radware

HOW TO KEEP APIs SECURE FROM BOT CYBERATTACKS

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

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.

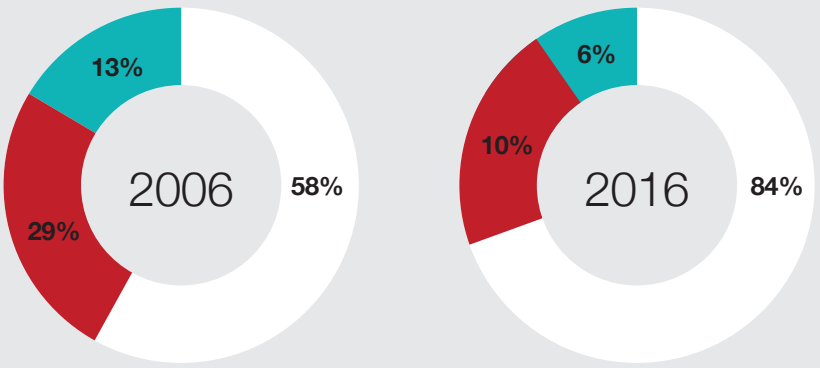


Figure 1: Distribution of API protocols and styles based on directory of APIs listed at Programmable Web

May 2016

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 2: Most common automated threats targeting APIs

KEY API VULNERABILITIES AND AUTOMATED ATTACKS

1 Authentication Flaws and Account Takeover

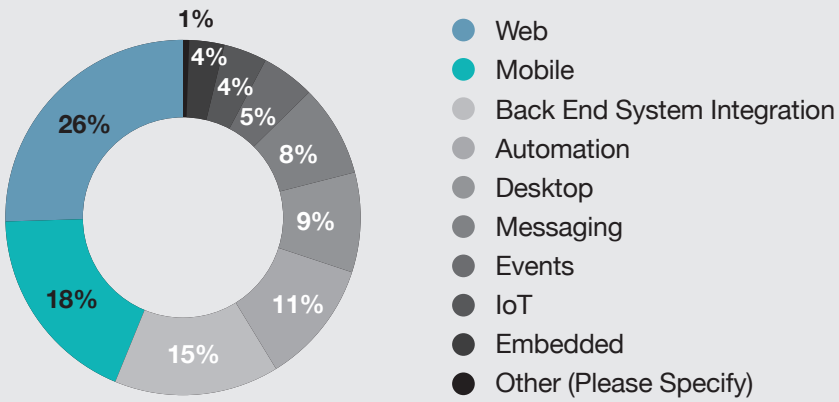
Many APIs do not check authentication status when the request comes from a genuine user. Attackers exploit such flaws in different ways, such as session hijacking and account aggregation, to imitate genuine API calls. Attackers also reverse engineer mobile applications to discover how APIs are invoked.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

2 Lack of Robust Encryption

Many APIs lack robust encryption between the API client and server. Attackers exploit vulnerabilities through man-in-the-middle 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 complicate 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.

Figure 3: 56% are not standard web or mobile APIs and require a tailored solution

(Source: The State of API 2019, SMARTBEAR)



3 Business Logic Vulnerability

APIs are vulnerable to business logic abuse. This is exactly why a dedicated bot management solution is required and why applying detection heuristics that are good for both web and mobile apps can generate many errors — false positives and false negatives. Radware's solution is tailored to learn the communication flow and invocation context and use challenge-response authentication (such as CAPTCHA) on suspected API calls to avert potential business logic abuse attempts. Responses to these challenges helps Radware build a closed-loop feedback system that dynamically improves Bot Manager's machine-learning models.

4 Poor Endpoint Security

Most IoT devices and microservice tools are programmed to communicate with the server 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 easily re-sequence the API order, thereby resulting in a data breach. Radware uses intelligence gathered from its global customer base to take preemptive action against potential attempts to access IoT endpoints and microservice tools illegally.

AN API SECURITY CHECKLIST

These top 9 best practices are a must for protecting your API infrastructures against hacking and abuses.

- 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 critical
- 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
- Supporting clustered API implementation to handle fault tolerance
- Track usage and journey of API calls to find anomalies

RADWARE BOT MANAGER PROTECTS APIS

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.

HOW RADWARE BOT MANAGER HANDLES MALICIOUS BOT TARGETING APIS

API Flow Control – Protect Machine to Machine & IoT	API Client SDK – Protect Machine to Machine APIs
Each API is a node and the probability of a flow navigation from one node to the other represented by the arch weight. Low probability flows will be blocked.	Effectively fingerprinting and uniquely identifying attack sources over APIs to detect Bot Attacks on APIs through a new, unique application agnostic SDK.
Invocation Context – Protect Web and Mobile APIs	**Authentication Flow – ATO Protection for APIs**
Disallow direct access to APIs without a previous web transaction or invocation from a mobile device.	Validate legitimate access to assets. Detect unsuccessful login flow and block attack source generating multiple unsuccessful API login attempts.

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.