radware

THE FOUR BIGGEST CHALLENGES TO KEEPING MODERN APPLICATIONS SECURE

Modern applications are incredibly difficult to keep secure. Whether they are web or mobile, custom developed or cloud-based, applications are now scattered across a plethora of digital platforms and frameworks. To support and accelerate business operations, applications now rely heavily on third-party resources that interact via APIs. Unsecure APIs represent an application security blind spot, and as a result, the attack surface threatening applications is growing exponentially. Application vulnerabilities are now the fastest-growing cybersecurity threat to organizations, according to a year-over-year comparison of Radware's annual *Global Application & Network Security Report*.

Applications, and the APIs they leverage, must be protected against an expanding variety of attack methods. In addition, DevOps and agile development practices mean that applications are in a state of constant flux, and security policies must adapt to keep pace. Security solutions should make educated decisions in real time to mitigate the more advanced attacks now targeting applications. In addition, comprehensive protection is required that goes beyond implementation of a web application firewall (WAF). According to Radware's *The State of Web Application Security* report, only 33% of organizations say that their WAF mitigates all types of web application attacks.

THE TOP 10 THREATS TARGETING APPLICATIONS

The OWASP Top 10 list provides a starting point for ensuring protection from the most common and virulent threats — application misconfigurations that can lead to vulnerabilities, and detection tactics and mitigations. This list serves as an industry benchmark for the application security community and defines the basic capabilities required from a WAF to protect from common attacks like injections, cross-site scripting, cross-site request forgery, session hijacking and others. There are innumerous ways to exploit these vulnerabilities, and WAFs must be tested for security effectiveness.

Vulnerability protection is just the beginning. Advanced threats mean that application security solutions must do much more. Specifically, there are four major challenges that must be overcome to keep modern applications secure.

CHALLENGE 1: BOT MANAGEMENT

Fifty-two percent of internet traffic is bot generated, half of which are "bad" bots. Unfortunately, 79% of organizations can't make a clear distinction between good and bad bots, according to the aforementioned web application security report. This myopic view into bot traffic leaves businesses open to an array of attacks, including takeover of user accounts and payment information, scraping of confidential data, tying up inventory and skewing marketing/website analytics. Next-generation bots are highly sophisticated, mimicking human behavior and bypassing CAPTCHA or other security challenges. Distributed bots render IP-based and even device fingerprinting-based protection ineffective.

CHALLENGE 2: SECURING APIs

Machine-to-machine communications, integrated IoTs, event-driven functions and other use cases all leverage APIs to deliver agility and ubiquitous connectivity. Threats to API vulnerabilities include injections, protocol attacks, parameter manipulations, invalidated redirects and bot attacks. According to Radware's *The State of Web Application Security*, one-third of attacks against APIs intend to yield a denial-of-service (DoS) state, in addition to an array of other attack types (see Figure 1). Despite the security vulnerability that APIs pose in an app-driven world, businesses tend to grant API access to sensitive data without inspecting APIs to detect malicious activity.

7 COMMON ATTACKS AGAINST APIs

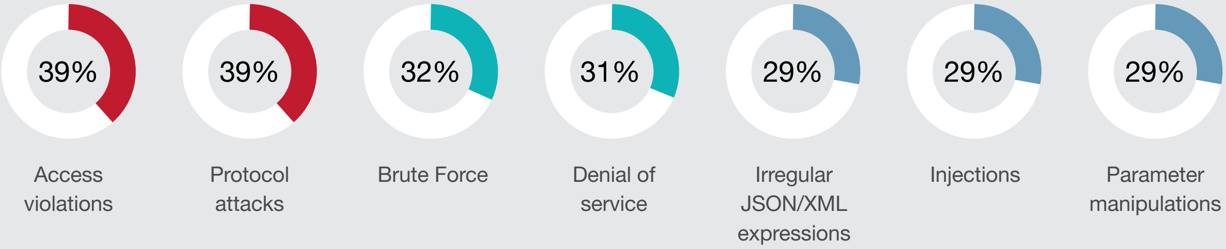

Figure 1: Seven common attacks against APIs[1]

CHALLENGE 3: DENIAL OF SERVICE

Different types of application-layer DoS attacks are still very effective at taking down application services. Examples of attacks include HTTP/S Floods, low and slow attacks (Slowloris, LOIC, Torshammer), dynamic IP attacks, buffer overflow, Brute Force attacks and more. Driven largely by IoT botnets, application-layer attacks have become the preferred DDoS attack vector. Even the best application protection is worthless if the service can be taken down.

CHALLENGE 4: CONTINUOUS SECURITY

In DevOps, agility is often valued at the expense of security. Agile development and rollout methodologies result in applications being continuously modified and updated. In such a fluid environment, it is difficult to frequently update security policies to safeguard sensitive data without creating a high number of false positives. It is a task beyond the abilities of any security expert, as the error rate and additional operational costs imposed can be enormous. Machine learning security solutions are key, as they can map application resources, analyze possible threats and create and optimize security policies in real time.

[1] Radware's *The State of Web Application Security report*

SUMMARY

Successful organizations must establish and use repeatable processes and security controls, and application managers need to take charge of the application life cycle. The organization needs to have an application security program in place that effectively coordinates all facets of its infrastructure.

To that end, be sure that any application security solution that your company evaluates not only meets your existing security needs but also is flexible enough to adapt to future infrastructure environments and attack vectors. Make sure that it fulfills these six key criteria:

- Application security solutions must encompass not only web and mobile apps but also APIs
- Include a bot management solution to overcome the most sophisticated bot-based attacks
- Mitigating DDoS attacks is an essential and integrated part of application security solutions
- A future-proof solution should protect containerized applications and serverless functions and integrate with automation, provisioning and orchestration tools
- To keep up with DevOps/agile development practices, security solutions should be able to update security policies automatically and in real time
- A fully managed service should be considered to remove complexity and minimize resource utilization

LEARN MORE ABOUT RADWARE'S **WEB APPLICATION FIREWALL** AND **BOT MANAGEMENT** SOLUTION.

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.

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.