Radware Bot Manager has an enhanced capability to analyze API traffic for the right context and disallows direct access to APIs without a previous web transaction or invocation from a mobile device. The module allows you to filter 'bad' API calls as soon as they initiate any communication.

.

RADWARE BOT MANAGER PROTECTS APIs IN AZURE

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 leverages proprietary Intent-based Deep Behavior 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.

> Radware Bot Manager is a fully managed service providing comprehensive protection against bot attacks on websites, mobile applications, and API's.
>
> Radware Bot Manager API endpoints are available in Azure and the protected application can asynchronously/synchronously query the API endpoint to determine if the user is flagged as a malicious Bot. This provides ultra-low latency for all Azure hosted customers with high bot detection capability and ultra-fast response time.

The mitigation options offered by Radware Bot Manager are flexible and the user has the option to set various difficulty levels for the mitigation actions like showing a CAPTCHA, outright blocking, as well as redirect loops, dropping requests, feeding fake data, and more.

The growing impact of API attacks on business cannot be ignored. Developers should investigate moving away from conventional security systems and adopt more robust and specialized solutions that can block automated attacks in real-time. With Covid-19 many businesses are moving online, where they are immediately under the constant threat of malicious botmasters that are trying to steal data and disrupt business. How prepared are you to protect your business and consumers?

EIGHT ADVANTAGES OF RADWARE BOT MANAGER FOR APIs

1. Purpose-built to Prevent API Abuse

Radware Bot Manager for APIs is specifically designed to consider all automated threats to APIs. The solution leverages advanced machine learning that resemble the API environment and intercommunication patterns, monitoring the invocation context and allowing flow control to detect and prevent any malicious activity.

2. Broad Attack Detection and Coverage to Secure Sensitive Information

Radware Bot Manager protects APIs from sophisticated bot behaviors in real time. It intercepts the response from the API service and collects relevant data to precisely track all login/authentication accesses and prevents account takeover (credential stuffing, Brute Force) attempts on authentication APIs.

3. Edge-to-Endpoint API Security

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

4. 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.

5. Comprehensive Reporting and Analytics

Radware 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.

6. Flexible Deployment Options

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

7. Complete Application and API Security Suite

Easy integration with Radware's Web Application Firewall (WAF) and Distributed Denial-of-Service (DDoS) mitigation solutions on premises and in the cloud.

8. Fully Managed Service

A cloud security service integrated with Radware's Cloud WAF — a seamless experience for onboarding, reporting, and configuration with a unified portal.

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: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.